SUMMARY OF TOPICS

The following is being proposed for preliminary review and comment only:

1. For Preliminary Review Only: Proposed First Edition of the Standard for Safety for the Evaluation of Autonomous Products, UL 4600

COMMENTS DUE: NOVEMBER 1, 2019

This proposal is for review and comment only (no ballot at this time). Please note that comments on a preliminary review document will not receive a response from the proposal author through CSDS. Instead, the proposal author will be asked to review the comments and adjust the proposals and/or supporting rationale as the author determines to be appropriate. The preliminary review process is an informal mechanism that provides authors with the opportunity to refine their proposals before they advance to the next stage in UL's standards development process.

Please provide your comments using the spreadsheet template provided in Supporting Documentation under Quick View access box on right-hand side of the CSDS work area. You should upload your final comment spreadsheet as an attachment, with a minimum of text in the free text box. Only spreadsheet entries will be tracked for action. Please make comments as specific, concrete, and actionable as possible.

Normally, the next step in the process is the more formal STP ballot and public review process. Only comments posted during the STP ballot and public review process will be provided with a response in CSDS.

1. For Preliminary Review Only: Proposed First Edition of the Standard for Safety for the Evaluation of Autonomous Products, UL 4600

BACKGROUND

A proposal for the First Edition of the Standard for Safety for the Evaluation of Autonomous Products, UL 4600, was issued for review and comment on May 13, 2019. A Standards Technical Panel (STP) Meeting was held on June 12 and 13, 2019 to discuss the comments that were received on the proposal. After the meeting, the following task groups were formed: 1) Mandatory Requirement Statements; 2) Key Terms Definitions; 3) Other Terms Definitions (combined with Task Group 2); 4) Assessment Tools and Reporting; 5) Single Point of Failure Definition/Description; 6)

Vehicle Simulation Considerations; 7) Review of Assessment; 8) Document Navigability Diagram; 9) Component Assessment Interface Plan; and 10) Overlap with Existing Standards. The current proposal reflects recommendations made by these task groups, other changes that were discussed during the June 2019 STP meeting, as well as other STP comments received on the August 9, 2019 review of the proposed document.

RATIONALE

Proposal submitted by: Deborah Prince, STP 4600 Chair, on behalf of Task Group for UL 4600

The proposed first edition of the Standard for the Evaluation of Autonomous Products, UL 4600, will cover the safety principles, tools, techniques, and lifecycle processes for building and evaluating a safety argument for fully autonomous vehicles (e.g., SAE Level 4 vehicles). Evaluation includes product ability to perform the intended function safely – and avoid performing unsafe functions whether intended or unintended. Operation is assumed to occur without human intervention based on the current system state and ability to sense and otherwise interpret the operating environment. Human contributions to safety in other than normal operation are considered (e.g., maintenance). However, the extent to which humans mitigate risk while they are performing the dynamic driving task is outside the scope of the standard.

NOTE FROM STP CHAIR:

The format of the preliminary review draft standard may seem unconventional, as well as some of the terminology used, but the proposed standard has been drafted this way intentionally in order to assist users of the standard. In this preliminary review draft, the use of informative text within the body of the normative standard has also been used intentionally for ease of review. This format may ultimately be revised as the STP continues the drafting process. As with any draft standard, it is possible that there will be numbering changes, including reordering of sections and clauses before release of the ballot draft version.

Any pilot use should consider the traceability implications of a major re-numbering of that type. The intent is to stabilize numbering for revisions once an approved version has been released.

PROPOSAL

Contents

Table of Clauses

1 Preface (Informative)

1.1 Goals

1.1.1 This standard is intended to help ensure that an acceptably thorough consideration of safety for an autonomous product has been performed during the design process and will continue to be done throughout the system lifecycle. It does so by emphasizing repeatable assessment of the thoroughness of a safety case.

1.1.2 The developer is responsible for a safe outcome when deploying the autonomous product under consideration. Assessment according to this standard is intended to support this by providing a check and balance mechanism for the safety related aspects of development, support, and lifecycle operation.

1.2 Approach

1.2.1 Autonomous systems promise to provide unprecedented capabilities in a number of domains, including self-driving passenger cars and cargo delivery robots. However, some common aspects of autonomous technology such as use of machine learning and nondeterministic algorithms present novel challenges for safety assurance. An additional challenge to safety standardization is providing flexibility that might be required by a quickly evolving technology while still providing a long-lived framework for safety assurance.

1.2.2 The approach taken in this standard (UL 4600) is to require a goal-based safety case that encompasses essentially the entirety of the material necessary for safety assurance. The safety case includes a structured set of goals, argument, and evidence supporting the proposition that the item is acceptably safe for deployment. In support of that goal, UL 4600 assessments emphasize ensuring that the safety case is reasonably complete and well formed. In particular, UL 4600 provides guidance to improve consistency and completeness of the safety case. To this end, some best-practice process activities and granular work products are specifically required (e.g., creation of a hazard list). However, no specific overall design process is mandated, nor are there mandates for specific methods used to create the majority of work products (e.g., a V-style development process is not required; any reasonable approach used to create a list of hazards can be acceptable). In keeping with this approach, the order of the sections in this standard do not imply a set of process steps. Rather, sections are grouped by topics and characteristics that should be considered when assessing the completeness and validity of the safety case.

1.2.3 For the purposes of this standard, an autonomous system along with its operational and lifecycle support (collectively, the “item” being assessed) is one that operates in a defined Operational Design Domain without requirement or expectation of human intervention in operational behavior. An example is a passenger-capable vehicle operating on public roads for

which neither the passengers (if any) nor any remote operator is expected to monitor vehicle behavior for safety. A lack of human operator supervision (e.g., no human having or sharing responsibility for safe performance of the dynamic driving task) has pervasive implications on safety compared to human supervised items, especially in the area of managing violations of environmental and operational design limitations. It is important to note that humans are likely to assume responsibility for some safety related lifecycle and infrastructure areas, such as managing risk mitigation for novel hazards and performing required maintenance.

1.2.4 Verification and validation of an autonomous item involves more than simply testing its responses in typical situations to see how they compare with human operator performance. An autonomous item's behavior might be different than (but compatible with) human operator behaviors and might need to deal with situations a human operator would not normally experience. Moreover, there might be an expectation that an autonomous item successfully handles a wide variety of exceptional or unusual situations beyond the normal expectations of human operator proficiency. In many autonomous items there will be an expectation of continual item evolution in response to changing operational conditions, discovered latent operational requirements, and discovered hazards. Additionally, autonomous systems often incorporate intentionally non-deterministic behavior, use of inductive learning technology, heuristics, and other technical approaches beyond the scope of some conventional safety design approaches. As a result, it can be expected that while ensuring the safety of such items can build upon conventional safety design approaches, some significant changes in strategy are likely to be required at the item safety level as described in the next section.

1.2.5 This standard does NOT define a process, but rather puts forth assessment criteria to determine the acceptability of a safety case. As such, the ordering of sections, clauses, and prompt elements does NOT imply temporal ordering or other process path dependencies.

1.2.6 **NOTE:** This standard generally uses the term "item" rather than "system" or "product" when referring to the scope of the safety case as well as the operation of the item. This approach is in recognition of the possibility that the safety of the item might rely upon infrastructure, services, support processes, and other factors that might not normally be considered part of a system such as a vehicle per se, but which materially affect its safety and therefore are all considered within the scope of the item being assessed for conformance.

1.3 Key principles

1.3.1 A set of key principles underlie the approach:

(1) Define minimum acceptance criteria for the safety case. The standard does not specify how a design must be created, but rather describes a minimum set of topics to be considered in creating and assessing the safety case. In the same vein, a threshold for determining what is acceptably safe is not defined. Rather, the requirement is for the safety case to define safety acceptance criteria with respect to a defined operational

design domain, argue their sufficiency, and argue that the item actually meets these criteria.

(2) Use feedback. While due care is required before deploying an item, the novelty and fast evolution of autonomy technology might require the use of feedback loops to attain practical safety. Feedback is required for a number of purposes, including: validating assumptions made during the design process, detecting changes in the operational environment, detecting issues with the item's capabilities, detecting issues with the item design, detecting issues with the safety case, detecting issues with the application of this standard to the item, collecting lessons learned, and detecting issues with this standard itself. Ensuring that these feedback paths exist and are effective is specifically addressed by the standard.

(3) Provide prompts. The general format of the standard is a set of high-level clauses in which each clause is supported by a set of prompts. The prompts are topics to consider in when determining whether the safety case is acceptable in terms of meeting the intended scope and purpose of the clause. These prompts in aggregate act as a repository for collective knowledge and "lessons learned" including both things to consider and Pitfalls that can be encountered when using a potentially risky technique or approach. Many of the prompts have to do with potential hazards that must be considered. The prompt lists have been seeded based on experience, lessons learned, and standards content. Sources include traditional automotive functional safety, aerospace safety, military item safety, chemical process safety, and other domains. While traceability to individual prompts is generally included in the safety case (in accordance with a set of rules governing argument rigor), in many cases the response to a prompt can be "does not apply" or acceptance of a risk that is argued to be insubstantial. Thus, tailoring of the application of the standard is accomplished not by excluding some of the standard's clauses from consideration without explanation, but rather by recording an argument that specific prompts do not require further action in support of a safety case deviation.

(4) Repeatable assessments. Assessment of each clause in the standard starts with an examination of the portion of the safety case that traces to that clause. (Other elements of assessment can be identified as well, depending upon the clause.) The goal is to assess whether the safety case is substantially complete and well-formed. The developers have a responsibility to interpret and apply data in light of their knowledge of the technical details of the system. Self-auditors have a responsibility to ensure that the safety case is complete and well formed, as well as ensure that the technical content is reasonable. Self-auditors do not have an independence requirement. However, in return, there is a presumption that self-auditors are familiar enough with the technical details of the item to make informed decisions as to safety case technical validity. In contrast, independent assessors are not responsible for authoritatively interpreting technical data or finding technical defects in the item. However, independent assessors are tasked with ensuring that the self-auditors have not let slip defects with the form and coverage of the safety case. Thus, the emphasis of independent assessors is upon ensuring that the

prompts regarding each clause have been addressed by the safety case in an apparently reasonable way. The basis of judgement for independent assessors is primarily completeness and consistency of the safety case in light of the clauses and prompt elements of this standard, which is intended to provide reasonably repeatable, objective independent assessment results. Ultimately the item design team is responsible for safety, but a repeatable assessment process helps with consistency of execution and should reduce the number of surprises resulting from safety assessments. See Section 17 for more information on assessment.

(5) Embrace uncertainty. The combination of likely nondeterministic item behaviors, possibility of exceptional operational environments, continual change of the real world environment, and typical use of inductive learning approaches to developing autonomous item features means that uncertainty regarding item behavior is to be expected. (Not all of these characteristics necessarily apply to all items.) Rather than adopt a strategy in which any “unknown unknown” that presents non-trivial risk is viewed as a potential item defect that is presumed to be found before initial product release, unknowns are instead considered a normal aspect of the item design and lifecycle. Discovery of unknowns (informally, “surprises”) are explicitly managed using feedback strategies. This is not to say that deployed items should be excessively risky, but rather simply this acknowledges the reality that the degree of risk when deploying is itself uncertain to some degree. Moreover, the perceived risk changes in response to newly discovered hazards, environmental changes, and newly created risk mitigation measures during the lifecycle. Therefore, managing unknowns that will inevitably manifest during deployment should be proactive rather than reactive. Pervasive feedback results in a change of perspective for release criteria compared to traditional safety approaches. Rather than a presumption that an item is safe enough for indefinite use unchanged when released, instead the strategy is that the item is reasonably believed to be safe enough to begin a process of continual feedback and improvement in the face of potential surprises and a changing operational environment. This approach is consistent with a continual update strategy. It also permits gathering additional evidence to strengthen the safety case in response to new knowledge and changing conditions via making adjustments informed by field experience.

1.4 Key approaches

1.4.1 Creating a safety standard inevitably requires a number of decisions with regard to key concepts and choice of approaches. Some salient decisions and strategies are discussed in the following subsections.

1.4.2 **Item-level risk target.** The risk target value after all mitigations have applied at the item level must be defined in the safety case. However, a specific target value is not mandated, nor is a particular methodology specified for setting such a target value (see Section 6.4.3).

1.4.3 **Integrity levels.** This standard requires the use of at least two integrity levels (at least one level one for substantively life critical severity, and at least a second level for lower severity risks). Flexibility is provided and permits the use of any reasonable SIL, ASIL, DAL, or similar approach, with developers encouraged to use an accepted functional safety standard relevant to the application domain (see Section 6.4). Correspondingly, any failure rate targets are defined in conjunction with the definition of the integrity level approach documented within the safety case rather than within this standard (see Section 16.2).

1.4.4 **Process model.** There is no requirement for a traditional “V” style process model found in many other safety standards. However, the process model must be defined and must directly or indirectly include a set of best practice item engineering activities performed with suitable engineering rigor and quality monitoring. (See Section 9.)

1.4.5 **Independent assessment.** A lack of independent checks and balances brings with it an elevated risk of adverse safety outcomes. On the other hand, strictly requiring external assessment is not a panacea in practice. Moreover, it is unlikely that completely independent assessors can find all potential safety problems since they are not intimately aware of the details of a particular item design. The approach taken by this standard is to require two layers of assessment. The first layer is a self-audit that can be done collaboratively with the design team to ensure that the safety case is well formed and credible while including input from experts in the item’s design, implementation, and other factors. The second layer is an independent assessment that essentially checks the work of the self-audit process employing a reasonable degree of both technical and safety case construction competence for this independent check. The independence and competence of the independent assessors must be argued and included as part of the independent assessment report. (See Section 17.3.)

1.4.6 **Assessment consistency.** The role of independent assessors is not to find specific technical defects in the design; that is the job of the developers and the self-audit process. Rather, independent assessors primarily consider whether the safety case is well formed and reasonably complete after the self-audit process has been performed. This is intended to increase consistency between a rigorously performed self-audit and independent assessment outcomes. The inclusion of numerous prompt elements for the safety case makes the question about whether particular aspects of operation, argument epistemic defeaters, and other items are expected in the safety case more objective to the degree it can be made responsive to the lists. This approach still provides and independent checks and balances without as much reliance upon variable assessor experience and subjective assessor judgement. As part of this approach, it is essential that prompt element lists be robust and be updated over time in response to lessons learned. In return for a reduced expectation of external assessor discovery of significant system defects, developers and self-auditors assume an increased responsibility for safety. If a system is unsafe, that outcome is primarily the responsibility of the developers, not the independent assessor.

(There is nothing preventing developers from obtaining external advice on safety approaches and technical specifics. However, providing that advice is not a burden placed upon the independent assessor by this standard.)

1.4.7 **Incremental change assessment.** It is expected that item updates might be made many times during the system lifecycle as a result of the operation of feedback loops and as the result of operational environment changes. A balance is required between ensuring that assessment is done to ensure changes do not compromise safety versus making it impractical to perform rapid deployment of important changes that improve safety and security. The standard uses a multi-tiered approach. Rather than create an arbitrary technical metric cutoff point for “small” vs. “large” changes that might not actually correspond to the effects of a change upon item-level risk, each change is subject to impact analysis with increased level of scrutiny triggered in response to larger impact from one change or an accumulated set of changes. “Small” changes require an analysis to update and ensure the validity of the safety case using a self-audit process responsive to impact analysis. When changes have a significant potential impact on safety, they additionally require independent assessment. Independent assessment is also performed periodically to address accumulations of small changes to both the item and its operational environment. An essential point is that every system instance can trace its claim to safety to a valid safety case at every point at time that it is operating throughout its entire lifecycle.

1.4.8 **Simulation vs. Testing.** Autonomous item complexity is such that relying upon simulation results in arguing safety is typically a practical necessity. Simulation results can be used so long as their accuracy is justified, simulation run coverage is justified, and an appropriate non-zero amount of physical testing is used to validate simulation results (e.g., Section 12.2.1.)

1.4.9 **Tailoring.** Different items will have different characteristics and needs. However, even if some aspect of the standard is not applicable it must actually be argued that this is the case, however simple the argument. Tailoring is done responsive to a set of argument rigor levels defined for each standard requirement. MANDATORY prompt elements must be addressed for every item somewhere in the safety case without exception. REQUIRED prompt elements must be addressed, but can be stated to be not applicable if there is a compelling case made that it is inherently inapplicable (e.g., a required prompt element applies to a technology that is not used anywhere in the item). HIGHLY RECOMMENDED prompt elements are optional, but a non-trivial reason must be stated if they are waived, and that reason should be technically substantive. RECOMMENDED prompt elements can be included or disregarded with no comment in the safety case, and are present simply as completely optional suggestions. Thus, tailoring is not performed by eliminating portions of the standard from consideration, but rather by the degree to which prompt elements are either addressed or justified in the safety case as being not applicable. It is important to note that the tailoring is not coupled to integrity level assignments, but rather is performed within the safety case within the tailoring constraints just discussed. In other words, this tailoring is a generally orthogonal concept to criticality. (In

practice there is likely to be some coupling to the degree that integrity level approaches affect which specific prompt elements have deviations justified by a reference to functional safety standard integrity-based requirements. However, this is likely to be true for only a small fraction of prompt elements and is not the primary role of UL 4600 tailoring just described.)

1.4.10 **Component safety cases.** An interface mechanism is provided for partitioning the assessment of components. Components include both hardware and software System Elements out of Context (SEooC). A design-by-contract style approach is used in which a SEooC safety case interface contains a set of claimed component properties, a set of assumptions that must be true for those properties to hold, and a fault model considered in the assessment of the validity of the component claims. Items which are SEooCs create a safety case that exports this interface. Complete product-level safety cases can then use a SEooC assessment result as evidence so long as the product-level safety case shows that the SEooC assessment remains valid in the context of the product. (See Section 5.7.) SEooC interfaces can be nested into sub-components as needed. An essential point is that every component included in a system instance can trace its claim to safety to a valid safety case at every instant that it is operating throughout its entire lifecycle, including valid SEooC safety cases. Components can export the obligation to cover clauses and prompt elements, including MANDATORY prompt elements, to their overarching safety cases.

1.4.11 **Role of humans.** This standard primarily covers fully autonomous item operation with no human expected to monitor or ensure item operational safety in real time. However, humans are potentially passengers, present in the operational environment, involved in lifecycle operations, and relevant to many aspects of safety case arguments. Therefore, human interfaces and human interactions are covered as factors that must be considered by the safety case. Safe transition to and from operational modes that involve human control is also in scope. However, human operator ability to safety supervise or control the item (e.g., factors affecting human attention lapses and ability to assume control in a given situation) are out of scope, as are details of arguing satisfactory human performance of assumptions and obligations related to them in the safety case. (See Section 7.)

1.4.12 **Autonomy.** Autonomous item operation is in scope, including issues relating to non-deterministic behavior and items designed using inductive training (“learning”) approaches. (See Section 8.)

1.4.13 **Updates.** This standard is intended to be updated on a regular basis (e.g., under UL’s continuous maintenance process). It is recognized that frequent updates can impose a burden on users of the standard. Change control procedures for the standard are intended to account for a balance between the need for updates and the need for timely feedback loop execution. The section numbering structure (including the use of Not Applicable (N/A) subsections) is intended to minimize the need for renumbering across versions.

1.4.14 **Cyber Security.** The specifics of security are out of scope for this standard. However, a security plan is required in general, and areas in which security issues can particularly affect safety are noted. (See Section 10.8.)

1.4.15 **Terminology.** Terms essential to repeatable assessment according to this standard (e.g., related to safety case construction) are defined. (See Sections 4.1 and 4.2.) Other terms are intended to be interpreted in a way that corresponds to general use by practitioners. If there is doubt as to interpretation, the safety case can define specific terms in a way that is compatible with providing acceptable product safety.

1.4.16 **Other topics.** Also included in scope are: risk assessment; development processes; verification, validation & test; dependability; data and networking; tool qualification; off-the-shelf, third party, and legacy components; lifecycle concerns; maintenance and inspection; and metrics.

1.5 Use of this standard with other standards

1.5.1 Historically, many safety standards have addressed functional safety (e.g., IEC 61508, ISO 26262). Some standards have gone beyond functional safety to deal with gaps in requirements and exceptional operational environments (e.g., for the automotive domain, ISO/PAS 21448, which deals with Safety of the Intended Function: SOTIF). Some standards have treated system level safety in a prescriptive manner. However, complete removal of humans from performing aspects (including supervision) of autonomous item operation brings with it numerous additional concerns. This standard is intended to work with existing standards to provide the additional elements necessary to assure that safety aspects of fully autonomous item operation have been considered in a comprehensive manner when creating a safety case.

1.5.2 To the maximum extent practicable, it is intended that developers can take advantage of effort expended and assessment credit gained for conformance to other standards. Developers may incorporate materials into their safety case generated as a result of executing processes and generating work products required by other standards.

1.5.3 It is envisioned that the use of this standard with other standards will occur in the following manner. (To be clear, this is an informative, not normative, characterization of one potential process.) A high-level safety case and item architectural approach are created. Appropriate functional and other safety standards and/or practices are selected and applied to generate work products. Those work products are used to populate the safety case. It is likely that revisions and iterations will be required based on safety case analysis. It is also likely that tool support will be highly desirable to support traceability and safety case structural analysis. Eventually the process converges to create a well formed, complete safety case that passes first a self-audit, and then an independent assessment. A state of completeness can be claimed via addition of arguments that there are plans for detecting and addressing “unknowns” as they

emerge during at-scale operation. There must be a credible argument that the net risk from the manifestation of incidents from those unknowns will be acceptable when considering field engineering feedback responses. Once operations begin, a continual stream of revisions and changes occurs, accompanied by self-audit and independent assessment activities responsive to the impact of each change. Eventually all the deployed items are retired with accompanying cessation of feedback monitoring. Sequencing and overlap of these described activities are flexible, and no particular design methodology is implied by this description.

1.5.4 It is the intent of this standard to be compatible with existing relevant safety standards to the maximum extent practicable, and in particular avoid prohibiting any activity or approach that is required by those standards. In particular, compatibility with ISO 26262:2018 and ISO/PAS 21448:2019 has been considered. Annex A discusses a mapping of some clauses of this standard onto ISO 26262:2018 and ISO/PAS 21448:2019. Other safety standards such as IEC 61508 are relevant and expected to be generally compatible, but detailed analysis of IEC 61508 and other functional safety standards is out of scope for this version of UL 4600.

1.5.5 While a degree of topical overlap between this standard and other standards will be apparent, this is actually an essential feature rather than undesirable duplication. Functional safety and design methodology standards typically provide guidance on how to perform engineering activities. Typically they provide strong guidance on process and methods, but rely upon developer and assessor expertise and experience to make sure analysis results, reviews, and other activities are performed in an acceptably thorough manner. (As an example, a list of hazards can be rigorously developed using a particular method. However, there might be a hazard that one organization has on its list that is not on the list of another organization building a similar item. In the absence of collaboration or standardized end application hazard lists, this type of mismatch of hazard lists is especially likely to occur in novel application areas due to differences between experiences of individuals in the two organizations and their assessors.) Moreover, variation across both developers and assessors can provide uneven results and varied assessment rigor and, in the worst case, loss events that for another organization/assessor pair were both foreseeable and reasonably avoidable.

1.5.6 Even assuming perfect developer and assessor capability when executing any particular standard, creating safe autonomous products requires collecting together potentially many such standards as well as an accumulation of best practices that are not yet standardized. Moreover, best practice design and validation activities can change fairly rapidly over time as novel technology matures. Thus, while use of existing functional safety standards is highly desirable, it is likely that there will be gaps between successful conformance to those standards and the creation of an acceptable safety case for complex autonomous items.

1.5.7 This standard is intended to supplement rather than supersede traditional functional safety and SOTIF standards. The main goal of UL 4600 is to make sure that the cumulative work products produced as a consequence of following other standards and other best practices do

not leave any holes that present an unreasonable risk to autonomous product safety. Therefore, one approach to conformance to UL 4600 is to conform to functional safety standards and other design guidance to achieve maximum coverage of the scope of this standard, filling in any remaining holes with best practices and other approaches as required. If the engineering activities defined in other standards plus collected practices provides less than 100% coverage of the relevant safety case contents needed to conform to this standard, that means something is missing that is required for a credible safety case. In practice it is likely that the approach taken when conforming to other standards may need to adjust to ensure that work products meet the requirements of UL 4600, even though that might go beyond the strict minimum requirements of other standards.

1.5.8 To the degree that the safety case relies upon an assessment according to any other safety standard, or otherwise takes credit for a separate evaluative process, acceptable evidence supporting the validity of that separate evaluative process it is necessary. Reliance upon other assessments can, for example, include an assessment report from an independent, qualified third-party assessor stating that the properties taken credit for in the safety case are true. However, if the separate evaluative process has not been performed with at least the rigor specified by this standard (UL 4600), additional evaluation within the scope of the safety case is necessary.

1.5.9 Two areas out of scope for this standard are setting acceptable risk levels and setting forth requirements for ethical product release decisions and any ethical aspects of product behavior. For both topics the developer records what decisions have been made, but this standard does not establish acceptance criteria beyond that they have been recorded. Other standards such as the IEEE P7000 series provide guidance on those topics.

1.6 Automotive vs. other application domains

1.6.1 The scope of this standard is to a generalized autonomous item standard framework using light autonomous road vehicles (e.g., ones for which ISO 26262 is applicable) as a concrete example. To that end, this version of the standard includes extensive prompt lists applicable to light autonomous road vehicles (both passenger and cargo vehicles). Many of the prompts will apply to other autonomous ground vehicles and even other types of autonomous items, but no specific attempt has been made to include extensive prompts for other applications, nor to segregate road vehicle prompts from more general prompts.

1.6.2 This standard can potentially be applied to a variety of other types of items by establishing an end product profile that specifies some or all of the following:

a) List prompt elements that are presumptively inapplicable. This amounts to defining an alternate ODD profile compatible with the product use.
   EXAMPLE: traffic flow control signal interpretation for an off-road application.

b) Identify any analogous requirements for inapplicable prompts.
EXAMPLE: warehouse infrastructure signal recognition for a warehouse robot application is added to ODD prompt element lists.
c) Identify new domain-specific prompts for the intended application.
EXAMPLE: Hazards associated with misaligning a robot with automated cargo transfer mechanisms

1.6.3 Additionally, for applications including automotive an end product standard might need to additionally address other aspects of safety such as fire safety and high voltage electrical safety.

1.6.4 Even in the lack of an end product standard for other applications, a similar tailoring approach can be followed within a safety case via exercising the option to declare REQUIRED and HIGHLY RECOMMENDED prompt elements inapplicable for other domains while adding additional prompt elements that might be applicable.

2 Scope

2.1 Scope summary

2.1.1 This standard covers the safety principles, risk mitigation, tools, techniques, and lifecycle processes for building and evaluating a safety argument for vehicles that can operate in an autonomous mode.

2.1.2 Operation is assumed to occur without human supervision and without expectation of human intervention in performing the dynamic driving task and other normal system operations based upon the current item state and ability to sense and otherwise interpret the operating environment. Human contributions to safety in other than normal operation are considered (e.g., maintenance), as are interactions with humans who are not operating the item (e.g., pedestrians).

2.1.3 This standard assumes that the item autonomously operates starting at some well-defined initial state to some other well-defined end state without human intervention. Human input might influence the selection of desirable states (e.g., via a passenger requesting a destination). However, the extent to which human operators mitigate or introduce risk by performing or supervising a dynamic control task (e.g., by driving or taking responsibility for monitoring system operation) is outside the scope of the standard. Similarly, the extent to which human operator performance or non-performance is involved in risks related to transferring human driver control to or from the item is also outside the scope of the standard. However, ensuring that the item itself properly performs any change of control functions if and when it is supposed to is generally within the scope of the standard since it can adversely affect operation in fully autonomous mode as well. Thus, while portions of this standard might be helpful for addressing less than fully autonomous vehicles, issues involving human driver responsibilities, vigilance, and ability to properly accept responsibility for vehicle control are out of scope for this standard.

2.1.4 While information security is an essential topic, the details of that area are out of scope for this standard beyond a general requirement for a Security Plan and prompt elements that are possibly unique to autonomous vehicle operation in comparison to other vehicular security requirements. Reasonably foreseeable misuse and abuse as well as physical attacks (e.g., physical sensor damage) are in scope.

2.1.5 The requirements of this standard are considered a minimum appropriate level of completeness and rigor necessary to create an acceptably well-formed and acceptably complete item safety case. In particular, prompt element lists are considered non-exhaustive, with an expectation that design teams will include additional items as relevant to the item and its operational design domain.

2.2 Elements in scope

2.2.1 Specific aspects of item operation and safety related issues which are explicitly intended to be in scope for this standard include:

a) Operation of autonomous items in potentially unstructured environments
EXAMPLE: A vehicle is the first vehicle directed into an open farm field containing a mixture of viable and non-viable areas for traversal and parking as part of an ad hoc overflow event parking process. There are no lane markings and no positioning beacons. Moreover, there are cows and hay bales randomly placed in the field. There are no humans assisting with organizing vehicle parking positions. This situation is in scope for the standard.
EXAMPLE: A crowd has spilled into the street at a fire scene. Emergency response equipment, response personnel, victims, and casual observers are moving without regard to normal road use patterns. Fire hoses, falling pieces of burning debris, small explosions, traffic signal power outages, damaged pavement, and other disruptions to normal infrastructure expectations exist. Multiple injured people at building exits are calling for pickup by autonomous vehicle ride hail services to be transported to urgent care medical facilities. This situation is in scope for the standard.
NOTE: A particular item's safety case might require a structured environment for safe operation as specified by an ODD description. However, structure is not assumed to be present by default. Therefore, operation in unstructured environments must be specifically disclaimed by the safety case if applicable.

b) Operation with potentially inaccurate, incorrect, incomplete, or misleading sensor inputs

c) The effects of potentially inaccurate, incorrect, incomplete, or biased data, including test data, field report data, other validation data and machine learning training data.

d) Potential defects and failures of hardware and/or software in the item, data collection functions, data processing functions, communications, engineering support systems, tools, and infrastructure support.

e) Human contributions to potential risk, including passengers, pedestrians, other road users, non-road users, cargo handlers, maintainers and inspectors. This includes acts of omission and commission; accidental and malicious physical acts; and human roles in creating as well as mitigating risk.

f) Lifecycle considerations, including design data collection, engineering data management, tool qualification, design, implementation, testing, other validation, field data collection, operations, maintenance, updates, upgrades, and retirement. Lifecycle considerations also encompass potential changes to the environment which may affect ODDs and OEDRs.

g) Inclusion of risk mitigation and other aspects of contributions to the safety case made by conformance with other standards, and in particular both ISO 26262 and ISO/PAS 21448 standards for products within scope for those standards.

h) Ability to use a heterogeneous approach to arguments, including use of diverse standards to support safety (e.g., use of different but acceptable functional safety standards for different item subsystems).

2.2.2 None of the described of in-scope topics is intended to require that the item successfully delivers full service in all situations described. Rather, the requirement is to consider all prompt elements and argue that risk is acceptable despite these factors. In many cases that will involve crafting an ODD that excludes problematic prompt elements. However, excluding a prompt element from the ODD (or similar approach) creates an obligation to argue that the exclusion does not itself result in unacceptable risk.

2.2.3 **EXAMPLE:** Unpaved roads without lane markings are excluded from the ODD. The safety case generally argues that geo-fencing and map creation will exclude all unpaved roads. It is further argued that this exclusion encompasses quickly identifying roads undergoing repaving projects that are temporarily unpaved but still carrying traffic.

2.2.4 **EXAMPLE:** Snow is excluded from the ODD. Snow is still part of the safety case to cover un-forecast snow that occurs during an operational mission. The safety case generally argues that it can successfully terminate a mission via in-lane stop despite snow. It further argues (with evidence) that snow will happen so infrequently in the deployment location that the elevated product risk presented by occasional in-lane stops is acceptable.

2.3 Scope limitations

2.3.1 A significant scope limitation of this standard is that it does not cover the detailed topics relevant to ensuring that that humans are able to provide effective safety supervision for an autonomous item. Rather, coverage is limited to fully autonomous operation with no human supervision as well as aspects of the item during human supervised operation that do not relate to arguing human supervision effectiveness. Similarly, aspects of the ability of a human operator to safely control the item are out of scope. More specifically, the following are explicitly intended to be out of scope for this standard:

a) Aspects of items as well as item-level safety of operational modes for which the locus of control is outside the item itself
EXAMPLES: End-to-end system-level safety (including the human supervisor or driver) of teleoperated modes of operation is excluded to the degree it relies upon a human teleoperator to control, supervise, or otherwise ensure system safety.
NOTE: A product-level “item” is intended to include offboard functions that participate in control of a vehicle, such as a cloud-based route planning system.
NOTE: The proper response to teleoperated commands and proper transmission of teleoperation data out of the vehicle is in scope. However, whether teleoperation is actually safe at a system level is out of scope due to human involvement in the driving task.

b) Human factors related to safety during or after a handoff or mode switch that makes a human responsible for the dynamic control task safety.
EXAMPLE: The details of ensuring that a human supervisor is available and able to safely take over item operation upon request and continue to operate the vehicle safely when some or all autonomy functions are disabled are out of scope.
c) Risk mitigation or other safety argument credit taken for the contribution of humans to the dynamic driving task (e.g., human driver, human safety supervisor, human teleoperator, issues of human alertness, issues of human situational awareness).
EXAMPLE: The details of how safe and effective human/machine interfaces should be provided to teleoperators are out of scope.
d) Road testing of prototype vehicles to the degree that safety argument takes credit for a human performing and/or supervising the dynamic driving task.
e) Specifics regarding the ability of humans to acceptably meet expectations for non-driving roles in item safety. To be clear, identifying the human contribution to the safety case (e.g., via performing inspections, or a human's ability to correctly perceive and interpret signals provided by the item) is in scope. However, specifying the details of how to actually ensure that the contribution is being done in an acceptable manner in terms of human behaviors, psychology, limitations, and so on is out of scope. While competency frameworks, staff skill lists, and experience requirements are potentially helpful topics to cover a safety case, specifics regarding these topics are out of scope for this standard.
f) Evaluation of the suitability and effectiveness of human interface devices. To be clear, the need to identify such devices and the need to ensure suitability and effectiveness is in scope, but specifying requirements for how to meet that need is out of scope.

2.3.2 **EXAMPLE:** A car in autonomous operation is not supposed to transfer vehicle control to an occupant under any circumstance during a mission. It does in fact attempt to transfer vehicle control to an occupant, providing three seconds of warning.

In Scope for UL 4600: Incorrectly attempting to transfer control in violation of fully autonomous operational mode.

Out of Scope for UL 4600: Whether three seconds is enough warning for effective handoff. Whether occupant is a qualified driver.

2.3.3 **EXAMPLE:** An autonomous car is designed to transfer control to a qualified human driver under some circumstances with a 10 second warning, and the driver is both competent and aware of this handoff mission parameter.

In Scope for UL 4600: Transferring control without the full 10 seconds of warning. A defectively designed brake control mechanism that under some circumstances prevents the human driver from actually regaining control at the designated time (e.g., human driver's brake pedal disabled despite having attempted to perform a handoff). Whether brake pedal actuation by a human is intended to initiate a handoff under specified conditions.

Out of Scope for UL 4600: Whether ten seconds is enough warning for effective handoff in any particular handoff situation. Whether depression of a brake pedal by a human driver is a

safe (from human factors point of view) handoff initiation mechanism. Checking whether occupant is a qualified driver. Checking whether the driver has sufficient cognitive ability for safe operation. Checking whether human driver is in correct seating position to assume operational control. Safety of vehicle once control has been transferred to the human driver. Effectiveness of Advanced Driver Assistance (ADAS) functions in mitigating risk while under human driver control.

2.3.4 There a number of additional topics out of scope. Reference to these topics should be made where relevant to the safety case, but specifics such as prompt elements to provide technical depth are not included in this standard:

a) The specific intended function (e.g. surface cleaning, fragile cargo delivery)
   NOTE: This topic might be covered by an end product standard.
b) End product requirements
   NOTE: It is intended that end product standards can reference or require this standard.
c) Legal and policy issues
   EXAMPLES: Determining liability, what records retention policies are appropriate, what level or product risk is actually acceptable to society.
d) Ethical issues
   EXAMPLES: Resolving questions of acceptable risk, evaluating comparative severity of different loss event scenarios
e) Electric Vehicle safety
   EXAMPLES: Safe battery design, safe battery management algorithms, battery thermal management
f) General vehicle safety
   EXAMPLES: Crash mitigation, passenger restraints, refueling/recharging safety
g) Non-safety related quality aspects of performing the intended function
   EXAMPLES: Ride quality, fuel economy
h) Effectiveness of crash and injury mitigation mechanisms
   EXAMPLES: Seat belts, air bags, child seats

2.3.5 Also out of scope for the standard is any implied redefinition of existing standards and accepted practices to the degree that they are acceptable to support the safety case being made. Reference to these topics should be made where relevant to the safety case, but specifics are not included in this standard. These topics include:

a) Government regulations
   EXAMPLES: FMVSS, Federal Communications Commission radio frequency interference emission certification
b) Mechanical aspects of the item
   EXAMPLES: Sharp edges, pinch points, window lift motor closing pressure limits
c) Legacy operational procedures
   EXAMPLES: Car door operation, child locks on car doors, cargo loading and loading

d) Specifics of vehicle support for other than normal operations (except to the degree that the autonomy is expected to provide such support and that such provision is safety related)
   EXAMPLES: Autonomy support for non-safety related routine maintenance procedures in situations which do not present a hazard
e) Sufficiency and performance of controls and item response when a human is operating or supervising the dynamic driving task
   EXAMPLE: As required by FMVSS
f) Licensing, training, qualification and other aspects of ensuring human competence to operate or participate in the vehicle lifecycle
   NOTE: Credit can be taken for these in the safety case only to the degree that any standard or procedure conferring or documenting qualification provides objective evidence of abilities

3 Referenced Publications – WORK IN PROGRESS

3.1 Normative references

3.1.1 Any undated reference to a code or standard appearing in the requirements of this standard shall be interpreted as referring to the latest edition of that code or standard.

3.1.2 The following normative references are included in this standard:

Normative reference list: TBD

(typically categorizes references by publishing organization)

3.2 Informative references

3.2 Informative references

TBD

3.2.1 Refer to Annex ____ for a listing of supplemental standards.

TBD

4 Terms, Definitions, and Document Usage

4.1 How to interpret normative elements (Normative)

4.1.1 Commonly used constructions of this standard affect the safety case as follows. All elements are normative except “EXAMPLE,” and “REFERENCE” statements as well as any other content that is explicitly stated to be informative. (See Table 4.1 below for a summary of key safety case deviation explanations.)

a) **Numbered clauses** (starting at 5.1.1) are generally stated as “shall” conformance obligations. These are intended to be general statements, with supporting normative prompt elements providing further detail. Each clause is specifically addressed in the safety case with the exception of conformance assessment process clauses in Section 17 that deal with activities performed upon the safety case itself. An important part of navigability of the safety case is a capability to identify the portion(s) of the safety case that support fulfillment of each clause. The scope of all clauses is the safety related portion of the item unless otherwise stated.

b) **MANDATORY prompt elements:** Addressed by the safety case. Safety case deviations not permitted. Any safety case deviation results in a non-conformance.
EXAMPLE: “Identify hazards” is mandatory – it must be done.
EXAMPLE: A team attempts to argue that MANDATORY prompt element X does not apply to their item. This is an invalid attempt at a safety case deviation.
NOTE: In some cases, a MANDATORY prompt element refers to consideration of a different clause in a hierarchical manner. That should be interpreted as a mandatory inclusion of the associated higher-level goal in a safety argument, but not mandatory inclusion of all the non-mandatory prompt elements of the clause being referred to. In particular, such hierarchical references are not intended to override the safety case deviation rules.
EXAMPLE: MANDATORY prompt element X states that section Y is addressed by the safety case. Section Y has a HIGHLY RECOMMENDED prompt element Z. The net requirement is that satisfaction all clauses in Section Y must be addressed by the safety case, but a safety case deviation of prompt element Z is still permitted in accordance with its HIGHLY RECOMMENDED categorization.

c) **REQUIRED prompt elements:** Addressed by the safety case. Safety case deviation is permitted only if documented by argument that the prompt element is intrinsically incompatible with the item and/or its safety case. Support for each safety case deviation is explicitly noted in the safety case. End product standards can enumerate REQUIRED elements that can be omitted from the safety case (i.e., blanket default safety case deviations specified by an end product standard). The safety case is non-conformant if safety case deviations are not acceptably documented for REQUIRED elements. Safety case deviation for a reason other than intrinsic inapplicability results in a non-conformance. Field engineering feedback and change impact analysis are used to detect the possibility of a claim of intrinsic

incompatibility becoming invalid. Examples of acceptable safety case deviations include:

EXAMPLE: Safety case deviation for requirements on machine learning if item does not use machine learning-based techniques in any manner, including design, operation, and field operational data analysis.

EXAMPLE: Safety case deviation from recognizing road signs if item does not rely upon road signs in any safety related way. Arguments supporting this might be that the ODD specifically excludes road signs, or that the item exclusively uses a means other than road signs to gather equivalent information.

EXAMPLE: Safety case deviation from requirements specific to subdivision of an ODD into multiple ODD subsets if the item does not define ODD subsets (i.e., if an item uses a single monolithic ODD, then any requirement related to ODD subsets is not applicable).

EXAMPLE: Data does not yet exist because a potential event or condition has never occurred in the life of the item. An example would be records of correction of defects discovered during item operations if no items have yet been deployed. However, safety case deviation is not permitted for the mechanisms and procedures to collect and process such potential events – just the portions of the safety case contents that cannot exist until field events occur. It is a good practice to include clearly designated placeholder examples to populate empty data sets so as to exercise tools, procedures, and traceability.

d) **HIGHLY RECOMMENDED prompt elements:** These are best practices that should be followed, but may be omitted, especially for low risk items. Omissions are explicitly noted in the safety case with reasonable supporting argument to provide a hook for tracing root cause analysis back to those omissions. The safety case is considered well-formed so long as these omissions are simply noted with a rationale. In cases in which a generic prompt element of “others” is included, an omission rationale of “no others” is acceptable. A primary purpose of field engineering feedback is to ensure that a safety case deviation of any prompt element that contributes substantively to safety related issues is identified and the deviation revoked.

EXAMPLE: The use of a specific analysis technique is HIGHLY RECOMMENDED. The safety case notes that the technique was not used with a rationale of “other analysis techniques being used provide comparable information.” The safety case includes an argument that there is no history of incidents with an unknown root cause that could plausibly have been prevented via addition of this technique to the design approach. This argument is backed up by root cause analysis logs showing all root causes have been resolved, leaving no unresolved candidates that might in fact trace to the prompt element deviation. In the absence of other adverse information.

EXAMPLE: The rationale for a HIGHLY RECOMMENDED prompt element deviation is “Safety case review meeting of 9/23/2019 determined this was inapplicable.” While

light on technical content, this is specific documentation that a deliberate process was said to be used to decide not to address a prompt element. However, root cause analysis must still be performed of field issues, and might potentially invalidate this rationale depending upon field experience.

e) **RECOMMENDED prompt elements:** These are optional prompt elements documenting good practices and/or suggestions for helpful techniques. If adopted, they can be included in the safety case. However, addressing these prompt elements is entirely optional. The safety case is considered well-formed whether they are included or not.

f) **PITFALL prompt elements:** These are anti-patterns, typically of the general form: "If X is true, then item is prone to increased risk of Y." The intended interpretation is that if X is true (e.g., use of some design pattern X or engineering technique X appears in the safety case), then the safety case is considered invalid unless epistemic defeater Y has been explicitly argued to be false. In other words, Y presents item risk that is presumed to have been activated by X unless the safety case presents reasonable argument and evidence of mitigation of risk Y. More formally, the term "Pitfall" tags a conditional epistemic defeater prompt regarding defeasibility of a claim that the parent requirement has been met. Responding to a Pitfall prompt element might be accomplished in two ways. (1) Arguing that the precondition X is not true. This amounts to a justified safety case deviation for the prompt element. (2) Arguing that risk due to post condition Y is mitigated when or if precondition X is or might be true. Safety case deviation rules for Pitfalls apply according to the categorization (MANDATORY, REQUIRED, HIGHLY RECOMMENDED, or RECOMMENDED). A safety case deviation has occurred when there is no argument that the Pitfall has been avoided.

   NOTE: For assessment purposes each Pitfall only applies to the scope of the specific clause in which it is listed. However, it is a good practice (but optional) to consider while creating the safety argument that Pitfalls might have a larger impact.

g) **CONFORMANCE statements.** Conformance with each clause is evaluated via both self-audit and independent assessment according to Section 17. Each clause has a conformance statement that provides guidance identifying portions of the safety case and other information sources that are especially relevant to assessing conformance to that clause. Assessors are permitted to consider objective evidence beyond the conformance statement when the assessor determines that the situation warrants, but are limited in conformance determination by the written scope of the clause. (Self-auditors can and should consider whether prompt elements beyond those included in this standard need to be added for a particular item's safety case.) Conformance checks are performed by someone other than the developer of the item being checked for conformance (See Section 17). (There are limited exceptions for safety case artifacts being self-audited; see Section 17.2.2.)

h) **NOTE statements.** These are notes on how to interpret the normative elements of a section and in some cases provide rationale material.

i) **EXAMPLE lists (non-normative).** In some cases examples are provided. Examples are non-normative and, in many cases, will not apply to all items. Their primary purpose is to define by example to reduce potential ambiguity. A secondary purpose is to serve as an informative but incomplete checklist of commonly occurring topics that should be considered if applicable. It is expected and required that construction and assessment of the safety case go beyond the bounds of any examples. While exclusion of examples in a safety case does not by itself result in a finding of non-conformance, independent assessors are encouraged to suggest additional examples, as well as elevation of specific examples to normative prompt element status when warranted based on assessment experience.

j) **REFERENCE (non-normative).** References provide citations to materials such as other standards. They are non-normative by default.

4.1.2 Summary of safety case deviation approach for elements of different types of requirements is shown in Table 4.1:

Table 4.1
Safety Case Deviation Approach

MANDATORY	No safety case deviations permitted.
REQUIRED	Safety case deviations only for requirements that are intrinsically inapplicable due to the fundamental nature of the item and/or the current deployment state of the item. All safety case deviations recorded in safety case. Impact analysis and lifecycle tracking monitor the possibility of a change of applicability status.
HIGHLY RECOMMENDED	Safety case deviations permitted with a technical rationale. Impact analysis and lifecycle tracking monitor the possibility of a change of applicability status. All safety case deviations recorded in safety case with justification.
RECOMMENDED	Optional items. Need not be mentioned by safety case. No argument support required for safety case deviation.

4.1.3 Lists that support a particular clause, such as a list of MANDATORY or REQUIRED items, are interpreted in the following manner:

a) For the sake of brevity, the context of each item in a list is the overarching clause, even if not explicitly stated. This means lists generally provide a set of prompts for brevity and usability rather than fully stated “shall” statements.
b) There is no implied ranking, preference, or priority implied by list order unless explicitly stated.
c) **All prompt element lists are presumed to be potentially incomplete unless specifically stated otherwise. A well-formed and complete safety case extends lists as needed to achieve an acceptable safety outcome.** Unless otherwise stated, prompt element lists are to be considered as a minimum set of points to be considered in the safety case, and not an exhaustive set of all possible points.
d) If different prompt element lists appear to overlap, it is acceptable to trace a single argument or evidence branch to multiple prompt elements if desired. A common situation

is that a MANDATORY prompt element will give a generalized prompt element, whereas one or more REQUIRED prompt elements will give specific examples of that generalized element to ensure that they are considered if applicable.

e) If a single prompt element list contains apparently overlapping items, it is sufficient to trace to whichever prompt element seems most applicable to the developers. Such overlapped lists are often used to address issues of potentially different interpretations and terminology across domains and sub-domains.

f) Each prompt element in the list is accounted for at the stated level of safety case deviation rigor on a per-element basis. Therefore, if safety case deviation is desired for a ten-element list for a single REQUIRED section, the safety case documents safety case deviation in a way that is individually traceable to each of the ten prompt elements in the list. (A single justification statement for safety case deviation might trace to some or all of the ten elements, but that traceability must be documented.)

g) "At least one of" phrasing contains a sub-list of alternatives. Only one alternative within the list need be addressed in the safety case, although others might additionally be addressed if desired. This is true even if the "at least one of" occurs in a MANDATORY or REQUIRED list. Note that in some cases two or more prompt elements might be required in practice due to Pitfall statements or NOTES. Alternatives not listed can be considered to meet the "at least one of" criterion with suitable argument support as to acceptability. (This is according to the principle that prompt element lists are not considered to be exhaustive, and therefore safety cases can add prompt elements as appropriate to the local version of those prompt element lists.)

h) "Tailoring" of list items via omitting consideration of one or more requirements and/or list elements without acceptable justification is not permitted. Safety case deviations from list items are only permitted via the safety case deviation rules discussed in Table 4.1 above.

4.1.4 For simplicity and uniformity, references to sections, clauses, and prompt elements are made using a decimalized notation, notwithstanding the typographical conventions used in numbering the sections themselves.

EXAMPLE: 9.2.3.3(b)(1)(i) is a correctly formatted reference to a hypothetical prompt element sub-sub-list in the HIGHLY RECOMMENDED category of Section 9.2.3.

4.2 Terms and definitions (Normative)

4.2.1 Acceptable

Sufficient to achieve the overall item risk as determined in the safety case.

Example: "Acceptable test coverage" means that the amount of test coverage is sufficient to support the safety case's claim of overall item risk after taking claimed risk mitigation credit.

NOTE: This is an objective term related to the validity and completeness of the safety case, and not a subjective term related to any particular assessor's personal point of view.

See: Section 6.4.3

4.2.2 Activation (of faults or hazards)

An input or situation that causes the system to potentially fail due to a fault or hazard.
EXAMPLE: A bit in memory corrupted by a single event upset is a fault. That fault is activated when the memory location is read and results in a computational error that causes a failure in the form of an incorrect or unsafe item behavior.
NOTE: Fault mitigation such as error detection coding, among other mitigations, can prevent an activated fault from causing a failure.

4.2.3 AI Techniques

A general description of computational algorithms and other techniques that include inductive learning, intentionally non-deterministic behavior, rule-based systems, computer vision, heuristic searches, and other techniques. These are often referred to as “Artificial Intelligence” techniques.
NOTE: This term is meant to be a broadly interpreted descriptive term to encompass software that is not generally amenable to traditional software safety approaches. Whether or not actual “intelligence” is actually involved is a matter beyond the scope of this standard.

4.2.4 Argue

Construct a safety case (including claims, arguments, and evidence) that a particular requirement has been met. The resulting argument shows that evidence supports the claims.
EXAMPLE: “Developer shall argue that all hazards have been mitigated” directs the developers to include in the safety case claims, arguments, and evidence that each hazard has in fact been mitigated.

4.2.5 Assessor

One or more people who perform assessment.

4.2.6 Assessment

Review and evaluate the safety case.
NOTE: Two types of assessment are encompassed by this standard: self-audits and independent assessment.

4.2.7 Automated

Autonomous.

4.2.8 Autonomous

Operates without human oversight or intervention.
NOTE: This standard treats the terms “automated” and “autonomous” as generally interchangeable.
treats these two terms as generally interchangeable"

4.2.9 Autonomy

A capability or function that provides autonomous operation.

4.2.10 Brittleness (of a system)

Tendency to fail when encountering conditions that are only slightly different from conditions in which it works properly.

4.2.11 Chaotic (of a system)

Sensitive to initial conditions to the point of appearing to exhibit random behavior.
EXAMPLE: A robot that is pointed exactly at the center of mass of an obstacle using a completely deterministic algorithmic approach might decide on an apparently random basis to go around the obstacle to the left or right depending on minute variations in conditions beyond the capability of a tester to accurately control, making it impossible in practice to determine which action it will take.

4.2.12 Claim

A falsifiable statement that contributes to establishing that safety is acceptable.

4.2.13 Conformance

An independent assessment result indicates that the item's safety case meets the requirements of UL 4600. (See Section 17.1)

4.2.14 Criticality Level

A level categorizing the risk associated with an unmitigated hazard.
NOTE: Criticality level is intended to be a generic term that encompasses integrity level approaches and assurance level approaches such as SIL, DAL, and ASIL.

4.2.15 Demonstration

Operation of the item, functions, or components to show that a specific property, functionality, or other aspect of the item matches the safety case.

4.2.16 Doer/Checker

A heterogeneous architectural design pattern in which a Doer FCR performs a function while a second Checker FCR performs acceptance tests on the Doer, performing a mutual shutdown if the acceptance test fails.
NOTE: This general concept is also known in other contexts as a safety bag or monitor/actuator pair. It is a specific strategy for using an acceptance test.

4.2.17 Evidence

Data or other information used to support arguments.

4.2.18 Fault Containment Region (FCR)

“A collection of components that operate correctly regardless of any arbitrary logical or electrical fault outside the region.”
Reference: (Lala. J., and Harper, R. Architectural principles for safety-critical real-time applications, Proceedings of the IEEE, 82(1), Jan. 1994, pp. 25-40.)
NOTE: Two FCRs are required to ensure fault detection and/or fault mitigation in the presence of an arbitrary fault.

4.2.19 Fault Model

A specification of all the types of faults that are considered when performing fault analysis.
NOTE: A fault model can include multiple concurrent faults of different types.

4.2.20 Field Engineering Feedback

Acquisition of data from system operation for the purpose of supporting the safety case and identifying potential safety case issues.

4.2.21 Identify

Create an enumerated list responsive to a specified category, property, or other aspect of a clause with sufficient specificity to enable assessment.
(Alternate word form: Identification)

4.2.22 Incident

Occurrence of a safety-related failure which might have resulted in a loss event
NOTE: An incident does not necessarily result in a loss event. It is sufficient that in other circumstances an incident might possibly have resulted in a loss event.
EXAMPLE: A car fails to stop at a stop sign. There is no cross traffic, so no collision results. If cross traffic had been present, a collision could have occurred. This is an incident even though no loss event occurred.
NOTE: All loss events are also incidents. Therefore, the phrase “incidents” is equivalent to “incidents and loss events.”

4.2.23 Independent (failure)

Two or more Fault Containment Regions (FCRs) that have no correlated, common cause, and/or common mode fault conditions.
NOTE: Assuming no accumulation of faults over time, the probability of simultaneous fault activation can be expressed by a simple product of unconditional probabilities.

4.2.24 Independent (review and assessment)

An assessor or reviewer who has no direct incentive and no substantive indirect incentive influencing the result of a review or assessment process.

4.2.25 Item

A product, component, system of systems, or other product-related scope for which conformance to UL 4600 is assessed.
NOTE: The “item” may need to include infrastructure, offboard computing, offboard data storage, development processes, lifecycle support processes, supply chain quality assurance measures, and other aspects of ensuring safety beyond the boundaries of a deployed product itself. The “item” can include an entire product, or only portions of a product, but in any event will include all aspects required for conformance of the portion of the product contained within the item.

4.2.26 Life Critical

An aspect of a system for which a loss event could potentially result in the loss of a human life
NOTE: This is strictly a severity concept. A hazard can be life critical even if developers argue that the associated risk is low due to an improbability of occurrence in operation.

4.2.27 Loss

Human death, human injury, animal death, animal injury, property damage, environmental damage, or other substantive adverse outcome.
NOTE: Which losses are considered adverse is system specific. However, human death and significant human injury are always to be considered to be losses.
NOTE: Safety cases might elect to consider a financial cost caused by an item failure to also be a loss as a “substantive adverse outcome.”
NOTE: “Loss event” generally corresponds to the term “accident” in FAA Order 8040.4B and DefStan 00-056." However, the term “Loss” is used to avoid any preconceptions regarding liability and foreseeability.

4.2.28 Mitigate

Reduce to an acceptable level of risk.
NOTE: The level of acceptable risk depends upon the criticality of the specific risk being mitigated (e.g., life-critical vs. not life critical) and its contribution to item-level risk as established in the safety case. A hazard that presents acceptably low risk without overt mitigation action is still considered “mitigated” so long as it is argued that the risk presented is acceptably low. The word “mitigated” is equivalent to the concept of “acceptably mitigated.” (See definition of “acceptable.”) A risk is not considered mitigated until the mitigation approach, if any, is implemented and associated safety case arguments regarding mitigation have been updated (“tracked to closure”).

4.2.29 Nondeterminism

Behavior that is not repeatable.
NOTE: Nondeterminism might be caused by real time scheduling perturbations, use of pseudo-random algorithms, or other factors.
See also: Chaotic

4.2.30 Operational Design Domain (ODD)

The set of environments and situations the item is intended to operate within. This includes not only direct environmental conditions and geographic restrictions, but also a characterization of the set of objects, events, and other conditions that will occur within that environment.
NOTE: a system has a single ODD by definition. Assessment is made with regard to the entire ODD.
See also: ODD Subset

4.2.31 ODD Subset

A managed portion of an item's ODD.
EXAMPLE: An all-weather ODD is broken up into subsets for fair weather, rain, and snow/ice.
NOTE: An ODD subset might be defined to partition the operational space to ease design tasks, support phased deployment by adding additional subsets over time, or otherwise manage the complexity of a potentially large and varied ODD. The safety case might argue each ODD subset independently for some aspects of the safety case.

4.2.32 Passenger

A human in close proximity to and intentionally in close interaction with a product for the purpose of deriving utility from product use.
EXAMPLES: A human who is: riding in a vehicle, riding on a vehicle, performing cargo onload/offload, or other tasks that result intended vehicle interaction.
NOTE: This definition excludes humans performing traffic control, and other road users such as pedestrians.

4.2.33 Pedestrian

Any human not in, on, or entering/exiting a vehicle.
NOTE: This is intended to be interpreted broadly, including not only pedestrians on public roadways, but also any unprotected human in the vicinity of the system who might be injured or killed by the system.
NOTE: Passengers of one vehicle can be pedestrians from the point of view of a different vehicle.

4.2.34 Proof Test

A test that goes beyond BIST capabilities to detect latent faults.
NOTE: Proof tests historically referred to mechanical tests such as pressure testing vessels or moving emergency valves that cannot be done during normal system operation. They often involve exercising failsafes, exercising sensors that are used to detect failures, or otherwise performing off-line tests.

4.2.35 Provenance

The background of components, materials, supplies, software, and other aspects of the item, especially as conferring distinction or quality.

NOTE: In the context of UL 4600, this refers to establishing that COTS products and their components actually provide the required capabilities, and specifically excluding inferior, counterfeit, and other “unapproved” parts. This is different than variations in parts that provide acceptable capabilities and other versioning activities.

4.2.36 Quality Fade

A supply chain fault in which a component supplier degrades component quality over time via progressive use of substitute materials, substitute components, design changes, and/or elimination of protective components while apparently maintaining functionality and meeting tested parameter values.

4.2.37 Risk

A combination of the probability of occurrence of a loss event and the severity of that loss event.
NOTE: Risk is typically some weighted combination of probability and severity, potentially with a zero or non-linear weighting given to probability. This definition is not meant to exclude alternate but comparable formulations of risk.

4.2.38 Robust

Able to continue operation despite situations that are out of specification.
EXAMPLES: System continues normal or degrade operation despite receiving out of specification inputs, encountering ODD violations, suffering component faults, and encountering data not represented in machine learning training sets.
NOTE: Robustness is often a matter of degree rather than an absolute property.

4.2.39 Safe

Having an acceptable post-mitigation item level risk as defined by the safety case.
See Section 6.4.3.

4.2.40 Safety Case

A structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.
Source: Defence Standard 00-56 Issue 7 (Part 1): Safety Management Requirements for Defense Systems. UK Ministry of Defense. p. 26."

4.2.41 Safety Case Deviation

A recorded exclusion of a prompt element from consideration in accordance with the requirements of Section 4.1.

4.2.42 Safety Culture

The collection of beliefs, perceptions and values shared by workers and stakeholders participating in the development and lifecycle operation of the item.

4.2.43 Safety Related

A function, component, property, or other aspect of the system that affects safety directly or indirectly.

4.2.44 System Element out of Context (SEooC)

A stand-alone component that is the subject of a safety case fragment and assessment.
See Section 5.7.3.

4.2.45 Safety Performance Indicator (SPI)

A metric used to quantify safety performance
NOTE: This term is analogous to the term Key Performance Indicator (KPI), but is specific to safety related aspects of the item

GENERAL TERMINOLOGY REFERENCES:

- Avizienis, A., Laprie, J-C., Randell, B., Landwehr, C., “Basic Concepts and Taxonomy of Dependable and Secure Computing,” IEEE Trans. Dependable and Secure Computing, 1(1), Jan.-Mar. 2004, pp. 1-23.
- ISO 26262-1:2018
- ISO/PAS 21448:2019

4.3 Abbreviations and Acronyms (Informative)

a) AI: Artificial Intelligence
b) ASIL: Automotive Software Integrity Level
c) BIST: Built-In Self-Test
d) COTS: Commercial Off The Shelf
e) DAL: Design Assurance Level
f) DTC: Diagnostic Trouble Code
g) ECU: Electronic Control Unit
h) FCR: Fault Containment Region
i) FMVSS: Federal Motor Vehicle Safety Standards (USA)
j) GNSS: Global Navigation Satellite System
k) GPU: Graphics Processing Unit
l) HARA: Hazard and Risk Analysis
m) ISO: International Standards Organization
n) MEL: Minimum Equipment List
o) NDI: Non-Development Item
p) ODD: Operational Design Domain
q) OEDR: Object and Event Detection and Recognition
r) PSSA: Preliminary System Safety Assessment
s) SEBOK: System Engineering Body of Knowledge
t) SEooC: System Element Out of Context

u) SIL: Safety Integrity Level
v) SOUP: Software of Unknown Provenance / Systems of Unknown Provenance
w) SPI: Safety Performance Indicator
x) SQA: Software Quality Assurance
y) SWEBOK: SoftWare Engineering Body of Knowledge
z) V&V: Verification and Validation
aa) V2I: Vehicle-to-infrastructure
bb) V2V: Vehicle-to-vehicle
cc) V2X: Vehicle-to-other

5 Safety Case and Arguments

5.1 General

5.1.1 The safety case shall be a structured explanation in the form of goals, supported by argument and evidence, that justifies that the item is acceptably safe within a defined operational design domain, and covers the item's lifecycle.

5.1.1.1 MANDATORY:

a) Conformance is demonstrated based upon a documented safety case that:
   1) Uses an acceptable safety case format (see Section 5.2)
   2) Presents an acceptably complete argument supporting defined goals (see Section 5.3)
   3) Presents acceptable evidence (see Section 5.4)
   4) Addresses accepted risks (see Section 5.5)
   5) Addresses safety culture (see Section 5.6)

b) Configuration management of the safety case

5.1.1.2 REQUIRED:

a) Addresses Safety Elements out of Context (see Section 5.7)

b) Additional evidence not included in the safety case is provided upon request
   EXAMPLES: Test results are summarized in the safety case. Details and any additional descriptive material of evidence are made available upon request.

c) Any aspect of a purported safety case that is not documented or not provided is disregarded in performing the assessment.

d) Unless a Safety Element out of Context (SEooC) assessment is being performed, the safety case encompasses all safety related aspects of the entirety of the product and its lifecycle including both bespoke and off-the-shelf components, software, and subsystems. This specifically includes, but is not limited to:
   1) Sensors
   2) Actuators
   3) Computing components
      EXAMPLES: computing hardware, operating systems, libraries
   4) Vehicle platforms used as a basis for adding "autonomy kits"
      EXAMPLE: An add-on automated driving item kit assessment requires ensuring that aspects of safety related to the underlying commercially produced vehicle have been addressed in the safety case. Credit can be taken for previous assessments on the platform, but that is likely to leave gaps unless it was specifically assessed as a SEooC for the purpose of use as an autonomous vehicle platform.

5) On-line services
EXAMPLE: On-line map server provided from a cloud infrastructure to an operational vehicle on an as-needed basis
6) Logistical and maintenance support
7) Assumed infrastructure support
EXAMPLE: Road lane markings

e) Any aspect of a purported safety case that is not documented and/or written down, and is not provided to the assessor upon request, cannot be used in supporting a determination of conformance.
NOTE: Verbal statements and other materials not part of the safety case may be considered by the assessor to help with the assessment process, but cannot be used as supporting argument and/or evidence in evaluation of the safety case.
EXAMPLE: A developer verbally explains why a particular REQUIRED prompt element is inapplicable, but that explanation is not in the actual safety case, nor in any documentation referenced by the safety case. The lack of documented explanation for safety case deviation of that REQUIRED prompt element would cause a finding of non-conformance even though the assessor might consider the verbal explanation reasonable. The non-conformance finding could be remedied if the safety case is updated, but it is not the Assessor's responsibility to do so.
EXAMPLE: A tester verbally states that tests were performed on a particular configuration that is being deployed. However, documentation of the configuration that was actually tested has been lost and cannot be reconstructed with reasonable certainty. To the extent that documentation of the configuration tested is necessary for a well-formed safety case, the Assessor must find non-conformance due to the missing documentation, and potentially the tests must be re-run.
f) Identify any initial portion of lifecycle during which the safety case is not intended to be valid
EXAMPLE: The safety case does not apply until the time of the first public road testing within the lifecycle
NOTE: This permits completing the safety case in parallel with prototype development and potentially closed-course development testing. It is not intended to permit a claim of conformance for any vehicle operating on public roads at any time in its lifecycle.
g) Change management for the safety case

5.1.1.3 HIGHLY RECOMMENDED – N/A

5.1.1.4 RECOMMENDED – N/A

5.1.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

5.1.1.6.1 NOTE: This standard was written to help support the building of a well-formed safety case. Additional measures will be required to ensure operational safety. As an example, an end product standard might require conformance not only to this standard, but to other standards

involving topics such as electrical safety, fire safety, and passive occupant protection, among others.

5.1.1.6.2 NOTE: This clause is explicitly intended to require that the conformance documentation package is in the form of a safety case. (I.e., everything other than administrative matters dealing with the assessment itself is a part of the safety case). As a practical matter there may be a variety of documents, repositories, and tools used to provide details such as evidence that make it impractical to have the entire safety case in a single tool or uniformly formatted data set. However, assessment requires ability to access any such material to perform an assessment.

5.1.1.6.3 NOTE: In general, this section generally places requirements upon the structure and content of the safety argument. Other major sections generally place requirements upon determining the completeness of the safety case.
REFERENCE: MISRA “Guidelines for automotive safety arguments,” 2019.

5.2 Safety case style and format

5.2.1 The safety case shall use a defined, consistent format for goals, arguments, and evidence.

5.2.1.1 MANDATORY:

a) Definition of goal and argument syntax, semantics, and any graphical elements used
NOTE: Notation might not have formally defined semantics. However, best available information about the safety case notation and approach should be provided to facilitate interpretation that is as uniform as practical across the developer team and assessors.
b) Definition of evidence types, formats, data dictionaries, and schemas used
c) Assessor access to complete safety case
    1) Elements of the safety case not available to the assessor are not relied upon in conformance evaluation.

5.2.1.2 REQUIRED:

a) Adherence to defined formats within safety case
b) Assessor access to any available browsing, searching, reporting, and analysis tools relevant to understanding the safety case
NOTE: As a practical matter there are likely to be tools and other support used by the developers and self-auditors to make it easier to work with the safety case. Those same tools and other support are made available upon request.
c) Identify reasoning approach regarding completeness of inductive elements of the argument

5.2.1.3 HIGHLY RECOMMENDED:

a) Use of an established method to organize the safety case in a highly structured manner such as:
    1) OMG Structured Assurance Case Metamodel (SACM)

2) Goal Structuring Notation (GSN)
3) Claims Argument Evidence (CAE)
4) Toulmin Analysis

b) Use of tool support to aid in safety case comprehension and navigation

5.2.1.4 RECOMMENDED:

a) Use of a graphical interface for relevant parts of safety case navigation where it increases navigability
b) Use of structured text-based notation rather than free-form text where it increases ability to provide tool support

5.2.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.2.1.6.1 NOTE: Regarding the word “consistent” in the clause, it is permissible for different branches of a hierarchical argument to use alternative argument formats within reason, especially if argument applies to significantly different functions or subsystems. Alternatives can make sense due to either differing original source of argument structures or the need to use a technique more suitable to specific argument technical challenges. If more than one style is used, the style applicable to each section of argument corresponds to a clearly specified style.

5.2.1.6.2 NOTE: While a purely text-based approach can be acceptable, a highly structured approach for argument is strongly encouraged. A graphical plus browser tool approach applied to a graphical representation (or rendering of an underlying text-based representation) for at least the overarching argument structure can be beneficial.

5.2.2 The evidence used shall conform to defined, auditable formats.

5.2.2.1 MANDATORY:

a) A defined type for each set of evidence from a defined set of types used in the safety case
   EXAMPLES: Simulation output files, test plans, vehicle data logs
   NOTE: “Type” is meant in a flexible, generic sense. However, each set of evidence is of a defined type (even if each set is a unique type different from all other sets of evidence). That type is then associated with metadata that permits interpreting the evidence, per the next prompt element.
b) A defined format for each type of evidence, including at least:
   1) Definition of syntax and semantics, data fields, metadata fields
      NOTE: Semantics are defined to the degree practical given the type and nature of the evidence.
   2) Specification of criteria for evidence consistency, correctness, and completeness suitable to make the evidence auditable
   3) A defined means of validating any evidence that is not derived from acceptable data

EXAMPLE: Subjective expert judgment might be validated by data collection over the item lifecycle

EXAMPLE: An expert opinion that lightning strikes are too rare to be relevant used as evidence for neglecting lightning strike risk mitigation is backed up by argument that any lightning strikes that do occur to deployed vehicles will be recorded and that periodic analysis will be conducted to detect if lightning strike frequency in field data becomes too frequent to neglect. (It should be noted that it is well documented that lightning does in fact strike moving, occupied vehicles upon occasion, and a more suitable safety argument is likely to be that some form of risk mitigation is in place to ensure that the post-mitigation risk from lightning strikes is acceptable.)

5.2.2.2 REQUIRED – N/A

5.2.2.3 HIGHLY RECOMMENDED – N/A

5.2.2.4 RECOMMENDED:

a) Descriptive or tutorial examples for interpreting each type of evidence
b) Avoidance of unconstrained free text as a data type for evidence

5.2.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.2.2.6.1 NOTE: The clause permits each piece of evidence to have a different, defined type. Using a smaller number of consistent types of evidence wherever practical can help streamline the safety case for improved comprehensibility.

5.2.3 The goals and argument in the safety case shall be clear and consistent.

5.2.3.1 MANDATORY:

a) Correct use of natural language
b) Use of a single natural language in the goals and argument

   NOTE: The intent is that any natural language used in the entirety of the safety case, except for evidence, is in a single natural language appropriate for use by the item design team. Evidence can be in alternate natural languages. A reasonable workaround for legacy multi-lingual safety cases might be the use of SEooC-style component safety case interfaces between different-language sections. This does not preclude the use of additional mathematical notation and formal languages accessible to speakers of the natural language selected.

   NOTE: Component safety cases do not have to be in the same language as the item level safety case. However, a component safety interface must be included in the same language as the safety case. For example, a Chinese language component safety case can export an English language component safety interface that is used in an English language item level safety case (see Section 5.7.1).
c) Use of language reasonably understandable by a native speaker with general technical expertise in the item domain

NOTE: This is intended to make the safety case argument and goals accessible to an Assessor who is not part of the design team. Assessors are unlikely to be expert in the details of a particular item, but can be assumed to have general understanding of the domain and relevant technologies.

5.2.3.2 REQUIRED:

a) Definition and consistent use of any defined notation
EXAMPLES: Formal specification language, mathematical notation
b) Avoidance of substantive ambiguity

c) Use of diagrams, illustrations, interactive drawings, and other graphical approaches to supplement text when appropriate.

5.2.3.3 HIGHLY RECOMMENDED:

a) Identification of, adoption of and conformance to a technical writing style guide, including language use
b) Identification of, adoption of and conformance to a visual design language for applicable aspects of safety case related tool interfaces
c) Use of automated analysis tooling on the safety case
    1) Spell checker
    2) Grammar checker
    3) Detection and correction of excessively complex sentences
    4) Technical writing specific text style checker
    5) Traceability link checkers
d) Highlighting and careful use of qualifying statements and limiting phrases
EXAMPLES: Detect and exercise care with the phrases: “essentially all,” “should be,” “generally”
e) Highlighting and careful use of negations for clarity, especially multiple negations
EXAMPLES: “Not unlike,” “A safe outcome might NOT occur”

5.2.3.4 RECOMMENDED – N/A

5.2.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.3 Goal and argument sufficiency

5.3.1 The safety case goals shall encompass all identified safety related hazards and risks.

5.3.1.1 MANDATORY:

a) Definition of item safety requirements in the form of argument goals
    1) Safety requirements for intended functionality

2) Safety requirements for potentially unintended functionality
   EXAMPLE: Vehicle movement via response to a dispatching request is unintended when in a disabled maintenance state
3) Safety requirements for unsafe behaviors and states that must be avoided
   EXAMPLE: For functional safety this is often performed via hazard analysis
4) Safety requirements for mitigating faults in the item itself, including both design faults and operational faults
5) Safety requirements for mitigating faulty, exceptional, and unspecified environmental conditions
6) Safety requirements for life cycle considerations, including updates, inspections, maintenance, and monitoring of changing operational environments

b) Mapping of each identified hazard to a potential violation of at least one relevant safety requirement
c) Identification of an acceptable level of safety for each hazard identified

5.3.1.2 REQUIRED – N/A

5.3.1.3 HIGHLY RECOMMENDED:

a) Exclusion of goals unrelated to identified hazards and risks
   NOTE: This is a backward traceability requirement to avoid goals that aren't actually relevant to item safety.
   NOTE: For SEooC safety cases it is acceptable to trace safety case fragments to the exported SEooC boundary interface under the presumption that at least some users of the SEooC will have a higher level item safety case that completes the tracing relationship to identified hazards and risks.

5.3.1.4 RECOMMENDED – N/A

5.3.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.3.1.6.1 NOTE: The term "goals" as used in this clause is a generic term, and includes sub-goals.

5.3.2 The safety case argument shall support all identified goals.

5.3.2.1 MANDATORY:

a) Support safety case goals by acceptable argument
b) Identify criteria used to determine sufficiency of arguments

5.3.2.2 REQUIRED:

a) Use of epistemic defeaters in arguments
   NOTE: Many of the prompt elements in other clauses are epistemic defeaters. Additionally, reviews of each argument subtree can include consideration as to whether any additional epistemic defeaters are applicable.

b) **Pitfall:** Taking credit for conformance to a safety standard without specifically describing the limitations of the conformance assessment is prone to over-crediting safety attributes. (*)
NOTE: This is in effect an argument gap that does not support the identified goal(s). See also Section 5.7.
c) **Pitfall:** Taking credit for conformance to a safety standard designed for human operated equipment is prone to missing fault management control obligations implicitly placed upon autonomy. (*)
NOTE: This is a special, but important, case of the preceding Pitfall regarding limitations of conformance assessment to a safety standard.
EXAMPLE: Credit taken for ego vehicle controllability in assessing ISO 26262 conformance places a corresponding controllability obligation upon autonomy functions to exercise that same level of control. The need to argue a replacement for the human to provide the controllability assumed as part of ISO 26262 ASIL assignment might be missed if this Pitfall is not addressed.

5.3.2.3 HIGHLY RECOMMENDED:
a) Avoid including arguments not in support of an identified goal
b) Avoid including evidence not in support of arguments

5.3.2.4 RECOMMENDED – N/A

5.3.2.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

5.3.2.6.1 REFERENCE: (*) For Pitfalls see generally: Koopman, P., Kane, A. & Black, J., "Credible Autonomy Safety Arguments," Safety-Critical Items Symposium, Bristol UK, Feb. 2019.

5.3.3 The safety case shall avoid argument defects.

5.3.3.1 MANDATORY:
a) Identify candidate relevant logical fallacies
NOTE: This results in a checklist of logical fallacies to be avoided in the safety case.
b) Identify candidate relevant rhetorical devices
NOTE: This results in a checklist of rhetorical devices to be avoided in the safety case.

5.3.3.2 REQUIRED:
a) Avoid identified logical fallacies
b) Avoid identified rhetorical devices
c) **Pitfall:** Taking credit for proven in use technology that is used in a different operational environment or for a different purpose is prone to over-crediting safety attributes. (*)
    1) This Pitfall specifically includes COTS, legacy, and SEooC components, including hardware and/or software
    (**NOTE**: See Section 13.4)

2) This Pitfall specifically includes changes in item operational parameters that might be relevant to the component
EXAMPLE: Lions, J.L., Ariane 5 Flight 501 Failure, Report by the Inquiry Board, 1996

d) **Pitfall:** Discounting failures in field engineering feedback because there has been no previous failure is prone to inductively discounting multiple failures that, if taken as a set, substantively demonstrate invalidity of a safety case. (*)

e) **Pitfall:** Arguing coverage of autonomous failure analysis based on data from human-operated item is prone to missing some types of failures, including: (*)
1) Failures that are triggered by operational situations an autonomous item might enter that human operators typically avoid
2) Failures atypical of human mistakes that an autonomous item fault could trigger

f) **Pitfall:** Arguing risk mitigation via analysis of operational data and/or test data based on arrival rate of incidents (“surprises” or other potential failures) is prone to: (*)
1) Overlooking the additional compounding factor of the distribution of the means of different types of root causes
EXAMPLE: a heavy tail distribution of mean arrival rates of different types of triggering events for item failures
2) Overlooking the potential effects of infrequent but inevitable common cause events
EXAMPLES: Leap seconds, GPS date rollover, daylight savings time changes, or other time keeping anomalies

g) **Pitfall:** Arguing test coverage based upon human-designed test planning is prone to overlooking edge cases that apply to autonomous functions but would not generally be considered edge cases by a human item operator. (*)

h) **Pitfall:** Arguing item correctness based upon use of formal methods is prone to overlooking any invalidities in underlying assumptions made by the proofs (*)

i) **Pitfall:** Arguing that risk is low for a known hazard or variance from expected behavior based upon operational experience alone is prone to underestimating the possibility of catastrophic outcomes.
Reference: Rogers Commission Report; Report of Columbia Accident Investigation Board, 1986

j) **Pitfall:** Arguing low risk based upon unvalidated simulation results alone is prone to missing risks due to simulation defects, modeling faults, and simplifications made in the abstraction process to create the simulation.

5.3.3.3 HIGHLY RECOMMENDED – N/A

5.3.3.4 RECOMMENDED – N/A

5.3.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.3.3.6.1 REFERENCE: (*) For Pitfalls see generally: Koopman, P., Kane, A. & Black, J., "Credible Autonomy Safety Arguments," Safety-Critical Items Symposium, Bristol UK, Feb. 2019.

5.3.4 The safety case shall avoid inclusion of defective construction patterns.

5.3.4.1 MANDATORY:

a) Identify list of defective construction patterns of potential concern
NOTE: These include risky or otherwise unsuitable “patterns” in architecture, design, and implementation that are deemed unacceptable for the item. (These are not patterns actually in use, but rather a catalog of patterns that are to be avoided.)
NOTE: A minimum list includes identifying patterns enumerated in Section 5.3.4.2. The list can be further expanded based upon experience and literature research as determined by the design team.

5.3.4.2 REQUIRED:

a) Avoid identified defective construction patterns
b) **Pitfall:** Use of a “command override” pattern with a doer/checker architectural pattern is prone to failure to mitigate unsafe behaviors. (*)
c) **Pitfall:** Use of a checker that does not mitigate all hazards attributable to the associated doer is prone to failure to mitigate unsafe behaviors. (*)

5.3.4.3 HIGHLY RECOMMENDED – N/A

5.3.4.4 RECOMMENDED – N/A

5.3.4.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

5.3.4.6.1 REFERENCE: (*) For Pitfalls see generally: Koopman, P., Kane, A. & Black, J., "Credible Autonomy Safety Arguments," Safety-Critical Items Symposium, Bristol UK, Feb. 2019.

5.4 Evidence sufficiency

5.4.1 All argument in the safety case shall be supported by evidence.

5.4.1.1 MANDATORY:

a) Each argument element is traceable to supporting evidence.

5.4.1.2 REQUIRED – N/A

5.4.1.3 HIGHLY RECOMMENDED:

a) Use of the following categories of evidence:
    1) Experimental data
    2) Analytic data
    3) Procedure definitions

4) Development and V&V process data
5) V&V data
   EXAMPLES: test plans, test results
6) Qualitative analysis and subjective judgement
7) Field engineering feedback data
8) Placeholder for evidence that will be collected via field engineering feedback
9) Accepted risks, including evidence that risk is acceptable
10) Assumptions for which no evidence is provided, including basis of support that the assumption is reasonable

5.4.1.4 RECOMMENDED – N/A

5.4.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

5.4.1.6.1 NOTE: Traceability can be direct or can be indirect via sub-arguments and/or sub-claims

5.4.1.6.2 NOTE: Argument structures may contain sub-arguments and other supporting information. However, each argument branch ultimately traces to at least one element of supporting evidence that is acceptably broad in scope to support the claims being made. Arguments that are not supported either directly or indirectly (via sub-argument) by evidence is invalid.

5.4.2 Arguments shall encompass the validity of evidence.

5.4.2.1 MANDATORY:

a) Safety case records the experimental design or other data collection strategy for evidence
b) Identify criteria used to determine sufficiency of evidence

5.4.2.2 REQUIRED:

a) Argue evidence is sufficient to result in an acceptable safety case
   1) Describe manner in which evidence is used to support or refute the validity of an argument and/or goal.
   2) Arguments that risk of confirmation bias has been mitigated
b) Lifecycle monitoring performed upon any evidence fully or partially based upon any of:
   1) Unsupported expert or subjective opinion
   2) Existing practices that are not supported by data and are not supported by written public standards documents, public guidance documents, or similar cited sources
   3) Assumptions

   NOTE: Lifecycle monitoring is employed to monitor risk to the degree that argument relies upon opinion, assumptions, or potentially weak evidence.
c) Identification of epistemic defeaters and accompanying defeasibility arguments, including at least:

1) Potentially confounding experimental variables
2) Potential biases in data
3) Potentially insufficient quantity of data samples

5.4.2.3 HIGHLY RECOMMENDED:

a) Inclusion of counter-evidence and accompanying arguments
b) Lifecycle monitoring of evidence is based on consensus-based public standard approaches
c) **Pitfall:** Collection of data before argument has been created is prone to p hacking

5.4.2.4 RECOMMENDED – N/A

5.4.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, evidence gathering design, and design records.

5.4.2.6.1 Note: In practice, this clause may result in an argument structure of the form: the argument is valid because (1) it is supported by evidence, and (2) the evidence itself is valid. Valid evidence is at least supported by objective, factual data.

5.4.2.6.2 Note: The potential seat of epistemic defeaters and potential types of counter-evidence that might be collected is effectively unbounded. Some defeaters and counter-evidence is more likely to be relevant in practice. Selection guidance is provided by prompt elements in this standard and is additionally informed by developer experience.

5.4.2.6.3 Note: Unsupported expert opinion includes statements by domain experts that are not substantively supported by presented evidence. Opinions directly based upon scholarly papers, substantive data, and the like may be considered supported in this sense so long as that basis is stated as part of the evidence and the experimental context of the cited work is explicitly argued to apply to its use in the safety case.

5.4.3 Support of evidence validity shall encompass difficult to reproduce aspects of the item.

5.4.3.1 MANDATORY:

a) Identification of any nondeterministic and chaotic aspects of the item with regard to evidence (if none, so state)

5.4.3.2 REQUIRED:

a) Arguments and evidence to mitigate risk of invalidity due to nondeterministic aspects of the item and its operating environment (if none, so state)
   EXAMPLE: Use of concurrency management mechanisms to mitigate timing-sensitive concurrent access faults, use of seeded pseudo-random number generators to reproduce intentionally nondeterministic behaviors for testing repeatability.
   EXAMPLE: Fault injection used to fail components which would otherwise fail infrequently during testing.

b) Arguments and evidence to mitigate risk of invalidity due to chaotic aspects of the item and its operating environment (if none, so state)
EXAMPLE: Strategy for testing reproducibility when item behavior changes dramatically based on small input differences. For some items a concrete example is whether the item veers left or right when an obstacle appears exactly in front of it.
c) Any metrics used conform to the characteristics relating to SPI Metrics (See Section 16).

5.4.3.3 HIGHLY RECOMMENDED:
a) Use of statistical significance approaches

5.4.3.4 RECOMMENDED – N/A

5.4.3.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

5.4.3.6.1 NOTE: Nondeterminism means that an item can behave in different ways for identical initial conditions (e.g., due to use of a pseudo-random algorithm). Chaotic means that the item can behave in different ways due to perturbations in initial conditions that are smaller than the ability of validation methods to control. Both nondeterministic and chaotic properties result in varying responses to testing, for example, but are caused by different sources. An item can be both nondeterministic and chaotic. It is not essential to differentiate between these causes if either is acknowledged to be present, but mitigation of both possibilities must be considered in establishing the validity of evidence. Non-deterministic and chaotic behavior can undermine the validity and completeness of test results if tests pass by chance due to favorable system behavior in a particular test run.
See Also Section 12.4.7 regarding fault injection.

5.5 Accepted risks

5.5.1 Accepted risks shall be identified.

5.5.1.1 MANDATORY:
a) Identify acceptance criteria for any risk less than fully mitigated.

5.5.1.2 REQUIRED:
a) Identify any risk that is less than fully mitigated to an acceptable level as an “accepted risk.” These include but are not limited to:
    1) Unmitigated risks
    EXAMPLE: An item level safety assessment potential hazard that was determined to be extremely improbable or otherwise not something that could happen in the “real world” is an accepted risk and is included in the safety case as an unmitigated risk.
    2) Partially mitigated risks (i.e., risks not mitigated to a fully acceptable level)
    3) Unknown risks
    EXAMPLES: “known unknowns,” “unknown unknowns”

4) Risks for which mitigation is based on unsupported expert opinion, assumptions, or other less-than-comprehensive evidence and also are not in conformance with generally accepted industry practices such as standards documents

b) For less than fully mitigated risks (including accepted risks) characterize the level of mitigation and argue that the level of mitigation, if any, is acceptable in the context of the item safety case.
    1) Include an evaluation of the expected outcomes of each risk across the item lifecycle.

5.5.1.3 HIGHLY RECOMMENDED:

a) Characterization of post-mitigation level of risks that are deemed fully mitigated.

5.5.1.4 RECOMMENDED – N/A

5.5.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.5.1.6.1 NOTE: This includes acceptance of any remaining unknown risks, which should be broken down into categories if and as information exists to support doing so (e.g., “known unknowns”). It is understood that such risks might not be readily quantified, but yet they are being accepted when a decision to deploy is being made.

5.5.2 Accepted risks shall be tracked through the item lifecycle via field engineering feedback

5.5.2.1 MANDATORY – N/A

5.5.2.2 REQUIRED:

a) Field engineering feedback for accepted risks to ensure that the risk in practice is less than or equal to the level of risk stated as an expected outcome for item operation

b) Field engineering feedback explicitly considers risks due to gaps in risk analysis

5.5.2.3 HIGHLY RECOMMENDED:

a) Automated field data collection of incidents and loss events to determine if outcomes for accepted risks are within expectations on a per-risk basis

5.5.2.4 RECOMMENDED – N/A

5.5.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and design records.

5.5.2.6.1 NOTE: An example approach is including “unknown risks” in the safety case, noting them as “accepted risks,” justifying why acceptable risk analysis has been performed to permit accepting the resultant risks, and arguing that the root cause analysis procedure explicitly includes identifying novel risks so as to add them to the safety case in a timely fashion when they are encountered in the field.

5.6 Safety culture

5.6.1 The role of safety culture of the developer and supply chain in risk identification and mitigation shall be identified.

5.6.1.1 MANDATORY:

a) Definition of safety culture and role used as part of the risk mitigation approach, addressing at least:
    1) Role of safety staff in ensuring safety
    2) Role of non-safety staff in ensuring safety
    3) Role of management in ensuring safety
    4) Role of safety management item in organization
    5) Role of suppliers in ensuring safety
    6) Role of lifecycle participants in ensuring safety
    7) Independence of safety roles between engineering development stakeholders, deployment stakeholders, and business profitability stakeholders
    8) Upper management visibility of and delegation of authority to safety roles
b) Identify activities that support the communication and tracking to resolution of potentially safety related issues
c) Identify an acceptable set of ongoing field engineering feedback and continuous improvement activities related to safety culture
d) Identify an acceptable set of ongoing activities to gather information on hazards and risks from publicly available sources
   EXAMPLES: monitoring recall notices from other developers, accident investigation reports, regulatory actions in the item domain plus related domains, published statistical analyses of hazards.
e) Argue that the execution of identified activities and other identified factors results in an acceptable safety culture

5.6.1.2 REQUIRED:

a) **Pitfall:** Organizational structures in which engineering, business, and/or operational management can exert control or pressure upon roles tasked with ensuring safety are prone to degraded safety outcomes.
   EXAMPLE: Normalization of deviance

b) All activities that have access to safety related data identified as supporting the communication of potentially safety related issues
c) Identification of role in safety culture in ensuring that root cause analysis will be effective at identifying defects in safety cases and safety processes

5.6.1.3 HIGHLY RECOMMENDED:

a) Identification of metrics and feedback mechanisms used to evaluate and manage safety culture

b) Identification of roles and responsibilities accompanied by argument and evidence for suitable competency of staff
EXAMPLE: Evidence supporting an argument of Suitably Qualified and Experienced Personnel (SQEP)

5.6.1.4 RECOMMENDED – N/A

5.6.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

REFERENCE: See safety culture metrics for SPIs in Section 16.2.5

5.7 Item scope

5.7.1 The argument shall identify safety related aspects of the item, including potential faults and failures, encompassing the item lifecycle.

5.7.1.1 MANDATORY:

a) Identify and describe safety related functionality
b) Identify and describe safety related components
c) Identify and describe safety related properties
EXAMPLE: real time deadline for responding to hazards when credit is taken for response time in risk reduction argument
d) Identify and describe safety related aspects of non-operational lifecycle phases (See Section 14)
e) Identify and describe other aspects of the item related to safety
EXAMPLE: emergent properties such as total system weight if limited kinetic energy is part of the risk mitigation strategy
f) Functional requirements for safety related functionality
g) Acceptable coverage of identified fault models (See Section 6.2)
h) Coverage analysis for the V&V of each identified element
NOTE: See subsections within 12.3 for more information

5.7.1.2 REQUIRED:

a) Safety related exception handling capabilities
b) **Pitfall:** Components and functions that provide data to or otherwise affect the operation of safety related components and functions are themselves safety related, but are prone to being discounted as not safety related if traceability of data flows and other direct and indirect sources of interaction with safety related components is not performed rigorously.

5.7.1.3 HIGHLY RECOMMENDED – N/A

5.7.1.4 RECOMMENDED – N/A

5.7.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

5.7.1.6.1 NOTE: A primary goal of this clause is to ensure that aspects of the item that can contribute to or mitigate risk are identified to ensure inclusion in the safety case.

5.7.2 The safety case shall describe the concept of operations for the item.

5.7.2.1 MANDATORY:

a) Overview of mission capabilities
b) Overview of safety objectives
c) Overview of risk mitigation strategy
d) Overview of item hardware, software, and functional architecture
e) Overview of safety related functionality
f) Overview of item operational modes

5.7.2.2 REQUIRED – N/A

5.7.2.3 HIGHLY RECOMMENDED:

a) Overview of non-safety related functionality and overview of non-interference explanation with safety related functionality

5.7.2.4 RECOMMENDED – N/A

5.7.2.5 CONFORMANCE:
Conformance is checked via inspection of the safety case.

5.7.2.6.1 NOTE: This clause is intended to provide an overview of the item and specifically to provide contextual information needed for understanding the safety case.

5.7.3 The boundary within the safety case between any assessed Safety Element out of Context (SEooC) and the rest of the safety case shall include a specified interface.

5.7.3.1 MANDATORY – N/A

5.7.3.2 REQUIRED:

a) Identification of SEooC boundaries in the safety case, if any
b) For each SEooC boundary:
    1) List of SEooC properties that have been assessed
    2) List of SEooC assumptions that must be true for assessed properties to hold true
    3) SEooC fault model

4) Assessment report for SEooC in same language as item safety case using the assessment report
   NOTE: This might require a translation of the SEooC safety report from the language used for the component safety case to the language used in the item safety case
5) All other characteristics of SEooC that are used as evidence by safety case for the item that contains the SEooC.

5.7.3.3 HIGHLY RECOMMENDED – N/A

5.7.3.4 RECOMMENDED – N/A

5.7.3.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and design records.

5.7.3.6.1 NOTE: The concept of SEooC used here is generic and not limited to the functional safety aspects of the component as might be the case when that term is used in a functional safety standard. Assessment of a SEooC is performed for the full scope of its use in the safety argument.

5.7.3.6.2 NOTE: Lists of SEooC assumptions and properties are documented to the degree they are known. As additional assumptions and properties are discovered over the component lifecycle, they are added. Addition of an additional assumption or property might invalidate higher level safety cases using the SEooC. **Reference:** Lions, J., Ariane 5 Flight 501 Failure Report by the Inquiry Board, 19 July 1996.

5.7.3.6.3 NOTE: Other approaches to modular safety argument, re-use of argument fragments, inter-domain argument reuse, argument patterns, and so on are not specifically prohibited. However, establishing assessment criteria for alternate approaches is beyond the scope of this standard.

6 Risk Assessment

6.1 General

6.1.1 The safety case shall identify risks and argue acceptable mitigation.

6.1.1.1 MANDATORY:

a) Identification of fault models (See Section 6.2)
b) Identification of hazards (See Section 6.3)
c) Risk evaluation (See Section 6.4)
d) Risk mitigation and evaluation of mitigation effectiveness (See Section 6.5)

6.1.1.2 REQUIRED – N/A

6.1.1.3 HIGHLY RECOMMENDED:

a) Identification and use of a total item risk summing approach
b) Calculated probability of incident occurrence yields both probability and confidence for entire causal chain. Probability is considered unbounded unless coupled to confidence.

6.1.1.4 RECOMMENDED:

a) Use of Bayesian analysis for calculating probability of occurrence

6.1.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

6.1.1.6.1 NOTE: Risks that are accepted are still monitored as a mitigation for a situation in which the acceptance was based on an assumption that is incorrect or becomes incorrect. Thus, all risks are said to have been “mitigated” in the final safety case even if there is no explicit mitigation mechanism included in the item design.

6.2 Fault model

6.2.1 The argument shall define a fault model for safety related aspects of the item.

6.2.1.1 MANDATORY:

a) Fault model identified for each safety related item component, feature, or other aspect for which fault analysis is relevant
b) Design fault model
    1) Hardware fault model, including microelectronics
    2) Software fault model
c) Manufacturing fault model
d) Operational fault model

e) Non-operational fault model
EXAMPLES: Age-related component degradation, degradation of item due to lack of operation while in storage
f) Maintenance fault model
g) Procedural fault model
h) Item operation fault model
i) Tool fault model
j) Random faults
k) Systematic faults
l) Fault multiplicity
    1) Single fault
    2) Multiple faults due to a common cause
    3) Accumulation of multiple faults over the lifetime of the item
    NOTE: Credit can be taken for diagnosis, recovery, degraded operational modes, and repair capabilities if supported by evidence
m) Undetected (latent) faults
n) Permanent, transient, and intermittent faults
o) Traceability from each fault model to fault mitigation for applicable components, functions, and other aspects of the item.

6.2.1.2 REQUIRED:

a) Model of safety related expectations for correct or required operation for each safety related component or function.
NOTE: In some safety cases this might correspond to “safety requirements,” but it potentially broader if for example there are safety related non-functional aspects that need to be considered.
EXAMPLE: Abnormally excessive power consumption by a fail-safe device depletes a battery power supply, disabling a failsafe. In this case specified power consumption is a safety related expectation that might not normally be associated with a “safety requirement.”
b) Fail arbitrary fault model at the component level for complex electronic components within an FCR.
EXAMPLES: Programmable hardware, components containing software
NOTE: An arbitrary failure mode at the component level is an arbitrary fault symptom at the next higher level of abstraction, and therefore is being referred to as an arbitrary fault in this context.
c) Inclusion of “other” fault modes for non-complex electronic component fault analysis
EXAMPLE: Beyond “short” and “open” to include resistive faults and capacitive faults for connectors and passive electronic components
d) **Pitfall:** Simplistic fault models are prone to being unacceptable for describing faults in computer-based items
EXAMPLES: Assumptions that all component failures result in clean fail-stop semantics,

considering only input shorts to power/ground, considering only fail-stuck integrated circuit faults, and other fault models that are overly simplistic for some applications

6.2.1.3 HIGHLY RECOMMENDED:

a) Inclusion of electrical, mechanical, and other components that are relevant to ability of autonomy to operate safely
   EXAMPLES: Sensor mounting structure, vehicle wheels
b) Encompassing detected but un-annunciated faults
c) Use of Byzantine component fault model (includes hazardously misleading information)
d) **Pitfall:** Fault models limited by conclusory and subjective statements that a typical type of fault is “unrealistic” or would “not happen in the real world” are prone to significantly understating faults that actually do happen in fielded items.
   EXAMPLE: Exclusion of Byzantine faults in aerospace item fault models (see Driscoll, K., “Real Item Failures,” https://c3.nasa.gov/dashlink/resources/624/)

6.2.1.4 RECOMMENDED – N/A

6.2.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

See also: Fault Detection and Mitigation, Section 10.4
See also: Malicious Fault Model, Section 10.8.2

6.2.2 The software fault model shall include an acceptably broad set of potential software faults and failures.

6.2.2.1 MANDATORY:

a) Tool chain failure
   EXAMPLE: Tool produces incorrect software image or configuration
b) Incorrect requirements and algorithms
c) Incorrectly built software image including nonvolatile data
   EXAMPLE: Wrong version of library included
d) Incorrect installed software image, including nonvolatile data
   EXAMPLE: Deployed software image differs from validated software image
e) Incorrect software image version information, including nonvolatile data
f) Corrupted software image, including nonvolatile data
g) Data reporting tool failure
   EXAMPLE: Incident data reporting tool reports incorrectly
h) Coding defects
i) Defects that corrupt data at run time
j) Defects that corrupt hardware runtime configuration
k) Timing faults

6.2.2.2 REQUIRED:

a) Faults resulting from use of hardware description languages (HDLs)

b) Third party component failure
EXAMPLE: RTOS defect, math library defect
c) Configuration reporting tool failure
d) Tool calibration and usage errors
EXAMPLE: Incorrect command line parameters used when running static analysis tool or compiler
e) Faults and failures associated with entry into and execution of supervisory sections of safety related software
EXAMPLE: Concurrency faults, timing faults, and data concurrency faults that might be caused by interrupt service routines and/or operating system scheduling; disabling interrupts in a way that disrupts system scheduling
f) Defects in software embedded in third party components
EXAMPLES: Sensor firmware defects, network adapter firmware defects, storage module firmware defects
g) Machine learning brittleness
h) Corrupted data
i) Boundary value faults
EXAMPLES: Off-by-one, incorrect handling of borderline cases, array index values at boundaries of array size
j) Exceptional value faults
EXAMPLES: Null pointers, floating point infinity, zero length character strings
k) Out of range value faults
EXAMPLES: Off-scale sensor values, buffer overflows, numeric overflow, floating point underflow
l) Software faults that corrupt memory
    1) Data memory
        i) Volatile memory
        ii) Non-volatile memory
        iii) Stack
        iv) Heap
        v) Statically allocated data
    2) Program memory
m) Software faults that result in incorrect hardware performance
EXAMPLES: Software corruption of hardware configuration, including clock rate dividers, I/O pin configurations, and power management settings
n) Software defects that defeat integrity checks
EXAMPLE: Spurious watchdog timer kick
o) Software component crash
p) Software component hang
q) Software component misses real time deadline
r) Time keeping faults, including:

1) Time keeping overflow
   EXAMPLE: Timer rollover
2) Time keeping roundoff
   EXAMPLE: 32-bit floating point representation of time suffers roundoff error when incremented by tenths of a second
3) Incorrect handling of time keeping discontinuities
   EXAMPLES: Leap second, leap year, “Y2K” bug, Unix time rollover in 2038, Daylight Savings Time, GPS week rollover
4) Incorrect handling of time zones
   EXAMPLES: Crossing international date line, crossing time zone boundaries, changes to time zone boundaries and/or offsets
5) Incorrect calculation of local solar time and position
   EXAMPLE: ODD precludes driving with the sun visible on the horizon due to potential camera issues, but item’s calculation of apparent sun angle at the item’s current position (latitude, longitude, altitude) and date is incorrect due to incorrect calculations and/or incorrect nautical almanac stored date values.

s) **Pitfall:** Use of a fail-crash software fault model is prone to overlooking fail active and other dangerous software failure behaviors.

6.2.2.3 HIGHLY RECOMMENDED:

a) Other sources of systematic faults and errors
b) A specified fault model for malicious data faults
c) An unbounded model for malicious data faults with the sole exception of adversary not knowing secret key values

6.2.2.4 RECOMMENDED – N/A

6.2.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.3 The microelectronic and electronic hardware fault model shall cover an acceptably broad set of potential run-times as well as fabrication faults and failures.

6.2.3.1 MANDATORY:

a) Power supply faults
b) Thermal faults
   EXAMPLE: Clock throttling due to excessive temperature, early failure due to chronic operation at or above maximum rated temperature
c) IC fabrication faults
d) Embedded firmware defects
e) Single event upsets

6.2.3.2 REQUIRED:

a) Clocking faults

b) Errata and design defects
c) Specific types of power supply faults:
    1) Under-voltage (brownout)
       EXAMPLES: Incorrectly configured brown-out protection; brown-out threshold voltage set for microcontroller requirements but is too low for associated non-volatile memory chip causing memory corruption when writing
    2) Fast transient power spikes that do not activate brownout protection
    3) Over-voltage
        i) Due to regulator failure
        ii) Due to external application of high voltage
            EXAMPLE: Tow truck applies 24V jump voltage to 12V electrical system
        iii) Due to power cabling faults
    4) Power phasing and polarity faults
        i) Reverse polarity battery installation
        ii) Application of DC external voltage with reverse polarity
        iii) Coupling with mismatch AC phase angle
        iv) Coupling with incorrect AC 3-phase rotation direction
    5) Loss of at least one supply voltages
    6) Insufficient power supply capability
       EXAMPLE: Weak programming of nonvolatile memory cell due to power supply voltage sag during programming due to high current demand
    7) Voltage regulation failure
        i) Off-chip regulator
        ii) On-chip regulator
    8) Back-feeding or parasitic power supplied via signal inputs
       EXAMPLE: Processor fails to shut down or operates in an anomalous way due to backfeeding supply
d) Multiple adjacent single event upset faults for small geometry devices prone to such faults
e) Design changes
   EXAMPLES: Mask change since most recent design validation, die shrink, temperature qualification range change, vendor changes for a specific component (e.g., produced with different mask or on different fab)
f) Excessive cycling of life-limited devices
   EXAMPLE: Excessive EEPROM cycles that cause cell wearout
g) Memory degradation
   EXAMPLES: Refresh fault, loss of stored charge over time for nonvolatile memory

6.2.3.3 HIGHLY RECOMMENDED:

a) Single event upset fault model includes:
    1) Storage cell faults
       NOTE: Small geometry cells can suffer upsets to multiple physically proximate bits from one single event upset

2) Random logic faults
3) Configuration register faults
4) Storage controller logic
   NOTE: Upsets in controller logic can result in incorrect memory addressing and/or data handling, violating assumptions about single event upsets only affecting a small number of data bits.

b) IC damage
   EXAMPLES: Damage due to voltage spikes, over-temperature operation
c) IC bias
   EXAMPLES: MEMS inertial navigation sensor offset

6.2.3.4 RECOMMENDED – N/A

6.2.3.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.3.6.1 NOTE: This clause is intended primarily as a requirement for comprehensive electronic fault models. Consideration of multiple faults and sequences of faults is dealt with in other sections of this standard.
See also: Section 14.5 (e.g., counterfeit components), Section 14.4 (e.g., use of correct components in manufacturing)

6.2.4 The sensor fault model shall include an acceptably broad set of potential run-times as well as fabrication faults and failures.

6.2.4.1 MANDATORY:

a) Sensor failure
b) Faults, corruption, data loss, and integrity loss in sensor data
c) Physical sensor compromise (partial or total failure)

6.2.4.2 REQUIRED:

a) Sensor component degradation
   EXAMPLES: Sensitivity, loss of calibration, violated temperature specification, abrasion, wear & tear
b) Adverse sensor environmental conditions in operation and in storage
   EXAMPLES: Rain, water splash, mud, icing, dirt, low/high temperatures, low/high humidity
c) Loss of sensor alignment or calibration
d) Transient sensor faults
e) Communication failure
f) Timing failure
   EXAMPLES: Late or incorrectly time stamped data, excessive sensor reporting latency
g) Configuration fault
   EXAMPLES: Configuration data, incompatible version

h) Malicious mechanical physical sensor compromise
EXAMPLE: Defacement, alignment compromise, gouged optics, blunt force impact

6.2.4.3 HIGHLY RECOMMENDED:

a) Malicious computer attack on externally accessible physical sensor compromise if within scope for the security plan
EXAMPLE: Via access to vehicle network; malicious sensor software update

6.2.4.4 RECOMMENDED – N/A

6.2.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.5 The communication fault model shall include an acceptably broad set of potential run-times as well as fabrication faults and failures.

6.2.5.1 MANDATORY:

a) Identified fault model for communications

6.2.5.2 REQUIRED:

a) Communication link loss
b) Communication packet errors
EXAMPLES: Random bit flips, burst errors, packet loss
c) Congestion
EXAMPLES: Excessive latency, repetition, insertion
d) Channel overload
EXAMPLES: Babbling idiot
e) Communication timing
EXAMPLES: High latency, early messages, large latency jitter
f) Faults, corruption, data loss, and integrity loss in data from external sources
EXAMPLES: Masquerade faults, message collisions, channel interference
g) Data integrity check failures
EXAMPLES: Error detection code has insufficient Hamming Distance for operational environment; error detection capability implemented incorrectly, providing reduced bit error detection ability
h) Time-based synchronization and time keeping failures
EXAMPLES: Inconsistent handling of time keeping discontinuities such as leap second, insufficiently robust time synchronization in the presence of a faulty node, time keeping differences between item and remote devices
i) Human communication malfunctions or failures, including at least:
    1) Incorrect behavior of communication features
    2) Obscuration of communication features
    EXAMPLES: Due to ice, snow, lighting conditions, glare, mud, viewer use of polarized sunglasses, vehicle aspect, vehicle distance, vehicle speed
    3) Failure of human to notice communication features

4) Incorrect interpretation by human of communication features
5) Errors of human omission
6) Errors of human commission
7) Human slip errors
   NOTE: A “slip” is an incorrect action followed relatively quickly by human self-correction
8) Willful or defiant failure to comply with intent of communication features

6.2.5.3 HIGHLY RECOMMENDED:

a) Incompatible terminal in network

6.2.5.4 RECOMMENDED:

a) Malicious denial of service if within scope for the security plan
b) Malicious masquerade attacks if within scope for the security plan
c) Other malicious communication faults if within scope for the security plan

6.2.5.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.6 The data fault model shall include an acceptably broad set of data-related faults and failures.

6.2.6.1 MANDATORY:

a) Data storage faults
b) Data transmission faults

6.2.6.2 REQUIRED:

a) Data value faults
   1) Detected data value corruption
   2) Undetected data value corruption
   3) Incorrect data value
   4) Incorrect data format and/or units
   5) Stale data value
      EXAMPLE: Data value not updated despite incrementing time stamp
   6) Malicious data value faults in accordance with security plan
   7) Inadequate data value size
      EXAMPLE: 64-bit floating point value converted to 16-bit integer value results in overflow
b) Metadata faults and related faults
   1) Corrupted metadata
   2) Incorrect metadata
   3) Incorrect versioning and/or configuration information
   4) Incorrect sender and/or receiver for message
   5) Data routing faults

6) Invalid time stamp information
EXAMPLES: Inaccurate time stamp, time stamp rollover, time stamps go "backward" in time

c) Data sequencing and related faults
1) Omitted and/or lost data
2) Delayed data
3) Incorrect order of data sequence
4) Consistency of related data

d) Data retention faults
1) Data not retained long enough
2) Data retained too long
3) Data privacy policies incorrectly implemented per security plan

e) Data authenticity faults in accordance with security plan

6.2.6.3 HIGHLY RECOMMENDED:

a) Identify random fault model
EXAMPLES: Bisymmetric random independent inversion ("bit flips"), burst errors, erasure errors, errors corresponding to RAM data word size, errors corresponding to RAM chip width

b) Identify systematic fault model
EXAMPLE: Incorrect message header associated with data due to software defect

c) Storage-related faults
EXAMPLES: Dynamic RAM refresh failure, delay due to retries after detection of transient storage retrieval faults

6.2.6.4 RECOMMENDED – N/A

6.2.6.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

Reference: SCSC-127 Data Safety Guidance
See also: Section 11 Data and Networking

6.2.7 The electronic and electrical fault model shall include an acceptably broad set of potential run-times as well as fabrication faults and failures.

6.2.7.1 MANDATORY:

a) Connector, conductor, and circuit board faults and failures
1) Short to power/ground
2) Resistive short to power/ground
3) Short between adjacent conductors and/or pins
4) Resistive short between adjacent conductors and/or pins
5) Open connection
EXAMPLES: Broken wire, bent pin, including power, ground, shielding

6) Resistive or intermittent open
EXAMPLES: Cold solder joint, loose connector, corrosion
7) Resistive ground fault
EXAMPLE: Floating ground(s) for each ground trace and combinations of ground traces
8) Resistive power fault
EXAMPLE: Loss of each power trace, loss of each power supply, failure of upstream power sources that affect multiple power supplies
9) Chafing and mechanical wear

b) Active and passive electronic component failures including circuit boards
EXAMPLE: Identified via hardware FMEA, FMECA results
c) Corrosion and electrical contact contamination
d) Water intrusion
e) Thermal faults
EXAMPLE: Loss of thermal contact with heat sink, excessive heat generation from component
f) EMI/EMC
EXAMPLE: Electromagnetic shielding faults

6.2.7.2 REQUIRED:

a) Environmental faults that violate component specifications
b) Mechanical wearout and degradation
EXAMPLES: Potentiometer wear, contactor sparking due to surface pitting
c) Contactor welding
d) Excessive power cycling
e) Power transient on transfer switch activation between redundant power sources

6.2.7.3 HIGHLY RECOMMENDED:

a) Identify other fault mechanisms based on historical data and device specifications

6.2.7.4 RECOMMENDED – N/A

6.2.7.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.8 The mechanical and non-electronic fault model shall include an acceptably broad set of potential run-times as well as fabrication faults and failures.

6.2.8.1 MANDATORY – N/A

6.2.8.2 REQUIRED:

a) Conformance to an end-item standard or other relevant accepted practices that encompasses at least the following items as they relate to safety related failures within scope for this standard:
1) Mechanical motion, including vibration
2) Environmental conditions, including temperature

3) Item contamination, including dirt as well as debris produced by mechanical wear
4) Electrical item integrity, including connectors and wiring harnesses
5) Auxiliary item integrity, including energy sources and power distribution items

6.2.8.3 HIGHLY RECOMMENDED:

a) Isolation for
    1) Shock
    2) Vibration
    3) Fluid barriers
    4) Zonal damage isolation
b) Excessive temperature
    1) Environmental conditions too hot
    2) Environmental conditions too cold
    3) Loss temperature regulation ability
c) Dust, dirt, grit
d) Oil spray
e) Salt spray
f) Freezing
g) Auxiliary mechanical power
    1) Hydraulics
    2) Pneumatics
    3) Vacuum assist
h) Support structures
    EXAMPLES: Bend, break, flex, vibration, resonance, air turbulence
i) Battery failures
    EXAMPLES: Overheat, fluid discharge, depletion, cell failure, fire
j) Other identified standards and best practices associated with end item application

6.2.8.4 RECOMMENDED – N/A

6.2.8.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.9 The procedural fault model shall include an acceptably broad set of potential faults and failures.

6.2.9.1 MANDATORY:

a) Operational procedure definition faults
b) Operational procedure execution faults
c) Out of specification routine maintenance
d) Maintenance procedure definition faults
e) Maintenance procedure execution faults
f) Out of specification corrective maintenance

g) Configuration management failure
EXAMPLES: Update to invalid configuration; installation of unverified configuration
h) For each procedural fault model, consider:
1) Omission
2) Commission
3) Deviation
4) Incomplete or partial execution
NOTE: This includes fault models in Sections 6.2.9.2-6.2.9.4

6.2.9.2 REQUIRED:
a) Maintenance by unqualified personnel
b) Operation by unqualified personnel
c) Software update faults
d) Faults in execution of non-software recalls

6.2.9.3 HIGHLY RECOMMENDED:
a) Maintenance by personnel without permission

6.2.9.4 RECOMMENDED:
a) Operation by personnel without permission

6.2.9.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

6.2.10 The item level fault model shall include an acceptably broad set of faults and failures.

6.2.10.1 MANDATORY:
a) Operation outside of designed ODD
1) Excursion from ODD caused by item malfunction
2) Excursion from ODD caused by change in environment
3) Unintentional attempted use outside ODD
b) Exposure to environmental conditions beyond design specifications
1) Operational exposure
2) Non-operating exposure
EXAMPLE: Item designed for above-freezing conditions is exposed to freezing temperatures during transport
c) Invalidation of ODD model due to environmental changes

6.2.10.2 REQUIRED – N/A

6.2.10.3 HIGHLY RECOMMENDED:
a) Intentional attempted use outside ODD
NOTE: In some cases this may be justifiable. This prompt element provides feedback traceability for use cases missed in analysis.

EXAMPLE: Repositioning via carrying product on a transport truck if previously not considered in defining ODD.

6.2.10.4 RECOMMENDED – N/A

6.2.10.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

See Also Section 8.1.

6.2.11 The infrastructure fault model shall include an acceptably broad set of faults and failures.

6.2.11.1 MANDATORY:

a) For each safety related aspect identified in Infrastructure Support, Section 11.4.1, define a fault model.

6.2.11.2 REQUIRED:

a) Defined fault model includes at least the following (when applicable to each identified safety related aspect):
    1) Missing or fail-silent feature or function
       EXAMPLE: Missing sign, failed emitter, worn out road markings
    2) Incorrect placement or information
       EXAMPLE: Navigation aid displaced from recorded location
    3) Infrastructure maintenance faults
       EXAMPLE: Temporary markings not set up properly during road construction
    4) Defaced, degraded or otherwise altered or modified to not meet requirements in a non-malicious manner
       EXAMPLES: Paint other spilled substance obscures markings, shrub obscures signage, worn out lane markings, signs faded by sun
    5) Obscured or degraded by weather or other operational conditions
       EXAMPLES: Coated with ice, covered with water, covered with mud
    6) Differences between actual status and status in item model
       EXAMPLES: Physical placement disagrees with mapped location, physical features disagree with mapped model of features

6.2.11.3 HIGHLY RECOMMENDED:

a) Maliciously manipulated, altered, or added in accordance with the security plan
   EXAMPLES: Stop sign symbols added to environment, adversarial image attacks
b) Incorrect location
   EXAMPLE: Stop line placed at incorrect location
c) Incorrect type
   EXAMPLE: Incorrect lettering on an informational sign
d) Temporarily failures or alterations
   EXAMPLE: Navigational aid outage during maintenance, loss of power to lights

6.2.11.4 RECOMMENDED:

a) Other failures according to the device or feature

6.2.11.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence and design documents.

6.2.11.6.1 NOTE: This clause has a relationship to map data. A relevant consideration is what happens when road markings and map data disagree due to missing data, incorrect data, stale data, or degraded infrastructure such as a sign that has been run over by another vehicle. These issues could not only affect the ego vehicle but also other vehicles. For example, a missing stop sign can increase the risk that other vehicles, especially with human drivers, fail to stop at a mapped stop sign location, increasing risk to a cross-traffic vehicle.

6.3 Hazards

6.3.1 Potentially relevant hazards shall be identified.

6.3.1.1 MANDATORY:

a) Hazard Log that lists identified hazards and mitigation status
    1) Each hazard traces to a corresponding hazard mitigation approach
    2) Mitigation status of each hazard is kept current and tracked to resolution to acceptable level of post-mitigation risk
b) Identify acceptable level of completeness of hazards listed
   NOTE: This imposes an obligation upon the creator of the safety case to define a target level of completeness for hazard identification. The assessment criteria are: (1) the level of completeness has been defined; (2) in accordance with feedback requirements, any issue with that defined level being insufficiently rigorous is likely to be detected via the feedback mechanism.
c) Inclusion of hazards related to emergent properties and interactions of components
   NOTE: Emergent properties and hazards due to component interactions are difficult to allocate to a single component level hazard, but can nonetheless present risk.
   EXAMPLE: Missed timing deadline due to processor overload in a high-complexity operational environment.

6.3.1.2 REQUIRED:

a) Hazard log meets its defined level of completeness
b) Hazard log updated in response to newly identified hazards
c) Incorporation of hazards and risks identified in response to all clauses of this standard
d) Contribution of Commercial-Off-The-Shelf (COTS) items and other Non-Developmental Items (NDIs) to hazards
   REFERENCE: See Section 13.4
e) Include hazards identified responsive to other clauses in this standard

6.3.1.3 HIGHLY RECOMMENDED:

a) To the extent that a hazard list is considered a different design artifact than a hazard log, then the hazard log is used to update the hazard list.
b) Use of at least one of the following hazard identification techniques:
    1) Failure Mode and Effects Analysis (FMEA)
    2) Failure Mode, Effects and Criticality Analysis (FMECA)
    3) Qualitative Fault Tree Analysis
    4) Design Failure Mode and Effects Analysis (DFMEA)
    5) Hazard and Operability Analysis (HAZOP)
    6) Hazard Analysis and Risk Assessment (HARA)
    7) Common Cause Failure (CCF) analysis
    8) Common Mode Analysis (CMA)
    9) Zonal Safety Analysis (ZSA)
    10) System Functional Hazard Analysis (SFHA)
    11) Systems Theoretic Process Analysis (STPA)
    12) End product standard list of hazards
    13) Experience with item under consideration or similar items
    14) Safety of the Intended Function (SOTIF)-style approaches
c) Use of at least one technique in each of the following categories
    1) Bottom up analysis approaches
    2) Top-down analysis approaches
    3) Non-fault-based analysis approaches
d) **Pitfall:** Bottom-up approaches such as FMEA, FMECA, DFMEA are prone to missing hazards caused by component interactions, as well as correlated component faults, especially due to shared resources such as computational platforms (hardware, software, sensors, actuators)
    NOTE: This Pitfall motivates combining bottom-up approaches with top down approaches.
e) **Pitfall:** Analysis approaches that involve hypothesizing a fault or failure are prone to missing hazards resulting from non-faulty component behaviors and interactions.
f) **Pitfall:** Methods that hypothesize a constrained component fault model are prone to missing fail-active hardware failure modes and unconstrained software failure modes.

6.3.1.4 RECOMMENDED – N/A

6.3.1.5 CONFORMANCE:

Conformance is checked by inspection of the hazard log.

6.3.1.6.1 REFERENCE: ARP 4761

6.3.1.6.2 NOTE: Initial hazard log population can be based upon previous experience and use of acceptable recommended techniques. A combination of recommended methods for identifying hazards can ensure coverage and mitigate the stated Pitfalls depending upon the end-item application.

6.3.1.6.3 NOTE: Other requirements clauses place additional requirements upon the contents of the hazard log. A non-normative summary is that the hazard log contains:

a) List of hazards (see 6.3.1) that is updated and traces to resolution
b) Track each entry to resolution (mitigation to an acceptable risk, see 6.3.1)
c) Initial risk (see 6.4.1)
d) Criticality level (see 6.4.1) including if life critical or significant human injury (see 6.4.2)

6.3.1.6.4 NOTE: Identification of various types of hazards and risks is contained in numerous clauses throughout this standard. All such identified hazards and risks are intended to be incorporated into the hazard log and tracked to mitigation in accordance with Section 6 even if that is not specifically stated in other clauses.

6.4 Risk evaluation

6.4.1 Each identified hazard shall be given a criticality level and assigned an initial risk assuming the absence of mitigation.

6.4.1.1 MANDATORY:

a) Hazard Log records criticality level and initial risk for each hazard

6.4.1.2 REQUIRED:

a) Use of at least one of the following risk evaluation approaches:
    1) Risk table
    2) Risk equation (weighted probability times severity)
    3) Fault Tree Analysis (FTA)
    4) Event Tree Analysis (ETA)
    5) Preliminary Item Safety Assessment (PSSA)
    6) Hazard Analysis and Risk Assessment (HARA)
    7) Bowtie diagram
    8) Item-Theoretic Accident Model and Processes (STAMP)
    9) Field engineering feedback
    10) Other relevant risk evaluation approaches
b) Use of integrity level and related techniques
    EXAMPLES: integrity level and related techniques from ISO 26262, IEC 61508; development assurance level from DO-178
    1) **Pitfall:** Top-down techniques such as FTA are prone to missing common cause failures if not practiced in a way that is specifically intended to identify them.
    EXAMPLE: To avoid this Pitfall, an FTA tool might need to provide support for the same element to appear in multiple branches and for common cause faults involving that element to be detected when performing visualization and analysis.
    2) **Pitfall:** The accuracy of quantitative techniques depends upon several inputs, and is prone to inaccurate assigned probability of occurrence.
    NOTE: It is important to record clearly the justification for assignment of any quantitative inputs in a risk formula.

3) **Pitfall:** Quantitative techniques are prone to inaccurate and optimistic numeric estimates for high severity events.
   EXAMPLE: Fukushima Nuclear Power Station estimate of tsunami risk prior to events of March 11, 2011.
4) **Pitfall:** Quantitative techniques are prone to understating the requirement for risk mitigation for situations involving high severity combined with low probability and/or high severity combined with low exposure.
5) **Pitfall:** Level-based approaches are prone to under-estimating the net effect of high severity, low probability risks if based upon individual item operational exposure rather than deployed cohort operational exposure.
   EXAMPLE: Arguing that a probability of a fatal loss event of 1 in 1000 per item lifespan is negligible and therefore acceptable could result in 10,000 fatalities in a deployed cohort of 10 million items – which might not be acceptable in aggregate.
6) **Pitfall:** Risk acceptance argued via limited exposure and/or low probability of occurrence is prone to underestimate risk if there is insufficient data to statistically support a determination of claimed low probability/exposure.
7) **Pitfall:** Quantitative techniques are prone to understating the potential failure behavior of software if they assume that software failure modes are comparatively benign rather than assuming software can have an arbitrarily bad, quasi-malicious behavior that must be mitigated.
   EXAMPLE: Adoption of an excessively optimistic fail crash assumption (assumes all failures involve a silent, benign halting of processing) vs. fail-active dangerous behavior (assumes failures can produce incorrect dangerous results) in event of malfunction for non-redundant components
8) **Pitfall:** Legacy risk evaluation results that took credit for human operator actions are prone to placing an obligation upon the autonomy to perform comparable risk mitigation actions, with autonomy risk increased if such actions are not performed
   EXAMPLE: Lower ASIL assignment for ISO 26262 based upon credit taken for controllability may place an obligation upon the autonomous item to be able to perform a potentially undefined corrective action to exercise controllability after the corresponding component failure.
9) **Pitfall:** Detailed analysis of COTS components, legacy components and other NDIs is prone to being untenable due to unavailability of developer safety data
   REFERENCE: See Section 13.4

6.4.1.3 HIGHLY RECOMMENDED:

a) Use of integrity levels defined in an accepted domain-relevant functional safety standard
   NOTE: It might not be practical to use such integrity levels for all aspects of an autonomous systems, but it is highly recommended to do so to the extent reasonable.

6.4.1.4 RECOMMENDED – N/A

6.4.1.5 CONFORMANCE:
Conformance is checked by inspection of work product resulting from each technique used and the hazard log.

6.4.1.6.1 NOTE: Probability, exposure, safe failure fraction, and other factors beyond severity may be evaluated when assessing risk subject to acceptable evidence. Consistency between the representation and measurement units used to assigned risk and the acceptable risk criteria is important.

6.4.1.6.2 NOTE: Hazards assigned a risk that indicates they are not safety related are still included in the hazard log, but may be excluded from tracking through other risk assessment process steps. The hazard log records assigned criticality and risk.

6.4.1.6.3 NOTE: Other clauses result in a minimum net requirement of having different integrity levels defined for life critical vs. non-life critical safety properties (i.e., at least two levels of criticality, implying at least two integrity or assurance levels).

6.4.1.6.4 NOTE: It is noted that PSSA and HARA are phases/activities while FTA and ETA are techniques that can be used for performing those activities. No normative distinction is made other than that these are recognized approaches that are responsive to this clause.

6.4.2 Substantive life critical risks and substantive significant injury risks shall be specifically identified as distinct criticality levels.

6.4.2.1 MANDATORY:

a) Identification of substantive life critical risks in the Hazard Log; if none so state
b) Identification of substantive significant human injury risks in the Hazard Log; if none so state
   EXAMPLES: dismemberment, significant disfigurement, fracture, loss of an organ, extended temporary disability.

6.4.2.2 REQUIRED:

a) Life critical and significant human injury risks to encompass both item occupants and non-occupants.
b) Post-deployment monitoring for and potential escalation of theoretically life critical risks that have been deemed non-substantive.
   EXAMPLE: A risk with life critical severity has been deemed so extremely implausible (e.g., it is expected it will never occur in the life of the deployed set of all systems) that it is identified as non-substantive. Field engineering feedback monitors for the occurrence of incidents related to this risk. If such an incident occurs, it is reclassified as substantive with the item updated accordingly to avoid a future loss event related to that risk.
c) **Pitfall:** Any linkage of a determination of “substantive” thresholds to “reasonable,” “plausible,” “real world” or other constraints on fault models are prone to underestimating the probability of a loss event during the lifetime of a large deployed cohort.
   NOTE: Supporting such assertions by data, field engineering feedback of incident

monitoring, and/or limiting deployment to a small cohort are potential argument strategies.

6.4.2.3 HIGHLY RECOMMENDED:

a) Substantive life critical risk is defined by the safety case as more likely than not to result in one or more human fatalities within the ODD over the life of the deployed cohort.
NOTE: This implies that a "non-substantive" risk is less than 50% likely to happen ever in any item instance deployed in the entire cohort.
Reference: This parallels the definition of "extremely improbable" in FAA AC 25.1309
b) Substantive significant injury risk is defined by the safety case as more likely than not to result in one or more non-fatal "serious injury" as defined by legal codes applicable to the ODD over the life of the deployed cohort.

6.4.2.4 RECOMMENDED – N/A

6.4.2.5 CONFORMANCE:
Conformance is checked by inspection of work product from analysis and the hazard log.

6.4.2.6.1 NOTE: A "substantive" life critical risk is one which is expected to result in fatalities often enough that redundancy via use of two fault containment regions (FCRs) or arguments that a single-FCR approach will not fail in the life of the deployed cohort is warranted. This concept is specifically intended to provide compatibility with the ISO 26262 HARA process which can result in a high severity hazard receiving a comparatively low ASIL rating due to low exposure and/or high controllability, permitting less hardware provisioning for lower-ASIL functionality.

6.4.2.6.2 NOTE: As a practical matter this clause mandates the use of at least two criticality levels: life critical, and significant injury. It is acceptable to use an increased number of finer-grain criticality levels, including a non-critical level so long as the criticality level approach fully covers at least life critical criticality and serious injury criticality as identified, separate levels. Each criticality level will in turn impose requirements upon the integrity of safety related functions and components. The mapping of non-human loss events (e.g., property damage) to criticality levels is unconstrained, but in some systems will need to be treated with care if widespread environmental or property damage is possible due to a single loss event or set of common cause loss events.

6.4.2.6.3 NOTE: Traceability of safety relevance across component and function boundaries is essential (e.g., a sensor that provides data to a safety related function is itself safety related unless it is argued that the safety related function itself mitigates the risk of failure for that sensor).

6.4.3 Acceptable risk shall be specified.

6.4.3.1 MANDATORY:

a) Identify risk model used, including any calculation method
EXAMPLES: Risk = Probability * Severity; a defined risk table

b) Identify acceptable risk criteria according to the risk model

6.4.3.2 HIGHLY RECOMMENDED:

a) Use of at least one of:
   1) A Low As Reasonably Practicable (ALARP)
   2) Globalement Au Moins Aussi Bon (GAMAB)
      NOTE: This is generally similar to the notion of a "positive risk balance," which implies that the risk of autonomous system operation will be less than the risk of human system operation.
   3) Minimal Endogenous Mortality (MEM)
   4) Acceptable level of engineering rigor (LoR)
   5) No single fault or acceptably probable accumulated, correlated, common cause, or otherwise coincident faults that can result in the failure of a high criticality function
   6) End product standard requirements
   7) Regulatory requirements

b) **Pitfall:** Any mismatch or difference between actual item deployment and factors affecting baseline risk data is prone to causing inaccurate characterization of baseline risk
   EXAMPLES: demographics of potential victims, operational environment, usage patterns
   NOTE: Demographic distribution of potential victims can matter if identifiable subsets of the population such as children, sight impaired, elderly, or people with a particular skin coloration are statistically exposed to higher risk than the general population. Not only can such heterogeneous risk exposure be a problem in its own right, but also a change in proportion of population that fits a high-risk demographic subset could dramatically alter the expected overall risk to the population in a particular ODD.

6.4.3.3 HIGHLY RECOMMENDED – N/A

6.4.3.4 RECOMMENDED:

a) A method of accounting for the contribution of each hazard to the overall item risk. Use of more than one method for determining acceptable risk might be acceptable so long as there is a coherent evaluation of overall item risk vs. acceptable item risk.

6.4.3.5 CONFORMANCE:

Conformance is checked by inspection of a document describing the risk evaluation, mitigation, and acceptance approach.

6.4.3.6.1 REFERENCES: See also Section 6.5 which defines default minimum acceptable risk mitigation approaches.

6.4.3.6.2 NOTE: Acceptable risk in practice can be affected beyond a straightforward risk evaluation approach due to human perception of locus of control concerns, dread risk aversion, and perceived negative externalities. Perceived risk is not necessarily linearly tied to mathematical risk models such as Risk = Probability * Severity.

6.5 Risk mitigation and evaluation of mitigation effectiveness

6.5.1 A method for mitigating risks to ensure overall item risk is acceptable shall be identified.

6.5.1.1 MANDATORY:

a) Identify risk mitigation model
   EXAMPLE: Application of Level of Rigor (LoR) corresponding to identified risk; experimental evaluation of reduction in probability of activating a given hazard
b) Identify approach to evaluating risk mitigation effectiveness

6.5.1.2 REQUIRED:

a) Field engineering feedback based upon experience to identify unacceptably mitigated risks

6.5.1.3 HIGHLY RECOMMENDED:

a) Map each criticality level to a defined set of minimum activities, tools and/or techniques that are intended to ensure an acceptable level of risk mitigation has been accomplished
b) Use of at least one accepted approach for safety, including:
   1) Safety Integrity Levels (SIL, ASIL)
   2) Performance Levels (PL)
   3) Design Assurance Levels (DAL)
   4) Level of Rigor (LOR)

   NOTE: While software safety is expected to be a key portion of the safety case, the approach to safety used also encompasses digital hardware, sensors, actuator, mechanical, and other safety related aspects of the system.
c) Use of leading metrics to estimate post-mitigation risks
d) Comparison of leading metric predictions with lagging metric results to continually re-calibrate leading metrics

6.5.1.4 RECOMMENDED – N/A

6.5.1.5 CONFORMANCE:

Conformance is checked by inspection of a document describing the risk evaluation, mitigation, and acceptance approach.

6.5.1.6.1 NOTE: Due to the scope of this standard, humans performing a safety critical control task cannot be a mitigation mechanism for safety related failures or malfunctions. Having said that, it is important to demonstrate the expected human behavior of others is not impeded by the failure of the item (for example, it is undesirable for a passenger to be unable to exit the vehicle due to the doors and windows remaining locked during a battery fire).

6.5.1.6.2 NOTE: Generally safety cases will identify some combination of engineering rigor and field engineering feedback of data to ensure that risk mitigation has been successful. Specify the methods used if a heterogeneous set of methods. Acceptable scope and coverage of specific engineering techniques ensures that required risk mitigation is achieved.

6.5.1.6.3 NOTE: It is understood that in some cases evidence will consist of documenting the adoption of accepted industry best practices rather than quantitative evidence. However, argument and evidence based on adherence to accepted practices can be supported by field engineering feedback data to monitor the adequacy of those practices.

6.5.1.6.4 NOTE: To the extent relevant, coordinate use of risk mitigation techniques based on existing standards (and/or state of art in embedded software safety, related safety case studies, etc.) to create a consistent overall item risk mitigation approach. Any individual existing standard might not be acceptable for application to the entire item.

6.5.2 Substantive fatality and injury risks shall require as a minimum use of state-of-the-art practices.

6.5.2.1 MANDATORY:

a) Identify state of the art practices for high quality item designs applicable to the item

6.5.2.2 REQUIRED:

a) Argue and provide evidence that identified state of the art practices have been followed effectively for substantive significant human injury and substantive life critical item functions
b) Argue that adopted practices are adequate
EXAMPLE: New technologies such as machine learning frameworks might be dominated by research-quality tools of questionable suitability for life-critical applications, and might not have been developed with such critical applications in mind. Nonetheless their use might be prevalent and therefore arguably “accepted practice.”

6.5.2.3 HIGHLY RECOMMENDED:

a) Use of state-of-the-art practices identified in domain-relevant safety standards
EXAMPLE: Practices defined in a relevant functional safety standard used for all aspects of item design, included safety related aspects of the item not associated with safety functions.

6.5.2.4 RECOMMENDED – N/A

6.5.2.5 CONFORMANCE:

Conformance is checked by inspection safety argument and demonstration.

6.5.2.6.1 NOTE: In general, this clause is expected to trace to design process, tool qualification, and use of practices tied to a selected level of engineering rigor

6.5.3 Mitigation of life critical risks shall include mitigation of faults that affect a single Fault Containment Region (FCR)

6.5.3.1 MANDATORY – N/A

6.5.3.2 REQUIRED:

a) Identify single-FCR fault mitigation approach for each FCR associated with a life critical risk, if any
    1) Include aspects of fault model affecting each FCR

    NOTE: This includes common cause software, hardware, and other types of faults corresponding to the identified fault model(s) (see Section 12.4) that can one or more FCRs

b) For each identified life critical risk, use at least one of the following mitigation approaches:
    1) Use of multiple FCRs
    2) Use of a defined state-of-the-art mitigation argument approach when only a single FCR is used

    EXAMPLES: Use of PMHF approach defined in ISO 26262-5:2018, use of ASIL D approach defined in ISO 26262:2018.

    EXAMPLE: Derating and/or over-design to reduce mechanical and electrical faults failure rates
    3) Argue that a life critical risk is not substantive (if true), and is mitigated in accordance with criteria for serious injuries instead

    EXAMPLE: Argue that the risk will not result in any incidents within the operational lifetime of a deployed cohort; use of a defined SIL-style approach that rates life critical risk as non-substantive due to low exposure or other factors.

c) Any set of multiple FCRs that jointly contribute to a life critical risk are treated as a single FCR for the purpose of analysis if their joint failure rate could substantively contribute to human loss of life.
    1) Accumulation of faults over time considered in determining probability of joint failure

    NOTE: Multiple FCRs that have high, albeit independent, failure rates are likely to jointly fail simply by chance accumulation of failures if those failures are not corrected quickly, and thus are considered a single FCR for analysis
    2) Consideration of possible common cause faults that might have been otherwise discounted for other risks when determining FCR boundaries

    NOTE: For non-life critical risks common cause failures such as tool chain defects might possibly be discounted in general. A higher standard typically applies to common cause failures if a multi-FCR argument is being made for life critical risk mitigation.

d) Arguments that for each identified life critical risk the mitigation approach is acceptable, addressing at least:
    1) Predicted FCR failure rate(s)

2) Effects of imperfect fault detection
   NOTE: This includes both incomplete diagnosability of hardware faults and failure to detect incorrect software computational state
3) Potential accumulation of faults over time
   NOTE: This includes both hardware faults and software computational state faults.

NOTE: The approach is permitted to also account for unactivated faults, safe failure fraction, self-test, diagnosis, successful repairs, proof tests, and partial mitigation of faults as supported by arguments and evidence

6.5.3.3 HIGHLY RECOMMENDED:

a) Use of defense-in-depth measures
   EXAMPLE: Use of a low-integrity failsafe in combination with a high integrity single-FCR function that is also the subject of a single-FCR mitigation argument
b) **Pitfall:** Claims of high diagnostic and/or fault detection coverage based on simplistic mechanisms are prone to being too optimistic.
   EXAMPLE: A watchdog timer provides useful – but far from perfect – detection of software execution faults.
c) **Pitfall:** Life critical risk mitigation approaches used in other than the end item application envisioned in the defining source material for that mitigation approach are prone to providing insufficient risk mitigation.
   EXAMPLE: ISO 26262 was originally intended for passenger vehicles, and has corresponding assumptions embedded in the formulation of ASIL D requirements. Use in vehicles with higher duty cycles and/or significantly more numerous life critical components might violate those implicit assumptions, necessitating arguments that the approaches are remain valid for the intended application.

6.5.3.4 RECOMMENDED – N/A

6.5.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument and demonstration.

6.5.3.6.1 NOTE: This is **NOT a requirement for full computer item redundancy**. For example, a multiple-FCR approach can use two or more heterogeneous FCRs such as a doer/checker pair.

See Also Section 10.3 Redundancy and Section 10 in General.

6.5.4 Each risk shall be mitigated to result in an acceptable overall item-level risk.

6.5.4.1 MANDATORY:

a) Hazard Log records mitigation of each hazard to an acceptable post-mitigation risk
   1) Mitigation traceable to supporting arguments and evidence
   2) Acceptability of risk traceable to supporting arguments and evidence

6.5.4.2 REQUIRED:

a) Collection and analysis of lifecycle field data measuring whether accepted risks remain acceptable over the item lifecycle
    1) Corrective action initiated if field data reveals accepted risk has been exceeded in operation
b) Inclusion of contribution of accepted risks to overall post-mitigation item risk

6.5.4.3 HIGHLY RECOMMENDED:

a) Application of engineering technical design and analysis approaches (engineering rigor)
b) Application of process rigor
c) Validation and testing
d) Use of redundancy and other fault tolerance strategies
e) Identification of safety goals at the item level
f) Identification of safety requirements
g) Inclusion of cybersecurity related risks in accordance with security plan

6.5.4.4 RECOMMENDED – N/A

6.5.4.5 CONFORMANCE:

Conformance is checked by inspection of argument traced from each entry in the hazard log recording that risk has been mitigated and evaluated to ensure that the post-mitigation item-level risk is acceptable.

6.5.4.6.1 NOTE: Removal of a hazard (for example, by restricting the ODD or removing an item feature) is an acceptable risk mitigation approach. Even though a design change has been made to remove a hazard, the hazard log indicates a status of “removed” rather than having the hazard log entry deleted so as to avoid a later design change that inadvertently but silently reinstates the hazard.

7 Interaction with Humans and Road Users

7.1 Human interaction

7.1.1 The safety case shall argue that hazards and risks involving human interactions have been identified.

7.1.1.1 MANDATORY:

a) Hazard and risk identification relating to interaction with humans addressed in the safety case, including at least:
   1) Transport
   2) Operations
   3) Maintenance

b) Address following topic areas:
   1) Human communication (See Section 7.2)
   2) Interactions with humans and interactions with animals (See Section 7.3)
   3) Human contribution to operational safety (See Section 7.4)
   4) Vehicle interaction (See Section 7.6)

7.1.1.2 REQUIRED:

a) Address following topic areas:
   1) Vulnerable road user interaction (See Section 7.5)
   2) Mode changes that invoke human safety responsibility (See Section 7.7)

b) Address at least the following topics within context of ODD:
   1) Interaction with vehicle occupants
   2) Interaction with other road users
   3) Interaction with humans in lifecycle scenarios
      EXAMPLES: Maintenance, commissioning, transport, storage
   4) Interaction in exceptional scenarios involving humans
      EXAMPLE: First responders, crowds on roadway (e.g., picket line, protests, accident scene)
   5) Communication with humans
   6) Identify any credit taken for human actions
   7) Address an acceptably broad demographic profile
   8) Account for mode changes that place obligations upon non-driving humans for safety
   9) Account for other obligations placed upon non-driving humans
   10) Interaction with non-human-operated vehicles

c) Identify methods to reduce severity of unavoidable collisions involving humans
   1) Vehicle design mitigation techniques
      EXAMPLES: Pedestrian air bags, use of pedestrian-sensing AEB as defense in depth approach

2) Vehicle operational mitigation
   EXAMPLE: Operation at less than 20 mph to reduce potential lethality of any pedestrian collision
3) Vehicle communication to humans (see Section 7.2)
   EXAMPLE: Activation of car horn, flashing headlights

7.1.1.3 HIGHLY RECOMMENDED – N/A

7.1.1.4 RECOMMENDED:

a) Effectiveness evaluation for education/awareness campaigns
   1) Public education and awareness
   2) Customer education and awareness
   3) Other stakeholder education
      EXAMPLES: Regulators, lifecycle stakeholders

7.1.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

7.1.1.6 NOTE: While the scope of this standard is limited to fully autonomous operation, safety is significantly affected by the manner in which the item interacts with non-drivers humans. All facets of safety involving humans other than humans “supervising” autonomous control tasks or performing dynamic control tasks are therefore within scope. Also in scope is autonomy responsibility for any transition between autonomous and human operational modes. In general, other standards and information sources should be consulted for accepted human interaction practices (e.g., user interface design guidelines). This standard limits itself to enumerating safety related issues in-scope for the autonomy safety case, which include identification and explanation of risk mitigation approach (but not the requirements for how mitigation should be performed) of risks that relate to human interaction with the item.

7.2 Human communication

7.2.1 Safety related communication features relevant to humans shall be identified.

7.2.1.1 MANDATORY:

a) Identify safety related active and passive communication features relevant to humans (if none, so state).
   EXAMPLES: Warning stickers, flashing lights, non-electronic communication mechanisms, electronic communication mechanisms
b) Annunciation of unmitigated equipment and functionality faults
   NOTE: This is not a requirement to annunciate all unmitigated faults. Rather, it is a requirement to identify which faults are annunciated. The overall safety case argues acceptability of decisions to annunciate faults or not.

7.2.1.2 REQUIRED:

a) Identify explicit human-oriented communication features including at least the following (for each category listed; if none so state):
   1) Conventional vehicle acoustic devices
      EXAMPLES: Horn, electric vehicle operational noisemaker, reverse motion audible warning
   2) Conventional visual devices
      EXAMPLES: Turn signals, brake lights, other signals required by motor vehicle codes
   3) Unconventional (not typically found on a conventional vehicle) devices
      EXAMPLES: Autonomous mode indicator, vehicle disabled indicator, microphone for picking up emergency vehicle sirens
   4) Voice interface features
      EXAMPLES: Passenger interface, interpretation of loudspeaker broadcast police verbal commands
   5) Gesture interface features
      EXAMPLES: Traffic direction interpretation (manual police traffic direction, crossing guards)
   6) Emergency procedure communications
      EXAMPLES: Passenger distress panic button, emergency procedure instructions to passengers, emergency procedure information provided to crash scene bystanders
   7) Other signaling features and devices, including passive devices, if any
      NOTE: Handling the categorization of devices that cross boundaries of these categories is unconstrained so long as all such devices are accounted for overall.
   8) Communications with passengers, cargo loaders, and other vehicle users
      i) Safety related operational status information
      ii) Cautions
      iii) Warnings
      iv) Alarms
   9) Communication with vulnerable road users
      EXAMPLE: A pedestrian-facing “I see you” indicator on ego vehicle

b) Identify implicit broadcast signaling features for which credit is taken in the safety case, including at least the following (for each category listed; if none so state):
   1) Motion control
      EXAMPLES: Creeping forward to signal intent to move, stopping at a particular location to signal intent to wait for a pedestrian in a crosswalk
      NOTE: This is not an endorsement of any particular motion control method of signaling, but rather a recognition that such types of signaling exist and should be identified if used.

2) Use of signaling channels other than as required by motor vehicle codes
EXAMPLE: flashing headlights to signal other vehicles should proceed when in a potentially ambiguous precedent situation, if such behavior is appropriate

c) Identify remote and indirect safety related communication channels, including if present (for each category listed; if none so state):
1) Passenger communication devices
EXAMPLE: Personal cell phone interface via a ride hailing and rider security app used to set destination, signal that it is time to egress, and confirm correct vehicle for ingress
2) Traffic marshalling communication devices
EXAMPLE: Taxi queue dispatcher request for next vehicle
3) Remote status and actuation capabilities, such as:
i) Vehicle disabled indication
ii) Dispatching
EXAMPLE: Destination request via passenger cell phone app, remote specification of destination and route by central operations
iii) Remote diagnosis
iv) Remote feature activation, including remote change of safety related behavior permissions and limitations
v) First responder support features
vi) Police support features
4) Maintenance and lifecycle communications
5) Teleoperation, including tele-supervision
6) V2X communications
i) Vehicle-to-vehicle (V2V)
ii) Vehicle-to-infrastructure (V2I)
iii) Vehicle-to-other (V2x)
7) Electronic communications to other vehicles intended for human consumption
EXAMPLES: V2V intent communication sent to human driven vehicle to inform the human driver

d) Identify mode and status indication
1) Annunciating changes of modal states
EXAMPLES: Entering and exiting maintenance mode, transitioning from parked on a street to driving
2) Mode confusion and status confusion
EXAMPLES: Mode indication, misleading info regarding item mode

e) Identify annunciation of degradation in safety related vehicle capabilities
1) To occupants
2) To potentially affected non-occupants
3) To remote operators and/or supervisors, if any
EXAMPLES: Violations of traffic regulations such as speed limits, low tire pressure alerts, loss of safety related redundancy, degradation that corresponds to a MEL that

is less complete than the fully functional item MEL.
NOTE: It is not the intention of make occupants or non-occupants responsible for safety in the event in response to such annunciation. Nor is it a requirement to annunciate all faults. Rather, this is a defense in depth measure to help humans create an accurate system operational status model.

f) For each identified safety related communication feature, identify which communication devices support outgoing communications, incoming communications, or both.
NOTE: This applies to all identified safety related communication features, including ones identified responsive to the MANDATORY sub-clause

7.2.1.3 HIGHLY RECOMMENDED – N/A

7.2.1.4 RECOMMENDED – N/A

7.2.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.2.1.6.1 NOTE: The term “communication feature” is intended to be interpreted broadly, including but not limited to lights, bells, buzzers, sirens, spoken messages (e.g., voice synthesizer), displayed text messages, symbols, on-vehicle signage, and any other method of explicitly conveying information to humans. Implicit signaling might be accomplished via vehicle positioning, vehicle motion, and other vehicle movement behaviors. Resolving the distinction for any areas of overlap is unconstrained so long as all aspects of the safety case that rely upon communicating with humans are accounted for.

7.2.1.6.2 NOTE: This section is not intended to state that any particular method of communication confers safety, is required, or is even a good idea. Rather, the intent is to ensure the effects of safety related communications used and credit potentially taken for them in the safety case (both potentially in terms of increasing or mitigating risk) are considered when assessing the safety argument.

7.3 Interactions with humans and animals

7.3.1 Hazards and risks related to interactions with human and animals shall be identified.

7.3.1.1 MANDATORY:

a) Identify hazards and risks relevant to humans (if none, so state)

7.3.1.2 REQUIRED:

a) Identify hazards and risk mitigation related to human passengers:
    1) Passenger ingress
    2) Occupant positioning before and during movement
    EXAMPLE: Child in car seat unbuckles during vehicle motion
    3) Vehicle component movement
    EXAMPLE: Powered seat repositions during vehicle operation, injuring a child

4) Interaction with, positioning for, and safety credit taken for crash safety features, if any
5) Passenger egress
    i) Trapped passenger
    EXAMPLE: Emergency service extrication
    ii) Unresponsive and/or incapacitated passenger
    iii) Urgent egress situations
    EXAMPLES: Medical emergency, vehicle fire
    iv) Egress of animal occupants
6) Occupant does not exit at conclusion of mission
    EXAMPLE: Incapacitated or intoxicated passenger, passenger engrossed in entertainment, homeless person, nobody present to unload cargo
7) Detection and handling of occupant distress
    EXAMPLES: Medical emergency, passenger request for urgent egress, trapped passenger, child left in hot vehicle, pet left in hot vehicle
8) Approaching the vehicle to transition to occupant status
    EXAMPLE: A ride-hail prospective customer approaches an operational vehicle stopped at a traffic signal and attempts to enter. However, the vehicle does not realize a prospective customer is intending to enter, and accelerates into the intersection while that prospective customer is gripping the door handle for entry. The prospective customer's clothing catches on a part of the vehicle, dragging the customer along.
    EXAMPLE: Passengers who have just missed a bus might chase after or grab onto that bus as it departs a stop.
    EXAMPLE: A potential passenger might approach a vehicle from behind, or from an occluded spot with an expectation that the vehicle is in the process of stopping to perform a pick-up but not be recognized in time by the vehicle to avoid a collision.
    NOTE: A potential occupant can be especially vulnerable while approaching a vehicle, especially if the vehicle is for some reason not expecting to be approached, or has limited sensing capabilities in the direction of the approach.

b) Identify hazards and risk mitigation related to cargo
1) Safety of humans while loading and unloading cargo
2) Passenger-carried cargo
    EXAMPLES: Luggage, hand-bags, hand carried items
3) Improper securing of cargo before and during vehicle operation
4) Improper vehicle loading
    EXAMPLES: Overweight, unsafe weight distribution, load extends outside vehicle boundaries, load presents unsafe wind profile
5) Vehicle loads that compromise vehicle operational characteristics
    EXAMPLE: Heavy sloshing liquid loads, loads that raise the vehicle center of gravity excessively

6) Attempted use of cargo capability for passengers or unintended animal transport
EXAMPLE: Attempted operation with adult, child, or pet in an unventilated, uncooled, unheated cargo compartment without acceptable passenger protection features

c) Identify hazards and risks related to other than human passengers, including at least:
1) Pedestrians
2) Other vulnerable road users (See Section 7.3.2)
3) Occupants of other vehicles
4) Non-road users
5) Lifecycle participants
6) Animals in vehicle
7) Humans attempting to rescue or otherwise extricate passengers, animals, or cargo from vehicle

d) Identify hazards and risks related to departures from mission parameter changes and expected operations related to passengers and cargo
1) Effect of failure of communication device during mission
EXAMPLE: Battery depletion of passenger cell phone used as mission interface
2) Effect of in extremis movements
EXAMPLES: Effect of panic stop or swerve to miss suddenly appearing obstacles on unsecured passengers and/or cargo, including unsecured cargo impact with passengers; unsecure cargo ejection from vehicle
3) Unauthorized/unintended change of mission parameters
EXAMPLES: Unauthorized third-party redirects vehicle destination; emergency safety over-ride accidentally engaged
4) Resolution of conflicting instructions, change of mission parameters, and inputs
EXAMPLES: Two adult passengers argue about what destination should be selected; child arguing with parent about whether to go to the school or the playground
NOTE: One resolution approach could involve the concept of defining an "authorized user/operator" hierarchy. However, resolution of this and other similar issues of determining which commands and control inputs are "authorized" is unconstrained so long as it is resolved acceptably in the safety case.

e) Identify hazards and risks while in standby or non-operational status
1) Effect of unexpected movements
EXAMPLE: Vehicle motion with door open
2) Dangerous environment in occupied vehicle between missions
EXAMPLES: Person sleeping in parked vehicle, child or pet left in parked vehicle
3) Fires or freezing involving vehicle contents caused by exposure to extreme temperatures
EXAMPLE: Flammable compressed gas container left in sunlight inside non-operational, uncooled vehicle on an extremely hot day

f) Identify any risk mitigation credit taken for human action or inaction

1) Dependence upon risk mitigation credit for communication channels (both implicit and explicit)
2) Dependence upon risk mitigation credit for expectations regarding expected human behavior
3) Dependence upon risk mitigation credit for ability to predict human behavior
   NOTE: Includes both statistical predictions based on historical data and real-time prediction regarding individual humans as they are encountered

7.3.1.3 HIGHLY RECOMMENDED:

a) Identify hazards and risks related to notifying occupants and external humans that vehicle has stopped movement
   EXAMPLES: Safe to exit vehicle; safe to release safety harness; safe to load/unload
b) For vehicles capable of carrying human passengers, identify hazards and risks related to:
   1) Auxiliary equipment operation during loading/unloading
      EXAMPLES: Automatic door motion, activation of active sensor emitters, automatic seat motion, automatic seatbelt adjustments, automatic cabin reconfiguration motion
   2) Communication of safety related information to passengers
      EXAMPLES: Emergency egress required due to detected battery fire, vehicle fire, stranding in dangerous location such as at a rail grade crossing
   3) Communication for emergency and police situations
      EXAMPLES: Instructions to passengers on requested behavior during a police stop
   4) Intervention for unsafe passenger behavior not otherwise covered in previous prompt elements
      EXAMPLES: Passenger attempts to circumvent safety features, passenger unsafely extends body parts out of open windows or sunroof, inter-passenger violence during shared ride
c) Identify hazards and risks related to exceptional passenger situations not covered in previous prompt elements
   1) Human attempts to ride on exterior of vehicle
   2) Human attempts to enter or exit during operation
      EXAMPLE: Through open window or sunroof
   3) Improper attempt to use vehicle for towing
      EXAMPLES: Bicyclist holds on to be towed, unsafe use of rope tied to vehicle to tow
   4) Command override capability
      EXAMPLES: Ordering vehicle to disobey traffic regulations to escape a perceived dangerous situation such as an attempted robbery, escape from wildfire, or outrunning a tornado

7.3.1.4 RECOMMENDED:

a) Identify hazards and risks related to cargo and animal transportation:
    1) Safety of animals being transported
    EXAMPLE: Environmental conditions, crash protection, dangerous cargo movement affecting animals
    2) Prevention of animals being transported from interfering with safe operation
    EXAMPLE: Animal moves controls, prevents item operation, destroys vulnerable safety related items
    3) Unintentional transportation of dangerous goods – non-malicious
    EXAMPLES: Toxic and/or otherwise hazardous cargo spill, transporting flammable liquids in open containers
    4) Obeying route limits for hazardous cargo

b) Identify hazards and risks related to specification, change, and cancellation of destination and routing information
    EXAMPLE: Reroute to hospital due to passenger medical condition, stop vehicle safely to permit passenger egress if passenger feels uncomfortable with the journey for some reason

c) Identify hazards and risks related to transportation of malicious goods
    EXAMPLE: Ego vehicle used for terrorist bomb delivery

d) Identify hazards and risks related to acceptance of voice commands
    EXAMPLES: Unsafe commands inadvertently picked up from radio, television or music player, animal makes noises incorrectly interpreted as human voice commands; incorrect interpretation of legitimate human passenger commands

7.3.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.3.1.6.1 NOTE: All identified hazards and risks are subject to mitigation according to other clauses. In some cases, mitigations might include or be limited to markings or instructional materials. If so, the safety case should include argument and evidence that markings and materials are acceptably effective.

7.3.2 Risk mitigation and fault model for human interactions shall encompass an acceptably broad demographic profile.

7.3.2.1 MANDATORY – N/A

7.3.2.2 REQUIRED:

a) Hazard analysis considers an acceptably broad demographic profile of humans considering the ODD
b) Risk mitigation considers an acceptably broad demographic profile of humans considering the ODD
c) Evidence that any risk mitigation credit taken for human actions or inactions covers identified ODDs situations and operational modes, including, but not limited to, the following population segments:

1) Children using restraining or protective equipment
   EXAMPLES: Car seats, booster seats, strollers
2) Other children
3) Varied body size and dimensions
   EXAMPLES: Average, short, tall, thin, obese accounting for varied international population norms
4) Varied other physical characteristics
   EXAMPLES: Skin tone, hair style
5) Varied clothing styles
   EXAMPLES: Winter vs. summer clothing, hats, gloves, face masks (for cold weather, surgical masks), barefoot, wet swimming attire
6) Cognitive impairment and erratic behavior
   EXAMPLES: Behavioral health issues, under the influence of drugs, sleep deprived
7) Sensory deficiencies
   EXAMPLES: Hearing impaired, sight impaired, color-blind
8) Temporary mobility impediments
   EXAMPLES: Carrying bags, walking a bicycle, child stroller, shopping cart
9) Permanent mobility impairments
   EXAMPLES: Slow movement, use of cane, use of walker
10) Humans with language/communication incompatibilities
    EXAMPLE: Unable to understand English messages displayed by vehicle
11) Unusual presentation
    EXAMPLES: Intoxicated human passed out in roadway, child falling off curb into roadway, amputees, unusual costumes
    See also: Section 8.4 Perception
12) Animals
13) Other relevant population segments (if none, so state)

d) Consideration of vulnerable humans:
   1) Humans on sidewalks and road shoulders
   2) Humans in parking lots
   3) Humans in protected roadway areas
      EXAMPLES: Bike lanes, pedestrians in crosswalks
   4) Humans in permanent pickup/drop-off zones
      EXAMPLES: Ride share pickup zones, school drop-off line, public transit stops
   5) Humans in temporary pickup/drop-off areas
      EXAMPLES: Surrounding school bus (e.g., with red flashing lights in US)
   6) Humans not normally aware they are exposed to potentially elevated risk from ego vehicle operation
      EXAMPLES: On lawns, in dwellings, in parked vehicles, sidewalk cafes, pedestrian-only zones

7) Humans using assistive and medical equipment
EXAMPLES: Wheelchairs, power chairs, crutches, walkers, intravenous fluid equipment, oxygen equipment
8) Humans operating light mobility systems
EXAMPLES: Bicycles, skateboards, scooters, mopeds, motorcycles, roller skates, other powered and unpowered mobility systems
9) Humans accompanied by objects that might hinder, constrain, or obscure them
EXAMPLES: Strollers (including children inside stroller), baby carriages (including baby inside carriage), wagons, luggage, carried boxes, pets, walking next to bicycle, shopping cart, backpacks, baby slings, head-carried objects, hats, costumes

See Also Section 7.6.1.2.

7.3.2.3 HIGHLY RECOMMENDED:

a) Consideration of high-risk scenarios in which humans do not have right of way
EXAMPLE: Pedestrian appearing suddenly in roadway after crossing in front of a public bus discharging passengers.
b) Hazards and risks due to signaling misunderstanding scenarios including:
1) Confusion about which pedestrian a signal is intended for
EXAMPLE: "I see you crossing the street" indication displayed to multiple pedestrians even though not all pedestrians are actually detected
2) Confusion about meaning of signal. To degree credit is taken for public awareness of signal interpretation, evidence that residual confusion does not unduly impair safety
3) Willful or defiant failure to comply with intent of communication features
4) **Pitfall:** Failure to consider different demographic norms is prone to resulting in humans misinterpreting a situation or signaling strategy.
EXAMPLES: Meanings of particular colors, meanings of symbols, road signage conventions, road traffic prioritization conventions

7.3.2.4 RECOMMENDED:

a) Use of language-independent symbols to supplement or replace written text notifications
b) Use of industry-standard tones and audio cues to supplement or replace spoken notifications

7.3.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.3.2.6.1 NOTE: The terms "demographic" and "population segment" are intended to be used in the broadest reasonable sense, including both physical and other characteristics of humans that can vary and are safety related.

7.3.2.6.2 NOTE: It is recognized that even a safe vehicle might not be able to avoid all loss events involving humans, especially if the humans are intentionally behaving in a dangerous manner.

7.3.3 Hazards which can be contributed to by human-settable item parameters shall be acceptably mitigated.

7.3.3.1 MANDATORY – N/A

7.3.3.2 REQUIRED:

a) Identify human-settable item parameters which can cause or contribute to hazards, including at least the following (if not relevant to safety, justify):
    1) Speed related behaviors
    EXAMPLES: Human command authority over vehicle speed limits, ability to command violation of speed regulations, ability to set speed or other operational parameters beyond safe limits for current driving conditions
    2) Traffic law interpretation and violation
    EXAMPLE: Human ability to command traffic law violations such as going through a red light due to perceived danger to occupants if remaining stopped at light
    3) Ability to turn off or circumvent safety devices and functions
    EXAMPLE: Ability to operate vehicle without proper seat belt use due to injured or immobile passenger, ability to command emergency vehicle operation despite material equipment faults
    4) Reasonably foreseeable misuses of such features
    EXAMPLES: Passenger command to violate traffic laws due to a stated passenger medical emergency when no emergency exists, passenger command to over-ride restraint protocol due to a non-existent medical condition
    5) Maintenance and test modes that permit human override of safety and regulatory items.
    6) Interference with other vehicles or infrastructure
    EXAMPLE: Commanding high beam headlights or other high energy active sensor operational modes when encountering oncoming traffic that is likely to interfere with other-vehicle sensor performance, human-commanded driving profile change increases risk of collision involving other vehicles
b) Describe mitigation approach for each identified risk
c) Argue effectiveness of mitigation approach for each identified risk
d) **Pitfall:** Arguments that safety feature circumvention is available only to authorized personnel are prone to invalidity when “cheat codes” and other simple circumvention techniques that apply to overly-simplistic protection strategies are inevitably made public.
    NOTE: “Cheat codes” and master password disclosure tend to occur in the normal course of the system lifecycle and are not necessarily the result of malicious attacks or car modification.

7.3.3.3 HIGHLY RECOMMENDED:

a) Hazards presented by destination and route selection, including:
    1) Passes outside the ODD

2) Exceeds vehicle range
3) Transit through or destination is a dangerous or prohibited area
   EXAMPLES: War zone, flooded area, fire zone, police activity zone, extreme weather area, portion of city not under police protection, unfriendly country border, exits jurisdiction that passenger is required to remain in by Court order
4) Destination is dangerous to passenger
   EXAMPLES: Mobility impaired passenger discharged in a location that does not have ramped access to sidewalk infrastructure, child discharged on side of busy highway with no sidewalk, passenger discharged at active shooter location
5) Destination is dangerous to non-passengers
   EXAMPLES: Destination selected in the middle of a pedestrian-only area

b) Hazards presented by involuntary destination selection
   1) Roadway obstruction forces mission termination
      EXAMPLE: Downed power line forces stopping in a road that is subject to flooding
   2) Equipment failure forces mission termination at a risky location
      EXAMPLE: Forced mission termination in an intersection, grade crossing, or busy highway that does not permit safe passenger egress
   3) Posted detour forces operation on a high-risk route

7.3.3.4 RECOMMENDED:

a) Consideration of potentially justified but exceptional human operational commands including:
   1. Loading/unloading in an unauthorized zone
      EXAMPLE: Unloading an injured passenger at an emergency room or urgent care center door rather than a designated parking spot
   2. Designating a parking location in exceptional position or on exceptional surface
      EXAMPLES: On homeowner lawn, beach, temporary unprepared surface, event parking in a farm field, parking on unprepared ground to side of road

7.3.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.3.3.6.1 NOTE: An acceptable justification can be that a particular listed type of setting is not accessible by a passenger. However, required aspects of potential human-settable mission parameters are specifically addressed by a well-formed safety case.

7.4 Human contribution to operational safety

7.4.1 Risk mitigation credit taken for human participation in safety related operations shall be identified and shall be argued to be acceptable.

7.4.1.1 MANDATORY:

a) Identify expectations and requirements of humans for which risk mitigation credit is taken. If none, so state.

b) No risk mitigation credit taken for human contribution to dynamic driving task.
NOTE: There is no assignment of safety responsibility for performing the dynamic driving task or other dynamic control actions transferred from the autonomous vehicle to passengers, non-occupants, operations participant, or other road users intended by this section when the item is operating in fully autonomous mode.
EXAMPLE: Attempting to take risk mitigation credit for a passenger noticing a highly unusual system failure or external event and pressing a “panic button” provided in the passenger compartment is not permitted. The provision of such a panic button is not prohibited, and might be a helpful defense-in-depth approach. However, potential use of such a button does not absolve the autonomous system from complete and full responsibility for acceptable risk mitigation without regard to the existence of that panic button.

7.4.1.2 REQUIRED:

a) Argue that identified expectations and requirements are acceptable.

b) Address potential for faulty performance of human participation in risk mitigation activities
EXAMPLES: Omitted, incomplete, incorrect, early, or late performance of safety related human obligations

c) **Pitfall:** Any argument based upon an assumption that a responsible human adult will notice something, behave a certain way, or not behave an unacceptable way is prone to insufficient risk mitigation in real world operation.
EXAMPLES: Not all humans are fully capable adults; not all responsible adults might realize they are expected to owe a duty to contribute to safe operation of the item; not all humans will be cooperative with item expectations of their behavior.

d) Identify responsibilities for risk mitigation assigned to item occupants. This includes but is not limited to:
    1) Pre-departure inspection
    2) Reporting of malfunctions or other issues
    EXAMPLE: Occupant expected to notice and report substantial vehicle damage due to a sideswipe during a mission
    3) Required occupant behaviors
    EXAMPLE: Requirement of occupant to close door completely before selecting a destination
    4) Prohibited occupant behaviors

5) Reasonably foreseeable misuse
EXAMPLES: Faked inspection reports, non-reporting of malfunctions, intentionally operating equipment with doors unsecured, risk-taking passenger thrill behavior
6) **Pitfall:** Adverse operational conditions are prone to resulting in abbreviated or inadequate inspections by occupants.
EXAMPLES: Required occupant inspections might be ineffective due to darkness, adverse weather, and unsafe traffic situations preventing walking entirely around the vehicle, reducing visibility, or curtailing procedural compliance.
7) **Pitfall:** Required occupant inspections are prone to being difficult to enforce in shared vehicles
EXAMPLE: A vehicle assumes missions last no longer than 30 minutes, and requires pre-mission inspections for each new mission. A shared vehicle spends an 8-hour operational shift never having emptied all passengers, but never carrying any one passenger for more than 15 minutes. Each new passenger enters an already-occupied vehicle, and potentially assuming that the previous passenger has conducted any pre-departure inspection. Who is responsible for pre-departure inspections? Will there be social pressure to skip the delay of such an inspection by new passengers caused by impatient passengers already in the vehicle?

e) Identify responsibilities and risk mitigation expectations assigned to non-occupants
1) Expectations placed upon vulnerable road user behaviors
2) Expectations placed upon behaviors for other road users
3) Expectations placed upon behaviors for non-road-users
4) Prohibited and required behaviors for lifecycle participants
NOTE: While the ability of the ego vehicle to control people is limited, it is reasonable to set expectations such as usually obeying traffic control devices so long as inevitable imperfect compliance of other road users is also considered. It is important to make the expectations as conditional assumptions in the safety case explicit.
EXAMPLE: Evidence that reveals bicyclists and pedestrians habitually violate traffic regulations would set an expectation of reduced risk mitigation credit claimed for traffic regulation adherence by bicyclists.
See also Section 7.5.1.2.

f) Identify responsibilities and risk mitigation otherwise assigned to humans
EXAMPLE: Maintenance or inspection activities (see Section 15.1).

g) Handling of maintenance, inspection, repair, and related faults
1) Deferred maintenance
2) Human-commanded operation in faulty or degraded mode
EXAMPLE: Command override to escape dangerous situation despite item faults, such as moving a damaged vehicle stopped on a railroad grade crossing

3) Use of overrides resulting in overly extended operation in potentially unsafe item configurations or environments

h) Strategy for ensuring acceptable performance of responsibilities for which credit is taken in the safety case including consideration of at least the following types of occupants and cargo types (within context of ODD):
   1) Responsible, trained adults
   2) Impaired and/or negligent adults
   3) Untrained adults
   4) Children
   5) Animals
   6) Inert cargo
   7) Active cargo
      EXAMPLES: Robots, drones, or delivery sub-vehicles being transported by the vehicle

   EXAMPLE: The likelihood of a small children not performing responsibilities expected of a responsible trained adult might be mitigated by requiring a competent, licensed adult driver to be present as an occupant during operation, or by designing an item which has no such expectations. Compliance enforcement for any such requirement would be part of a corresponding safety argument.

i) Ensuring compliance with human operational safety task burdens, including:
   1) Evidence of conformance to human-performed safety related procedures, checklists, schedules
   2) Updates to record keeping system as item configuration and safety case change
   3) Completeness and coverage of safety related procedures, checklists, schedules, and other documentation materials related to human operational safety tasks

j) The use of operational settings by which passengers can affect safety related item performance recorded as part of operational data
   EXAMPLES: “Ethical setting” switches, performance ability to command speed limit violation, ability to command traffic law violations
   NOTE: This is not a requirement to retain such data indefinitely. However, such data will contribute to incident analysis. Privacy and other concerns are relevant to this and other data collected by the vehicle.

k) Any safety related risk related to lifecycle human responsibilities including at least the following potential failure modes:
   1) Failure of a non-occupant to perform responsibility
   2) Incorrect performance of tasks and procedures by non-occupants (including deviations, partial completion, other errors of commission and omission)
   3) Unqualified non-occupant human
      EXAMPLES: Unqualified inspector, unqualified maintainer
   4) Quality defects in non-occupant human tasks
      EXAMPLES: Faked inspections, counterfeit materials, use of unauthorized workarounds

7.4.1.3 HIGHLY RECOMMENDED:

a) Occupants not held substantively responsible for safety related aspects of item operation beyond behaving in a generally reasonable manner in keeping with their demographic status

b) Non-occupants not held substantively responsible for safety related aspects of item operation beyond behaving in a reasonable manner in keeping with their demographic status

EXAMPLES: Unimpaired, responsible adult pedestrians are not expected to intentionally hide and then jump out in front of vehicles. Children can reasonably be expected to chase a ball into the roadway even if doing so is unsafe. Factory-trained repair staff can reasonably be expected to perform maintenance procedures properly within the framework of an acceptable quality assurance approach.

c) Consideration of fleet operations when considering training level of occupants

EXAMPLES: Unattended taxi service, unattended public group transit, rental cars with drivers new to the type of vehicle

7.4.1.4 RECOMMENDED – N/A

7.4.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.4.1.6.1 NOTE: Some mitigations for maintenance and inspection faults might be procedural, such as audits and random spot checks.

7.5 Vulnerable road user interaction

7.5.1 Hazard analysis shall include communication features and interactions relevant to vulnerable road users.

7.5.1.1 MANDATORY – N/A

7.5.1.2 REQUIRED:

a) Inclusion of vulnerable road users in hazard analysis. Specifically including:
   1) Reasonably foreseeable human attempts to influence vehicle behavior in good faith, including at least:
      i) Police, fire, other first responder traffic direction
      ii) School crossing guards and school crossing student helpers
      iii) Informal traffic direction attempted by humans

      EXAMPLES: Truck movement, vehicle egress from blind driveway, vehicle crash scene
   2) Reasonably foreseeable human non-compliance, including at least:
      i) Vulnerable road user accidentally falls into roadway
      ii) Vulnerable road user fails to yield right of way when required to do so
      iii) Vulnerable road user otherwise fails to obey traffic regulations
   3) Close-quarter interactions with vulnerable road users:

i) Ingress and egress operations
ii) Movement in pick-up and drop-off zones
iii) Identified crosswalks
EXAMPLE: Zebra crossings, parallel line crossings
iv) Unmarked crosswalks and potentially ambiguously designated crossing points
EXAMPLE: Primary street corners, secondary street corners, alleyway corners
v) Interactions with crowds and event attendees in or near roadway
vi) Swerving and other sudden lateral movement by vulnerable road users
EXAMPLE: Bicycle swerves to avoid a storm drain while ego vehicle is passing; scooter swerves to avoid a pothole, rider hits angled railroad track falls sideways off device spilling into roadway

See Also Section 7.6.1.2.

4) Equipment operation
i) Active sensor energy emission
EXAMPLE: Activation of sensor emitters such as non-eye-safe radar beamed at short children in a cross-walk or adult bending down to pick up something that has been dropped
NOTE: In some cases emission safety is based on low emission energy. However, if the argument is that energy will only be emitted when no pedestrians are in a vulnerable position, then factors such as ability of other sensors detect an appropriate clear space can become relevant.
ii) Mechanical component motion
EXAMPLE: Ego vehicle opens vehicle door into path of oncoming bicyclist

b) Identification and justification for risk mitigation credit taken for communications to non-passengers
1) Consideration of practical effectiveness
2) Operational history used as field engineering feedback for continual re-justification

7.5.1.3 HIGHLY RECOMMENDED

a) Interactions with non-human at risk road users that might present a danger to vehicle occupants, including:
1) Large wild animals
2) Large domesticated animals

7.5.1.4 RECOMMENDED:

a) Interactions with non-human at risk road users that do not generally present a danger to occupants, including:
1) Small wild animals
2) Livestock

3) Pets
4) Protected species
   EXAMPLE: Endangered species, threatened species, animals socially unacceptable to hit

7.5.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.5.1.6.1 NOTE: No clause in this standard is intended to support, advocate, or justify the transfer of liability from the item and its lifecycle support participants to a passenger, occupant, non-occupant, operations participant, or other road user.

7.5.2 Hazard analysis shall include potentially malicious misuse by vulnerable road users.

7.5.2.1 MANDATORY – N/A

7.5.2.2 REQUIRED:
a) Carjacking
b) Assault and/or robbery directed at passengers
c) Theft of and/or damage to cargo

7.5.2.3 HIGHLY RECOMMENDED:
a) Vehicle harassment by pedestrians
   EXAMPLES: Defiant jaywalking, squeegee punks
b) Intentional injury-seeking behaviors
   EXAMPLE: Pedestrian intentionally jumps out in front of vehicle
   NOTE: This is not a requirement to absolutely prevent impact with a pedestrian who is willfully attempting to be injured. Rather, this identifies a scenario that should be considered in hazard analysis, and in particular might reduce the credit that can be taken for humans avoiding risky situations.
c) Police and other first responder impersonation

7.5.2.4 RECOMMENDED – N/A

7.5.2.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.5.2.6.1 NOTE: This clause is intended to cover situations such as malicious pedestrians exploiting designed safe item behaviors for nefarious purposes, such as blocking movement of a vehicle in order to entrap passengers to attack them.

7.6 Other vehicle interaction

7.6.1 Hazard analysis shall include communication features and interactions relevant to other vehicles, including vehicles operated by humans.

7.6.1.1 MANDATORY:

a) Identify hazards and risks related to interactions with other vehicles. (If none, so state)
NOTE: Other vehicles operated by both humans and autonomous controls might behave erratically or in an excessively risky manner. Thus, this Section covers “other” vehicles in general.

7.6.1.2 REQUIRED:

a) Identify credit taken for assumptions regarding interactions with other vehicles
b) Include considerations for interacting with other autonomous vehicles
c) Include considerations for interacting with human operated vehicles, if present in ODD
d) All types of other vehicles within ODD including at least:
    1) Light passenger vehicles
    2) Heavy vehicles
    EXAMPLES: Buses, trucks, mobile homes
    3) Motorcycles
    4) Bicycles and other pedaled vehicles
    5) Mobility aids
    EXAMPLES: Scooters, skateboards, roller skates, “hoverboards,” and other powered and unpowered human mobility aids (whether technically classified as a “vehicle” or not)
    6) Special purpose vehicles
    EXAMPLES: construction equipment, farming equipment, oversize vehicles
    7) Other vehicles under full or partial human control
    8) Other fully autonomous vehicles
        i) Passenger vehicles
        ii) Cargo delivery vehicles
        iii) Bike lane users
        iv) Sidewalk users
        v) Low-flying air vehicles
e) Illegal, incorrect, and other unexpected other vehicle behavior, including at least the level to which fault mitigation will be attempted for:
    1) Violation of traffic rules by other road users
    EXAMPLES: Lane departure, wrong direction of travel on one-way road
    2) Violation of traffic control devices
    EXAMPLES: Running a red light, failure to yield, running stop sign
    3) Potentially justifiable rule violations by other vehicles
    EXAMPLES: Lane departure to avoid hitting human, lane departure to avoid obstacle such as downed tree

4) Equipment, environmental, and control command failures
EXAMPLES: Other vehicle loss of brakes, other vehicle skidding into intersection due to ice, collision from rear due to close following distance, vehicle being pushed into intersection due to collision from rear, distracted driving behaviors, impaired driving behaviors

f) Incorrect or misleading expression of intent by other vehicle
EXAMPLES: Omitted turn signal activation, false turn signal activation (not turning), V2V information promising a specific action differs from actual action such as failing to yield as promised

7.6.1.3 HIGHLY RECOMMENDED:

a) Heterogeneity of other vehicles
EXAMPLE: Different vehicles might have different interpretations of acceptable and desirable vehicle behaviors, and might behave differently. This is potentially true of both human operated vehicles and other types of autonomous items.

b) Potential received energy issues, including:
1) Electromagnetic Compatibility (EMC) issues that impair sensor effectiveness
2) Active emissions that can cause equipment damage and/or false readings
i) Light or laser emissions
EXAMPLE: Incoming high energy laser pulse damages lidar receiving circuitry
ii) Radio emissions
iii) Unintentionally directed toward vehicle sensors
iv) Intentionally directed toward vehicle sensors
v) Caused by other vehicles
vi) Caused by non-vehicle sources
EXAMPLE: Military equipment radar emissions
vii) Normal expected operational received energy
viii) Above expected operational received energy
ix) Broad spectrum received energy
EXAMPLE: Jamming, non-malicious EMI sources, solar flare disruption
3) Temporary sensor blinding
EXAMPLE: High beams blinding opposing vehicle, sun enters sensor field of view, celestial object or its reflection enters sensor field of view

c) Aggressive driving
EXAMPLES: Tailgating, accelerating on yellow light

d) Maneuvers that are perceived as excessively cautious
EXAMPLE: Ego vehicle driving at speed limit but significantly slower than traffic provokes a human to pass unsafely, resulting in a collision.
NOTE: This is not a requirement that vehicles behave unsafely due to human expectations that cars should value speed over safety, but rather is one consideration among many that should be considered in analysis. Mitigation might involve, for

example, communicating the danger causing the ego vehicle to be cautious to other human drivers.

e) Vehicle types, even if not normally expected within ODD:
    1) Off-road human conveyances that can operate on-road
    EXAMPLES: Farm equipment, construction equipment, skiers, snowboarders, snowmobiles
    2) Humans riding animals
    EXAMPLE: Horseback
    3) Animal powered vehicles
    EXAMPLE: Horse and wagon (avoid scaring horse)

7.6.1.4 RECOMMENDED:

a) Vehicle types, even if not normally expected within ODD
    1) Low flying and on-ground aircraft
    EXAMPLES: Helicopters, sail planes, ultralight aircraft, hang gliders that might use roadway as a landing strip
    2) Shallow draft and multi-modal vessels
    EXAMPLE: Hovercraft, flood rescue craft
    3) Novel human conveyance
    EXAMPLE: Jet pack, human roller ball, parachute, hot air balloon, Zorb ball

7.6.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.6.1.6.1 NOTE: While in many cases other human-operated vehicles might strictly be “at fault” for loss events, in real world driving a significant contribution to practical road safety is achieved by drivers compensating for the mistakes of other drivers and practicing the widely recognized concepts of defensive driving. In many jurisdictions, human drivers can have traffic offense penalties reduced by completing a defensive driving course, establishing this as an accepted safe road operation norm. This clause addresses incorporating such compensation into the safety case. As an example related principle: “Right of way is given, rather than taken.” (Mobileye, Implementing the RSS Model on NHTSA Pre-Crash Scenarios, https://www.mobileye.com/responsibility-sensitive-safety/rss_on_nhtsa.pdf Accessed 7 August 2019.)

7.7 Mode changes that invoke human safety responsibility

7.7.1 Hazard analysis shall include mode changes to and from modes which assign responsibility for safety to human vehicle operators.

7.7.1.1 MANDATORY – N/A

7.7.1.2 REQUIRED:

a) Identification of hazards related to any role of human performing dynamic driving operation, including identification of method of performing the following (if fully automated for an item, so state):
   1) Operation outside ODD
   2) Vehicle repositioning
      EXAMPLE: Moving a vehicle to a different spot on a driveway or parking lot under manual control
   3) Emergency vehicle movement
      EXAMPLE: To reposition vehicle after significant item failure
   4) Vehicle transportation support
      EXAMPLE: Load/unload from truck, support to assist in towing
   5) Maintenance support
      EXAMPLE: Testing procedures, repair confirmation, repositioning, equipment operation during maintenance
   6) Vehicle testing, even if not normally exposed to end customer
      EXAMPLE: Normal driver inadvertently activates vehicle testing mode via an unrecorded sequence of control manipulations
   7) Any use of manual controls, including detachable manual controls
      EXAMPLE: Plug-in vehicle control console, mobile phone control app
   8) Responsibilities following collision, loss event, incident
      i) Rendering aid and assistance
      ii) Summoning emergency assistance
      iii) Exchange of information
      EXAMPLES: Contact information, insurance information, license, registration

b) Safety argument for mode change to human driver mode including for each mode:
   1) Criteria for entering non-autonomous mode
   2) Criteria for changing between modes
   3) Criteria for entering for autonomous mode
   4) Responsibilities of human in initiating and confirming mode change
   5) Hazard mitigations that are inactive when in non-autonomous mode (i.e., the risk mitigation for which responsibility is assigned to the human driver)

c) Faulty mode change attempts
   EXAMPLES: Mode confusion in human, disagreement regarding active mode among autonomous item components

d) Mode change operations not commanded by and/or unexpected by a human driver
e) Hazards in fully autonomous mode caused by controls intended for other, non-fully-autonomous modes
   EXAMPLE: Passenger unqualified to drive bumps a pedal control without realizing it, initiating an unexpected transition to manual driving mode.
f) Mitigation for unexpected safety related behaviors during and immediately after mode change
   EXAMPLES: Unexpected vehicle motion, human controls do not match current vehicle state

7.7.1.3 HIGHLY RECOMMENDED:

a) Human accepting responsibility for ensuring safety is actually capable of assuming that responsibility and can reasonably be expected to do so when the transfer of responsibility occurs.
   NOTE: The complexities of this topic are significant, but details beyond recognizing it as a potential hazard are beyond the scope of this standard.

7.7.1.4 RECOMMENDED – N/A

7.7.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, and demonstration.

7.7.1.6.1 NOTE: Whether a human is physically present or tele-present does not affect whether the human is performing or supervising the dynamic driving task. (This does not mean that remote vs. local human operation of a vehicle is identical.)

7.7.1.6.2 NOTE: Safety of vehicle with human performing the dynamic driving task is beyond the scope of this standard. However, the safety of mode changes, including transition into and out of a human-operated mode is within scope. For example, risk due to an undesired transition into human controlled driving mode during autonomous vehicle operation (e.g., for a moving vehicle if the responsible human driver is asleep) is within the scope of this standard. Similarly, ensuring that a transition from human control to autonomous mode is done safely from the point of view of the vehicle is within the scope of this standard. However, methods for determining whether a human driver is competent to assume control and human interactions for how to safely hand over control are beyond the scope of this standard.

8 Autonomy Functions and Support

8.1 General autonomy pipeline

8.1.1 Hazards related to autonomy have been identified and mitigated.

8.1.1.1 MANDATORY:

a) Identify all hazards related to autonomy. If none, so state.
b) Autonomy-related implications of the ODD (See Section 8.2)
c) Sensing (See Section 8.3)
d) Perception (See Section 8.4)
e) Algorithms (See Section 8.5)
f) Planning (See Section 8.6)
g) Prediction (See Section 8.7)
h) Item trajectory and item control (See Section 8.8)
i) Actuation (See Section 8.9)
j) Timing (See Section 8.10)

8.1.1.2 REQUIRED:

a) Mitigate identified autonomy-related hazards

8.1.1.3 HIGHLY RECOMMENDED – N/A

8.1.1.4 RECOMMENDED – N/A

8.1.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.1.1.6.1 NOTE: The general organization of this autonomy section follows a common way to break down the different pieces of an autonomous item functional “pipeline.” However, there is no requirement that the item itself be architected this way so long as clauses are addressed.

8.1.1.6.2 NOTE: “Relating to autonomy” is intended to be read broadly, including but not limited to: a hazard that is caused by autonomy; a risk that is claimed to be mitigated by autonomy; and a risk mitigation measure that can be undermined by autonomy.

8.1.1.6.3 NOTE: Hazard mitigation strategies which involve non-autonomous functionality taking full responsibility for mitigation might not need to conform to the autonomy requirements.

8.1.2 The architecture and theory of operation for autonomy and strategy for safety of autonomous functionality shall be described.

8.1.2.1 MANDATORY

a) Overall theory of operation of autonomy and strategy for safety including principles of safe operation

b) Description of architecture
    1) Functions
    2) Components
    3) Redundancy strategy
    4) Coupling of autonomy pipeline (or other autonomy approach) stages
    5) Interfaces to other item functions and components
c) Description of Operational Design Domain (ODD)
    1) Methodology for defining
    2) Intended ODD
    3) ODD subdivision, if any
    4) Detecting ODD violations
d) Description of Sensing
    1) Sensing components
    2) Preprocessing done by sensors
    3) Interface to other components
    4) Sensor fusion approach
e) Description of Perception
    1) Conversion of sensor data to objects
    2) Object classification
    3) Identification of overall state as within or outside of ODD
f) Description of Planning
    1) Route planning
    2) Trajectory creation
g) Description of controls and actuation
    1) Trajectory execution
    2) Motion control
    3) Feedback to planning

8.1.2.2 REQUIRED:

a) Description of prediction approach used, if any
b) Description of Machine Learning (ML) approach, if any
    1) Data selection
    2) Data cleaning
    3) Algorithm selection
    4) ML architecture selection
    5) Model training approach
c) Performance metrics

8.1.2.3 HIGHLY RECOMMENDED – N/A

8.1.2.4 RECOMMENDED – N/A

8.1.2.5 CONFORMANCE:

Conformance is checked by inspection of a record containing the required topics.

8.1.2.6.1 NOTE: In practice this clause is intended to result in the creation of a Theory of Operation Manual for the autonomous aspects of the item that contains enough detail for the assessor to perform an informed assessment. Each aspect of autonomy noted is described in a way that can be understood by the assessor at a high enough level of abstraction that it can be used without reference to the details of the safety case. (Simply pointing to the autonomy argument structure to meet this clause is generally unacceptable, but portions of the argument can provide supporting details.) Adaptations in organization of topics may be made to conform to the system architecture, but all noted aspects of the item need to be addressed in a relevant manner.

8.2 Operational Design Domain (ODD)

8.2.1 The Operational Design Domain (ODD) shall be defined in an acceptably complete manner.

8.2.1.1 MANDATORY:

a) An acceptably complete ODD definition with traceability to ODD-dependent aspects of the safety case.
b) Argue that the item is safe within the ODD
c) Argue that the item is safe when the ODD has been exited
   EXAMPLE: A fault mitigation maneuver might exit the ODD intentionally, or a change in environment might force an unexpected ODD exit

8.2.1.2 REQUIRED:

a) Inclusion of environmental factors (See section 8.2.2)
b) Use of a defined scenario description language

8.2.1.3 HIGHLY RECOMMENDED:

a) Use of positive enumeration of ODD aspects
   EXAMPLE: ODD includes dry pavement, sunny days
b) Use of negative enumeration of ODD aspects
   EXAMPLE: ODD excludes operation during frozen precipitation events
c) Identification how ODD aspects which are covered by neither positive nor negative enumerations are handled
   EXAMPLES: Any situation not included in a positive enumeration list is considered an ODD violation; any situation not included in a negative enumeration list is considered a valid ODD, potentially with significant operational restrictions if not on a positive ODD enumeration list.

8.2.1.4 RECOMMENDED – N/A

8.2.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.2.2 The ODD shall cover relevant environmental aspects in which the autonomous item will be operating.

8.2.2.1 MANDATORY:

a) Documented definition of the ODD and relevant subsets including coverage of safety aspects
   NOTE: Generally this is expected to take the form of an ODD taxonomy.
b) Travel infrastructure
   EXAMPLES: Types of road surfaces, road geometries, bridge restrictions
c) Object coverage (i.e., objects defined as being within ODD)
d) Event coverage
   EXAMPLES: Interactions with infrastructure and other objects
e) Behavioral rules
   EXAMPLES: Traffic laws, vehicle path conflict resolution priority, local customs, justifiable rule breaking for safety
   NOTE: Ethical handling of behavioral rules might need to be coded in the AI itself implicitly or explicitly, and that encoding might result in behaviors that may be in violation of traffic rules.
f) Environmental effects
   EXAMPLES: Weather, illumination
g) Operational condition of item
   EXAMPLE: Temporary or permanent degradation of ego vehicle equipment
h) Operational duration
   EXAMPLE: Mission length, expected system operational life

8.2.2.2 REQUIRED:

a) A description of the strategy and the organization of any use of multiple ODDs or ODD subsets, if applicable.
b) Vulnerable populations
   EXAMPLES: Pedestrians, motorcycles, bikes, scooters, other at-risk road users, other road users
c) Support infrastructure, if any is relied upon
   EXAMPLES: Types of traffic signs, travel path geometry restrictions, other markings
d) Localization support, if relied upon
   EXAMPLES: GNSS availability, types of navigation markers, DSRC, other navaids
e) Compliance strategy of traffic rules and regulations
   EXAMPLE: Enumeration of applicable traffic regulations and corresponding ego vehicle behavioral constraints

f) Special road user rules, if applicable
EXAMPLES: Bicycles, motorcycles/lane splitting, interacting with construction vehicles, oversize vehicles, snowplows, sand/salt trucks, emergency response vehicles, street sweepers, horse-drawn vehicles
See Also Section 7.5.

g) Road obstructions
EXAMPLES: Pedestrian zone barriers, crowd control barriers, police vehicles intentionally blocking traffic, post-collision vehicles and associate debris, other road debris, other artificial obstructions

h) Operation across jurisdictional boundaries
EXAMPLES: Crossing time zone boundaries, crossing jurisdictions with different traffic rules, crossing national borders (customs and immigration controls), crossing agricultural control boundaries that prohibit transit of specific cargos, transiting other checkpoints

i) **Pitfall:** An ODD taxonomy defined by human analysis is prone to omitting aspects of the ODD that are learned by a machine-learning based perception subsystem.
EXAMPLES: An ODD does not include light haze in its definition since it is not visually perceptible by humans. However, light haze confounds the perception subsystem.

8.2.2.3 HIGHLY RECOMMENDED:

a) Seasonal effects
EXAMPLES: Foliage changes (e.g., leaves appearing), sun angle changes, seasonal behavioral patterns (e.g., summer beach traffic), seasonally-linked events (Oktoberfest, regatta crowds, fireworks gatherings, air shows)

b) Other relevant factors
EXAMPLE: Coefficient of friction ranges of road surface

c) Traceability from each aspect of the ODD to affected safety case elements

d) Strategy for organizing the ODD into ODD subsets
NOTE: Using ODD subsets is highly recommended, not required. However, if ODD subsets are in fact used, a number of REQUIRED prompt elements then come into play

8.2.2.4 RECOMMENDED – N/A

8.2.2.5 CONFORMANCE:

Conformance is checked via inspection of ODD definition and V&V evidence as it relates to ODD traceability.

Reference: Singapore Standards Council TR 61 Part 1: 2019.

8.2.3 ODD violations shall be handled in an acceptably safe manner.

8.2.3.1 MANDATORY:

a) Identify strategy for detecting when item is within bounds of the ODD

b) Identify strategy for risk mitigation while transitioning out of the ODD

8.2.3.2 REQUIRED:

a) Detect a departure from the ODD

b) Defined behavior when exiting and operating outside defined ODD
c) Ensure acceptable risk mitigation for defined outside-ODD behavior
d) If ODD subsets are defined:
    1) Strategy for risk mitigation while transitioning between ODD subsets
    2) Detect a departure from each defined ODD subset
    3) Ensure acceptable level of safety despite departure from each defined ODD subset
    NOTE: This includes both transitions between ODD subsets and transition outside the entire ODD.
    4) Detect and react to a change of conditions that requires transitioning to a different ODD subset
    EXAMPLES: Shifts in distribution means of detected objects, weather changes, lighting changes
    5) Define and handle ODD subset transition factors
    EXAMPLES: Geopolitical borders, weather changes, temporary road hazards
e) **Pitfall:** The characterization of an ODD is prone to change due to forces outside the item's control
    EXAMPLES: Addition of a new road sign type, geographically novel weather patterns, changes in road use regulations and local customs
    See also Section 8.2.4.

8.2.3.3 HIGHLY RECOMMENDED:

a) Identification of objects and events generally known, but not within a defined ODD or ODD subset
    EXAMPLES: Novel road markings, novel road signs, non-indigenous animals
b) Timing requirements of recognizing and reacting to ODD transitions and violations

8.2.3.4 RECOMMENDED:

a) Consideration of role of V2x in characterizing ODD and detecting ODD departures
b) Consideration of role of GNSS in characterizing ODD and detecting ODD departures

8.2.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration of ODD departure and transition behaviors.

8.2.3.6.1 NOTE: ODD departure can occur when any assumptions, constraints, or conditions are encountered that are not covered by the ODD definition. ODD departure could occur due to a requirements defect in describing the ODD (e.g., an object type that is legitimately found in the intended ODD was unintentionally omitted from vehicle training data). Some ODD departures can be involuntary through no fault or action of the item (e.g., unexpected weather).

8.2.3.6.2 NOTE: The item might have different behaviors and even a significantly different design for different subsets of the overall item ODD. Each requirement for the ODD overall applies to each ODD subset individually.

8.2.4 Changes to the ODD shall be detected and tracked to resolution.

8.2.4.1 MANDATORY:

a) Identify strategy for detecting safety related changes to ODD, including:
    1) New vehicles, elements, characteristics, behaviors, objects and other ODD aspects
    2) Modifications to characterization of ODD
    EXAMPLES: Change in frequency of safety related behaviors, safety related change in distribution of object types
b) Identify data monitoring source for each type of identified change
EXAMPLES: Road monitoring, mapping service provider, governmental agency
c) ODD model subject to configuration management and version control

8.2.4.2 REQUIRED:

a) Detect and track ODD changes to resolution
b) Define quality assurance approach to external data sources related to ODD change detection, addressing at least:
    1) Accuracy of change data
    2) Changes missing from data sets
    3) Data integrity
    4) Timeliness

8.2.4.3 HIGHLY RECOMMENDED:

a) ODD aspects that are no longer part of the ODD
EXAMPLE: Obsolete traffic signal types retired from service
NOTE: This statement is with regard to the expected occurrence of some aspect of the ODD no longer being expected. It might still be possible for that aspect to occur, but it is then treated as an ODD departure or ODD violation that is outside the intended ODD.

8.2.4.4 RECOMMENDED:

8.2.4.5 CONFORMANCE:

Conformance is checked via demonstration as well as inspection of design and validation evidence.

8.2.4.6.1 NOTE: Changes to the ODD are different from other safety related aspects of the system when they are not under the control of the item developer. Therefore, processes to detect ODD changes need to work in parallel with change management of the item and its design.

8.3 Sensing

8.3.1 The sensors shall provide acceptably correct, complete, and current data to the item in the context of the ODD.

8.3.1.1 MANDATORY:

a) Identify safety related sensors and sensor data and their role in providing data

8.3.1.2 REQUIRED:

a) Identify data quality requirements for acceptable operation, including:
    1) Accuracy
    2) Precision
    3) Resolution
b) Validation that sensor selection provides acceptable data quality
c) Mitigation of data quality issues in operation

8.3.1.3 HIGHLY RECOMMENDED:

a) Map ODD subsets to sensor degradation corresponding to operation within those subsets. (If ODD subsets are used)
    NOTE: See sensor degradation in Section 8.3.5. This item is to encourage mapping of degradation to each ODD subset, if subsets are used.

8.3.1.4 RECOMMENDED – N/A

8.3.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.3.1.6.1 NOTE: The general idea is that sensors provide information from which the item can build a model of the current state of the external world. Some of that data goes through perception (e.g., for detecting objects), while other data is used more directly (e.g., external temperature).

8.3.2 Calibration, data filtering, data processing and data identification techniques shall result in acceptable sensor performance within the defined ODD.

8.3.2.1 MANDATORY:

a) Description of approaches used for sensor data handling, including:
    1) Calibration
    2) Data filtering
    3) Data processing
    4) Anomalous data identification and handling
b) Description and evaluation of false positive vs. false negative trade off strategy

8.3.2.2 REQUIRED:

a) Calibration as it relates to:

1) Operations
2) Maintenance
3) Fault detection
4) Diagnostics
5) Scope of calibration to include physical mounting issues such as mounting bracket alignment, if applicable

b) Address each ODD subset (if ODD subsets are used)
c) Detection threshold (or other quantification) selection and validation of that threshold

8.3.2.3 HIGHLY RECOMMENDED:

a) Describe reliance upon temporal data filtering and potential hazards
EXAMPLES: Smoothing, ride-through of transient missed detections
b) Field engineering feedback data in support of detection threshold (or other quantification) acceptability
NOTE: Thresholds might need to change due to changing operational conditions, vehicle equipment aging, or other factors
c) **Pitfall:** Improvement of detection capabilities via filtering, data smoothing, or other similar techniques is prone to masking the possibility of future failures when filter time constants are violated.
EXAMPLE: Consider a safety argument that detection capabilities are acceptable with detection misses for up to 2 consecutive frames compensated via a tracking-based ride-through approach. This approach is prone to failing when 3 consecutive frame misses occur.

8.3.2.4 RECOMMENDED – N/A

8.3.2.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence.

8.3.2.6.1 NOTE: Data includes images, video streams, radar samples, inertial movement sensors, conventional vehicle sensors, and other sensor data

8.3.2.6.2 NOTE: The concept of sensor “damage” includes loss of calibration to the point that the sensor no longer satisfies assumptions made in the safety case. Therefore, calibration may trace to aspects of the safety case that are affected by sensor malfunction, degradation and damage. Calibration includes, but is not limited to, internal sensor calibration requirements, mounting requirements (e.g., physical alignment with item geometry), and relationship with other vehicle components (e.g., vehicle headlight brightness and spectral content as it relates to camera sensitivity to the illuminated scene).

8.3.3 Sensor fusion and redundancy management techniques, if necessary, shall result in acceptable sensor performance for the defined ODD.

8.3.3.1 MANDATORY:

a) Description of approaches used for sensor redundancy management and data fusion
NOTE: The redundancy approach might be that no redundancy is required.

b) Acceptable net sensor performance
EXAMPLE: Arguments considers whether the outputs of a sensor fusion algorithm providing acceptable ability to detect and classify.
c) Handling of safety related false negatives

8.3.3.2 REQUIRED:

a) Fusion of multiple instances of same sensing modality
b) Fusion of different sensor modalities
c) Conflict resolution for conflicting sensor data
    1) Sensor prioritization
    2) Voting, including any use of m-of-k strategies
d) Handling of safety related false positives from each sensor
e) **Pitfall:** Inconsistent voting and/or prioritization arguments are prone to missing sensor fusion problems
EXAMPLE: An inconsistent argument would be arguing both that multiple sensors vote to reduce false positives while also arguing in the same context that a detection on any single sensor is used to avoid false negatives. A more consistent argument that a 2 out of 3 sensor agreement approach is used to manage both false positives and false negatives.

8.3.3.3 HIGHLY RECOMMENDED:

a) Path dependencies, prioritization of sensing modes, and other sensor interactions on sensor fusion data flow
EXAMPLE: Consider a vehicle in which a radar is used to detect an object and a narrow-field camera is subsequently used for classification of the object detected by the radar. Assuming this is the entire set of sensors, if the radar fails to detect an object, then credit cannot be taken for camera-based sensor diversity because the camera will never be directed to look at the object.

8.3.3.4 RECOMMENDED – N/A

8.3.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

8.3.3.6.1 Note: The system architecture (e.g., early fusion vs. late fusion) will affect the argument. A clearly articulated strategy for sensor fusion and redundancy management in an overall item description is helpful in understanding the argument.

8.3.4 Any credit taken for sensor diversity and/or redundancy shall be justified.

8.3.4.1 MANDATORY – N/A

8.3.4.2 REQUIRED:

a) Identification strategy for sensor diversity and/or sensor redundancy
b) Quantitative support for overall sensor diversity, redundancy, and fusion strategy providing acceptably capable detection

NOTE: Quantitative analysis justifies the sensor diversity select, even if the result is use of a single sensor item

c) Identify relevant diverse properties of redundant sensors
    1) Operating spectra
    2) Noise sources
    3) Environmental limitations

EXAMPLES: Detection range and angular coverage for each type and instance of radar, LIDAR, ultrasonic sensor, visible light camera, and IR camera used.

EXAMPLES: Geometric coverage overlaps of sensor types and sensor instances

NOTE: Consider both placement diversity and operational mode diversity if different modalities are used.

NOTE: Vehicle operational speed, environmental conditions, roadway congestion, and other ODD factors as well as operational parameters may reduce effectiveness of sensor diversity strategies.

d) Coincident and common cause sensor failures

EXAMPLES: Blind spots, accumulated sensor degradation, expected joint arrival rates of statistically independent failures

e) Zonally correlated failures

EXAMPLES: Multiple sensors damaged by a single piece of road debris

See Also Section 10.3.

f) Other potential correlated sensor failures

EXAMPLES: Expected arrival rates of objects unlikely to be detected by multiple sensor instances/types, with quantitative support, including single sensors, pairs of sensors, etc.

g) **Pitfall:** Assumption of independent failures is prone to over-stating sensor fusion effectiveness

h) **Pitfall:** Blind spots due to vehicle geometry are prone to causing correlated sensor failures

EXAMPLES: Articulated vehicle pivot, underneath vehicle, in blind spots of parked vehicle about to start a mission

i) Traceability of sensor diversity and/or redundancy argument to operational environments and operational modes, including degraded vehicle modes and ODD subsets, if applicable.

j) Consideration of data sources when used as synthetic sensors or for sensor redundancy

EXAMPLES: High resolution maps used to augment navigation and infrastructure perception capabilities

k) Accounting for time constants of vehicle operation

EXAMPLE: Arguing that three detections in five samples is acceptable to identify an object could be invalid if in operation there is only time to collect three samples to meet response time requirements.

l) **Pitfall:** Existence of object and events that are difficult to sense via multiple sensing modalities is prone to causing correlated sensor failures.

EXAMPLE: Detached truck tire treads on a roadway might be difficult to detect with

LIDAR (rubber absorbs pulses), vision (black tire on black freshly paved black road surface), and radar (rubber with fabric belts combined with low profile in line of sight).

8.3.4.3 HIGHLY RECOMMENDED:

a) Field engineering feedback data mechanisms to detect precursor events
EXAMPLES: Detection and reporting of unanticipated sensor failure events that might indicate a novel correlation mechanism
b) Correlated and common cause degradation of capability even if outright sensor failures are not observed
EXAMPLE: Aging effects, reduced confidence, increased brittleness of detection accuracy
c) **Pitfall:** Common cause degradation source or zonal failures are prone to causing correlated sensor failures
EXAMPLES: Weather effects such as icing, mud splash, debris impact, electrical faults
d) **Pitfall:** Arguments that depends upon an assumption of within-ODD operation to argue sensor validity is prone to failing to detect ODD departures.
EXAMPLE: A limited-range detector might be unable to detect that an out-of-range situation has occurred due to an ODD violation that makes out-of-range detections safety related.

8.3.4.4 RECOMMENDED:

a) Sensor performance changes based on item operational mode, item component degradation, and operational environment

8.3.4.5 CONFORMANCE:

Conformance is checked via inspection of sensor characterization evidence, diversity/redundancy argument, and V&V evidence.

8.3.5 Risks resulting from potential sensor performance degradation shall be mitigated.

8.3.5.1 MANDATORY:

a) Analysis of effects of sensor degradation for each sensor based on sensor type, sensor location, and anticipated lifecycle operational environment.
NOTE: See also Section 8.3.4 for correlated sensor degradation across redundant and/or diverse sensors.
NOTE: Aggregating analysis for relevant characteristics of sensors of the same type is encouraged.

8.3.5.2 REQUIRED:

a) Detection of type and amount of sensor degradation to ensure that it is either within limits or item acceptably compensates for degradation
b) Consider at least the following:

1) Aging, wear-and-tear, non-catastrophic damage, loss of calibration.
   EXAMPLES: Lens discoloration, lens scouring, non-catastrophic debris impact damage
2) Environmental degradation that affects sensor performance
   EXAMPLES: Rain, haze, smoke, dust, glare, reflections, multi-path returns, mirages, EMC interference
3) Map degradation
   EXAMPLES: Staleness, incorrect data
   NOTE: For this purpose map information is considered a virtual sensor
4) Safety argument for sensor degradation corrective devices (if used)
   EXAMPLES: Wiper system, cleaning fluid system, sensor heater

8.3.5.3 HIGHLY RECOMMENDED:

a) Temporary sensor degradation that may be subject to in-mission or between-mission correction (if credit is taken)
   EXAMPLES: Accumulated precipitation, ice, dust accumulation, mud splash, bird droppings, bug splatter
   NOTE: If excluded from safety case, this may imply that all degradation is considered permanent.
b) Safety argument for sensor updates and adaptive functionality (if used)
   EXAMPLES: Automatic camera compensation for lens defects, automatic map updates
c) Validation of degradation models using field engineering feedback data
d) Traceability of degradation models to maintenance and inspection requirements
e) **Pitfall:** In the absence of effective field engineering feedback monitoring, unexpected sensor degradation is prone to occurring due to unanticipated effects
   EXAMPLES: Operational conditions, aging, wear and tear, vehicle abuse, sensor defects, and usage profiles
f) **Pitfall:** Supply chain issues are prone to compromising the integrity of critical support items
   EXAMPLE: Use of incorrect cleaning fluid composition results in frozen cleaning fluid in cold weather, resulting in a simultaneous failure of all sensor cleaning items

8.3.5.4 RECOMMENDED – N/A

8.3.5.5 CONFORMANCE:

Conformance is checked via inspection of design, V&V, demonstration, and field data evidence.

8.3.6 Sensor fault detection and fault management shall be acceptable.

8.3.6.1 MANDATORY:

a) Description of approaches used for fault detection and fault management
b) Acceptable fault detection, diagnosis and response
c) Covers permanent faults
d) Covers support systems including at least:

1) Electrical power
2) Thermal management

8.3.6.2 REQUIRED:

a) Calibration-related faults
b) Transient faults
   NOTE: If transient faults are not covered, then all faults have been assumed to be permanent.
c) Safety argument encompasses single and multiple accumulated as well as coincident sensor failures
   See also: Minimum Equipment List, Section 10.3.5.
d) Covers support systems including at least (if present):
   1) Fluid supplies
   2) Pneumatics
   3) Hydraulics
e) Built In Self-Test (BIST) functionality

8.3.6.3 HIGHLY RECOMMENDED:

a) Lifecycle data and field engineering feedback to improve fault models and failure rate predictions

8.3.6.4 RECOMMENDED – NA/

8.3.6.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence. Demonstration of transition to acceptable operational mode (e.g., safe state) for sensor failure(s).

8.3.7 Potential safety-critical faults due to active sensor emissions shall be traced to at least one hazard.

8.3.7.1 MANDATORY – N/A

8.3.7.2 REQUIRED:

a) Traceability of each identified hazard to potential sensor faults, if any
   See also: Hazard Identification, Section 6.2.1.
b) Vehicle operational behaviors (if active sensors are used)
   EXAMPLE: Eye safety concerns due to radar radiation while stopped at a crosswalk with small children in close proximity to vehicle
c) Maintenance, calibration, testing, and other non-operational environments (if active sensors are used)
   EXAMPLE: Eye safety concerns due to radar radiation while maintaining tires on service lift.
d) Trace assumptions regarding sensors in the safety case to sensor fault models
   EXAMPLE: Determination that LIDAR beam is eye safe because it is assumed that a rotational scanning device is operational

8.3.7.3 HIGHLY RECOMMENDED:

a) Equipment failures
EXAMPLE: Failure of beam scanning mechanism for laser that assumes scanning to ensure eye safe operation
b) Aggregated emissions from multiple deployed systems
EXAMPLE: Multiple active sensors from multiple vehicles direct emissions at a single spot of interest might negate an assumption that that only the emissions from a single vehicle need be considered when computing safe levels of energy emission

8.3.7.4 RECOMMENDED – N/A

8.3.7.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

8.3.7.6.1 NOTE: This clause is intended to capture issues relating to active energy emissions from active sensors that can cause hazards generally unrelated to their primary function (e.g., eye safety of emissions rather than whether the sensor correctly detects an obstacle).

8.4 Perception

8.4.1 Perception shall provide acceptable functional performance.

8.4.1.1 MANDATORY:

a) Identify safety related functions of perception system
b) Argue that perception system functions are acceptable

8.4.1.2 REQUIRED:

a) Identify acceptable performance characteristics, including the following:
    1) Perception latency
    2) False negative rate
    3) False positive rate
    4) Other relevant metrics, if any
NOTE: Relevant metrics may vary depending upon function performed and operating situation

8.4.1.3 HIGHLY RECOMMENDED:

a) Characterization of performance on safety related subsets of input space
EXAMPLE: False negative rate of humans in wheelchairs
b) **Pitfall:** Blanket performance data and metrics are prone to hiding situations in which an item fails in a small region of the ODD while working well in other regions
NOTE: An item that works perfectly in 99% of the ODD but malfunctions consistently in 1% of the ODD could be said to work 99% of the time, but might be unsafe essentially all the time in that 1% of the ODD if the failures are systematic rather than random.
EXAMPLE: Consider an item that has an elevated misclassification rate of construction workers in high visibility vests as non-humans, but classifies all other types of humans

with very high accuracy. Such a system would be biased toward potentially unsafe operation near construction workers.

8.4.1.4 RECOMMENDED – N/A

8.4.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.4.1.6.1 NOTE: Perception is used in a general sense, and might encompass aspects of the item such as object detection, classification, and prediction. Requirements placed upon perception are intended to apply to that functionality in general regardless of the label applied to particular architectural blocks.

8.4.2 A defined perception ontology shall provide acceptable coverage of the ODD.

8.4.2.1 MANDATORY:

a) A defined ontology of objects and events for the perception functionality
EXAMPLE: Produced as a result of feature engineering
b) Evidence that the ontology acceptably covers all safety related aspects of the ODD

8.4.2.2 REQUIRED:

a) Ontology mechanism for addressing objects and events encountered that are not explicitly in the ontology
b) Traceability of ODD subsets to subsets of the ontology (if ODD subsets are used)

8.4.2.3 HIGHLY RECOMMENDED:

a) Arguments that the ontology is acceptably fine grained because it enables acceptably accurate (or other relevant metric) behavioral prediction based on object or event classification

8.4.2.4 RECOMMENDED:

a) **Pitfall:** Multiple classification categories within the as-trained item that map to a single category in a human-designed ontology are prone to complicating test coverage assurance.
EXAMPLE: Consider an item that has many disjoint classification clusters that generally correspond to “normal pedestrian.” A human-designed test plan might only exercise obvious (to a human) clusters such as “adult” and “child” and credit the test plan for having thoroughly tested “normal pedestrian” scenarios. However, machine learning might have non-intuitive clusters that are entirely missed by the test plan, such as hypothetically “people with bare legs,” “people with no face visible,” and “people superimposed upon strong vertical edges in background.”

8.4.2.5 CONFORMANCE:

Conformance is checked via inspection of the ontology definition, inspection of evidence of ontology coverage, inspection of traceability to the ODD, and demonstration of correct classification according to the ontology.

8.4.2.6.1 Note: An acceptable ontology might include classifications, a set of labels that are applied, or some other way of designating the location and type of objects or events in sensor inputs. Depending upon the item, a human-friendly ontology of objects might not exist. However, a de facto ontology exists for any classifier, even if it is simply a flat list of classification bins. It is important to map the de facto ontology onto V&V activities to establish test coverage. A difficulty in V&V is that there effectively could be numerous essentially disjoint subsets of criteria that can each activate a particular classification outcome, and it can be difficult to know whether each such subset has been exercised. (For a deep neural network this can require reverse engineering operation to achieve test coverage, although this statement is not intended to specifically require such activity).

8.4.3 Perception shall map sensor inputs to the perception ontology with acceptable performance.

8.4.3.1 MANDATORY:

a) Description of method for and results from evaluating perception performance
   NOTE: Effectiveness in this context is ability to correctly map sensor inputs onto the perception ontology. Performance includes both effectiveness and speed.
b) Evaluation of performance on field data that has not been used in the machine learning design and training process
c) Coverage analysis of field test data with respect to the ODD

8.4.3.2 REQUIRED:

a) Repeatability of perception performance in context of statistical analysis of performance
b) Lack of errors, biases, or other problems due to preprocessing steps, if used
c) Acceptably low incidence of mislabeled training and validation data
d) Acceptable handling of objects and events that are not in the ontology
e) Acceptable data sanity (i.e., data comes from a properly synchronized and calibrated sensor suite compatible with the deployed vehicle sensors that is acceptable for scenario reconstruction)
f) Acceptable data quality (i.e., training data is acceptably faithful representation of the data distribution required to acceptably train the item)
g) Justify setting of Threshold (probability) values for classification (if used)
h) Coverage analysis of field test data with respect to ODD subsets, if used
i) **Pitfall:** Using accuracy as a primary metric is prone to giving false confidence in performance when applied to imbalanced data sets and/or when it discounts rare but high severity situations

8.4.3.3 HIGHLY RECOMMENDED:

a) Calibrating classifiers or using alternate methods to result in classification confidence being a close approximation of probability of correct classification in field operation
b) Use of suitable quantification approaches, including: (as acceptable at least one of)
    1) Receiver Operating Characteristic (ROC) curve characterization and validation
    2) Precision Recall curves
c) Validation using objects and events intentionally outside the ODD to determine item response
    EXAMPLE: Classification results when an object excluded from ODD is encountered to determine if it is classified as “unknown” or is incorrectly classified as a within-ODD object

8.4.3.4 RECOMMENDED – N/A

8.4.3.5 CONFORMANCE:

Conformance is checked via inspection of design, V&V evidence, performance assessment evidence, as well as demonstration.

8.4.3.6.1 NOTE: In the case that perception is based on machine learning, then machine learning related requirements described in other subsections apply, and in particular perception robustness.

8.4.3.6.2 NOTE: This clause intentionally places an architectural limitation upon the item in that mapping of perception results to an ontology must be observable. This can preclude the use of end-to-end machine learning that has not been designed to provide such observability. Defining validation criteria for end-to-end machine learning approaches is out of scope for this standard.

8.5 Machine learning and “AI” techniques

8.5.1 The safety case shall argue that any machine learning based approach and other “AI” approaches provide acceptable capabilities.

8.5.1.1 MANDATORY – N/A

8.5.1.2 REQUIRED:

a) Identification of the use of any machine learning, statistical analysis approaches, and other similar approaches for safety-related functionality (if used)
b) Identification of any other “AI” algorithmic approaches for safety-related functionality (if used)
    EXAMPLES: Rule-based items, non-machine learning perception algorithms
c) Integrity of identified algorithmic design and implementation
    NOTE: This is intended to cover the correctness of design and implementation of the underlying algorithms to a suitable integrity level independent of the argument of the integrity of the data being processed by the underlying algorithms.
    See also: Section 6.2.2, Section 9.

d) Appropriateness of algorithmic selection
e) Acceptability of performance
   See also: Sections 8.5.2-8.5.6.
f) **Pitfall:** Arguments that system level risk will be acceptable on average over a timeframe rather than at initial release due to reinforcement learning or other system adaptations are prone to incorrectly representing the actual outcome of system level risk at initial deployment.
   EXAMPLE: The argument that a certain level of system level risk is acceptable is based on an average risk prediction over a 12 month deployment. That average risk includes an initial period of otherwise unacceptable (but not specifically stated) high risk that is claimed to be offset by downstream reduced risk as a result of “fleet learning” and other feedback mechanisms. However, risk improvement does not occur as quickly as expected in real world operations, revealing that the initial release based upon speculative risk assessment was in fact not acceptably safe.
   NOTE: A justification based upon risk improvement over time is not necessarily invalid from a societal point of view. However, possible improvement over time is speculative. This Pitfall is intended to encourage an explicit discussion of expected system level risks, including a statement of system level risk at time of release. That target itself can be justified by a risk improvement argument, but it is improper to use an improvement argument to evade explicit statements regarding system level risk at time of release.

8.5.1.3 HIGHLY RECOMMENDED – N/A

8.5.1.4 RECOMMENDED – N/A

8.5.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.5.1.6.1 NOTE: The scope for use of machine learning is during item design, item operation, or any other safety related function or activity.
EXAMPLES: A deployed system that incorporates a deep neural network with fixed weights during operation is the result of a machine-learning-based design process. A system design approach that uses a machine-learning-based approach to generating tests is using machine learning.

8.5.1.6.2 NOTE: Subsection items within Section 8.5 are only relevant if machine learning has been used in a safety related way. This includes both use of machine learning at run-time as well as use of machine learning in design, code generation, training data creation, or other aspects of the design and validation process. If an architectural pattern is used that renders machine learning completely unrelated to safety, or if machine learning is not used at all, then that may be an acceptable rationale for safety case deviation.

8.5.2 The machine learning architecture, training, and V&V approach shall provide acceptable machine learning performance.

8.5.2.1 MANDATORY – N/A

8.5.2.2 REQUIRED:

a) Description of machine learning techniques used
EXAMPLE: Training technique, use of transfer learning
b) Description of machine learning architecture and hyperparameters
EXAMPLE: Type of network, number of layers
c) Definition of performance metrics and evaluation against those metrics
EXAMPLES: ROC curves, false positive rate, false negative rate, precision/recall
d) Traceability of performance metrics to argument that performance is acceptable
e) Arguments that V&V procedure follows best practices for machine learning
f) Evidence of suitable engineering rigor in the use of tools and techniques that are safety related
EXAMPLE: Tools supporting collection and analysis of test data, tool support for neural network weight configuration management
See also: Section 13.
g) **Pitfall:** Machine learning techniques are generally prone to overfitting, resulting in lower than expected performance in real world operation.
h) **Pitfall:** The validity of machine-learning-based technology or artifacts that are validated using other machine learning techniques is prone to having the validity undermined by a lack of confidence in the machine learning validation technique.
EXAMPLE: A machine learning based tool is being used to generate test data sets to validate a machine learning based system component. This leaves open the question of whether the test generator itself is acceptable.
NOTE: Even if confidence of the validation technique is independently established, the interactions between the two machine learning systems (e.g. introduction of communication of bias) need to be addressed when considering the quality of the validation results.

8.5.2.3 HIGHLY RECOMMENDED:

a) Suitability of machine learning technique and architecture to functionality
b) Evidence that item has not directly or indirectly learned aspects of the validation data set after iterated training data improvement and retraining.
See Reference: Beizer, B., “The Pesticide Paradox,” Software Testing Techniques, 1990
c) Comparison of predicted item performance to deployed performance
d) Calibration of classifier performance so that divergence between reported confidence and probability of correct classification is actually indicative of distributional shift
NOTE: In practice, a confidence metric based on training and validation data sets can diverge significantly from the probability of correct classification on data not contained in the training and validation data sets. One use of confidence is to detect ODD violations

via distributional shift. However, that distributional shift metric might not be valid on data beyond the training and validation data sets, potentially undermining the validity of distributional shift metrics.

8.5.2.4 RECOMMENDED:

a) **Pitfall:** Traditional “confidence” values are prone to violating intuitive uses of that word when the item is operating with field data vs. training/validation data sets.
NOTE: Unless “confidence” has been successfully calibrated, other metrics should be used to assess the probability of correct performance in the real world.

8.5.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

8.5.2.6.1 NOTE: It is understood that the set of accepted practices for machine learning validation is a moving target due to continued evolution of the technical area. New practices should be adopted and incorporated into the safety case within a reasonable period of time.

8.5.2.6.2 NOTE: Performance encompasses full range of functionality, and not just speed.

8.5.2.6.3 NOTE: See perception topic for further evaluation criteria and practices. This Section 8.5.2 applies to perception to the extent that perception uses machine learning-based techniques.

8.5.3 Machine learning training and V&V shall use acceptable data.

8.5.3.1 MANDATORY – N/A

8.5.3.2 REQUIRED:

a) Overall description of data qualification approach to ensuring data is acceptable
b) The type and quantity of data used for machine learning training and testing ensure acceptable performance across the entire ODD, addressing at least the following points:
    1) Safety related aspects of the ODD are substantively represented in the data
    2) Evaluation metrics account for required risk mitigation
    EXAMPLE: Events with low probability but high severity for failure are properly handled, despite being a very small fraction of expected real world data.
c) Data provenance: historical record of data and its origins
NOTE: This can support better understanding of data, track back sources of errors, and provide auditability and quality trails
d) Suitability analysis and control of training data collection and management to ensure that it accurately reflects the ODD
e) **Pitfall:** Random data selection, unintended biases in data collection, and data collection gaps are prone to resulting in substantive portions of the ODD not being represented acceptably with training and validation data
f) Arguments that machine learning training and testing has acceptable integrity, including:
    1) Data collection equipment has acceptable level of integrity

2) Preprocessing of data, data storage, and data retrieval does not unduly degrade data integrity
3) Data integrity assurance includes configuration management and version management
4) Data management tools and machine learning tools have an acceptable level of integrity
See also: tool assurance in Section 13.

g) Analysis of testing and deployment failures to detect data collection issues

8.5.3.3 HIGHLY RECOMMENDED:

a) Traceability of training and testing data to ODD coverage
1) Performance metrics applied at a fine grain level in addition to at an aggregate level
EXAMPLE: Performance metrics are considered per object type and weather condition for perception.
2) Statistically valid data collection from the ODD
b) Compatibility of data quality across data collection, training, validation, and operations
EXAMPLE: Different sensor suites used for data collection vs. operations could compromise operational performance.
c) Accounting for differences in individual sensors
EXAMPLE: Each vehicle has slightly different sensor characteristics even when properly calibrated, potentially resulting in different machine learning based algorithm performance
d) **Pitfall:** The arrival of novel objects and events in collected data could have a heavy-tail distribution on a per-novelty basis, which is prone to invalidating naïve statistical assumptions
e) Testing and analysis directed at identifying data collection gaps
f) Testing directed at exercising capability to determine ODD departure
g) Biases and faults in collected data identified and addressed
EXAMPLE: Training data collected via monitoring a human driver’s actions in a non-automated vehicle who was driving unsafely
h) Data covers relevant operational modes, including degraded modes
i) Data integrity assurance
REFERENCE: Data Safety Initiative Working Group guidance (DSIWG, Data Safety Guidance v. 3.1, SCSC-127D, Feb. 2019)

8.5.3.4 RECOMMENDED:

a) **Pitfall:** Test plans created by humans might not exercise internal-to-machine learning algorithm edge cases, and are prone to incomplete coverage

8.5.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

8.5.3.6.1 NOTE: Machine learning validation includes not only testing, but also assuring correctness, completeness, and provenance of training and testing data.

8.5.4 Machine learning-based functionality shall be acceptably robust to data variation.

8.5.4.1 MANDATORY – N/A

8.5.4.2 REQUIRED:

a) Description of method for and results from evaluating functionality robustness of machine learning-based aspects of item
    1) Mitigation of risks due to any lack of robustness
b) Description of method for and results from evaluating response to distributional shifts
    1) Mitigation of risks due to distributional shifts of data
c) Field engineering feedback regarding performance when “surprises” have been encountered
   EXAMPLE: Classification results when encountering something in the real world that has been intentionally omitted from the perception ontology for testing purposes and/or inserted in the real world as a test.
d) **Pitfall:** Machine learning is prone to overfitting to training data in ways that are not obvious until a robustness testing campaign has been run to expose brittleness

8.5.4.3 HIGHLY RECOMMENDED:

a) Test performance for diverse environmental conditions within the ODD and determine which conditions result in weak performance
b) Data alteration via simulation, modification of recorded data, and/or modification of streaming data:
    1) Photo-realistic modification (and analogous modification for radar, LIDAR, etc.), where applicable
    2) Changes in contrast, attenuation, and other global data sensor characteristics, where applicable
    3) Positional, size, rotation, and other transformations, where applicable
    4) Other sensor data modification that reveals perception weaknesses, where applicable
    5) Other noise-based modification
c) **Pitfall:** Classification items are prone to incorrectly classifying novel inputs as known detections rather than as unknowns
   NOTE: “Novel” inputs are inputs representing classes of objects and other objects of potential interest not in the training and validation data set.

8.5.4.4 RECOMMENDED – N/A

8.5.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

8.5.4.6.1 Note: Use of adversarial sensor modification (i.e., a malicious attack involving reverse engineering the perception item) should be considered if called for by the security plan. Non-adversarial robustness testing approaches are acceptable for use to uncover safety related

perception brittleness that is relevant to the defined ODD and defined security model, even if adversarial data modification is out of scope of the security plan.

8.5.5 Post-deployment changes to machine learning behavior shall not compromise safety.

8.5.5.1 MANDATORY – N/A

8.5.5.2 REQUIRED:

a) Description of any planned or actual post-validation and post-deployment changes to machine learning operation
   EXAMPLES: Weight adjustments, retraining, configuration changes
b) Strategy for identifying sufficiently large change to machine learning to require revalidation of the affected aspect of the item.
   NOTE: In the absence of a well-defined methodology for impact analysis on machine learning training data changes, this might require significant revalidation effort after every change.
c) Argue that field data used to supplement machine learning data sets is at an acceptable level of integrity
d) **Pitfall:** Modifying machine learning behavior via reinforcement learning is prone to invalidating the safety case.
   EXAMPLE: Reinforcement learning that changes item behavior after deployment and/or between validated updates can result in an unsafe item. A possible mitigation is enforcing a safety envelope around the machine learning behavior to ensure that modified behaviors do not result in increased risk.

8.5.5.3 HIGHLY RECOMMENDED

a) Field data used to supplement machine learning data sets is at least at the same level of integrity as the data used to originally train that machine learning based functionality

8.5.5.4 RECOMMENDED – N/A

8.5.5.5 CONFORMANCE:

Conformance is checked via inspection of design and field engineering feedback processes.

8.5.5.6.1 NOTE: It is important to continually revalidate machine learning based functionality that is continually updated based on experience. This clause envisions that revalidation (i.e., update and re-assessment of the safety case) is done after a sufficiently large change to machine learning functionality. However, and alternate approach that is also acceptable within this standard might be to have a fixed functionality safety checker that mitigates the risk of updated machine learning functionality acting in an unsafe manner.

8.5.6 The safety case shall address the acceptability of any other "Artificial Intelligence" ("AI") techniques used beyond machine learning.

8.5.6.1 MANDATORY – N/A

8.5.6.2 REQUIRED:

a) Identify and describe other AI techniques being used, if any
b) Argue that each used AI technique provides acceptable capabilities

8.5.6.3 HIGHLY RECOMMENDED:

a) Address non-deterministic aspects of AI technique
b) Address validity and coverage of any heuristics used
c) Address adherence to best practices for employing each technique
d) Identify and argue mitigation of potential hazards, and risks

8.5.6.4 RECOMMENDED:

a) To maximum extent practicable, rely upon traditional software safety argument approaches

8.5.6.5 CONFORMANCE:

Conformance is checked via inspection of the safety case.

8.5.6.6.1 NOTE: This clause is intended as a catch-all for non-machine-learning and heuristic techniques that are applied, such as expert items and classical non-machine-learning perception algorithms. It is intended to provide a starting framework for other techniques analogous to Sections 8.5.1 through 8.5.5.

8.6 Planning

8.6.1 The safety case shall argue that planning capabilities are acceptable.

8.6.1.1 MANDATORY:

a) Description of strategy and algorithms for planning
   NOTE: Use of an instantaneous response without constructing an explicit plan is still a strategy for planning.
b) Argue that planning is acceptable

8.6.1.2 REQUIRED – N/A

8.6.1.3 HIGHLY RECOMMENDED – N/A

8.6.1.4 RECOMMENDED – N/A

8.6.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.6.1.6.1 NOTE: Depending upon the specifics of the item, planning will generally include path planning, but might additionally include other types of planning.
EXAMPLES: Movement planning for an attached robot arm that loads cargo, clearance for an automatic door that is intended to avoid hitting obstacles when opening, launch space clearance requirements for a last-few-meters delivery UAV operating in tandem with an autonomous delivery truck.

8.6.2 The planning approach shall be documented.

8.6.2.1 MANDATORY:

a) Strategy, calculation approach, and design for obstacle avoidance algorithms
EXAMPLES: Static objects such as roadway debris; unusual vehicle operations (e.g., slow moving street sweeper, on-scene fire truck, on-scene tow truck performing extrication); dynamically configured objects such as drawbridges.
b) Strategy, calculation, and design for generating safe and feasible control actions
EXAMPLES: Accounting for item stability, panic stops, occupant safety

8.6.2.2 REQUIRED:

a) Describe interrelationship between planning and prediction
See also Section 8.7.
b) Describe relationship of perception to categorization of obstacles
EXAMPLES: Obstacles categorized as must not hit, can hit if necessary, not an obstacle
c) **Pitfall:** Failure to account for controllability (i.e., ability of the item to follow a specified path) is prone to resulting in effective loss of item control (item does not behave as commanded)

8.6.2.3 HIGHLY RECOMMENDED:

a) Spatial clearance goals based on object type
b) Strategy for avoiding high risk situations in preference to reacting to them
c) **Pitfall:** Excessive emphasis on permissiveness is prone to resulting in unsafe behaviors or guiding the item into a high-risk situation that results in a tactically unavoidable mishap
d) Prioritization strategy for behavior if an obstacle strike is unavoidable

8.6.2.4 RECOMMENDED – N/A

8.6.2.5 CONFORMANCE:
Conformance is checked via inspection of design, V&V evidence, and demonstration.

8.6.2.6.1 Note: Planning permissiveness is coupled to perception and prediction. A strategy of avoiding high risk situations via ODD selection and/or strategic planning to avoid risk can reduce reliance upon tactical loss mitigation behaviors. A “no win” situation might be avoidable via a longer planning horizon that avoids tactically risky situations.

8.6.3 The item shall have acceptable planning V&V.

8.6.3.1 MANDATORY:

a) Description of approaches used for planning V&V
b) Arguments and evidence that planning capabilities are acceptable

8.6.3.2 REQUIRED:

a) Ensure that no invalid (impossible to execute) plan will be accepted as valid
b) **Pitfall:** Arguments that certain mishaps are "impossible" to avoid (and therefore acceptable) is prone to abuse, resulting in increased risk.
   NOTE: A purely reactive item that continually puts itself into high risk situations resulting in incidents might not be acceptably safe. Ideally, the marginal change in risk due to an "unavoidable" mishap should be small if the item's planning horizon is lengthened over a broad range of planning horizon extending past the actual planning horizon. If this is not true, it is possible that the item is too short-sighted in its planning.

8.6.3.3 HIGHLY RECOMMENDED:

a) Validate that plans designated as "safe" meet designed stand-off distances to obstacles and other goals
   NOTE: Stand-off distances might be coupled to prediction capabilities
b) Validate that short-sighted planning horizons do not result in putting the system into situations with elevated risk that could reasonably be avoided
   EXAMPLE: A vehicle selects a path based on a shortest-historical-travel-time algorithm that traverses tertiary road surfaces unlikely to be treated in a winter storm because the first block of that path is clear of ice. However, the rest of the path turns out to be ice covered. A less risky but longer path on primary roads would be more likely to avoid ice.
c) Define and apply suitable V&V criteria for nondeterministic planning algorithms
d) Define and apply suitable V&V criteria for chaotic planning situations
   EXAMPLE: A small change in initial conditions could result in large changes in plan results, even if deterministic algorithms have been used. For example, whether item goes to right or left around an obstacle that is exactly in the item path might be difficult to control in practice if there is acceptable clearance on both sides of the obstacle and the item uses a non-deterministic planning algorithm.
e) Ensure that path planning and path updates meet real time item constraints
f) Consider implications of shifting of risk to other vehicles
   EXAMPLE: If the ego vehicle comes to an in-lane stop and turns on its 4-way flashers (or other emergency signal) and is struck by a trailing vehicle, that collision might be considered the other vehicle's fault. But, stopping in traffic could also be considered to have shifted risk onto other vehicles and overall increased risk across vehicles on that roadway.
   EXAMPLE: Consider an ego vehicle that obeys a safe following distance envelope and reacts with maximum braking force if the envelope is violated, even by a small amount. Such a vehicle might be struck from behind by trailing vehicle with less capable braking ability. While that collision might be considered the trailing vehicle's fault, less

aggressive braking for small envelope violations might decrease overall risk and severity of collisions.

8.6.3.4 RECOMMENDED:

a) Arguments that a safe plan can always be generated when the item is within its ODD
b) Arguments that a safe plan will always be generated when the item is within its ODD

8.6.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

8.6.3.6.1 NOTE: Ensuring that valid plans are generated when feasible is desirable, but has a limited role in a safety case because it is possible to enter a state where there is no feasible valid path due to an ODD departure, suddenly appearing obstacle, etc. Therefore, dealing with lack of a feasible valid path is required regardless and it is more a matter of frequency of how often that happens.

8.6.3.6.2 NOTE: Planning performance encompasses a full range of capabilities, not just speed. Safe planning is subject to the limits of bounded rationality (**REFERENCE:** Simon, Herb, "Science of the Artificial," 1996), which recognizes the limits of available information and computational resources in making decisions. This results in a tradeoff opportunity between reacting safely to dangerous tactical situations and taking a more strategic approach to avoiding getting into dangerous tactical situations. The safety case documents a selected strategy for creating an acceptable planning horizon according to this tradeoff and argues that the strategy has resulted in an item that is acceptably safe.

8.6.4 Risks resulting from planning failures shall be mitigated.

8.6.4.1 MANDATORY:

a) List of potential planning failures with traceability to mitigation

8.6.4.2 REQUIRED:

a) Handle case of no valid plan existing
   EXAMPLE: External environmental change such as a suddenly appearing obstacle
b) Handle case of planner not able to find a valid plan in a timely manner, even if one might exist

8.6.4.3 HIGHLY RECOMMENDED – N/A

8.6.4.4 RECOMMENDED:

a) Use of a safing mission strategy involving an alternate plan
   NOTE: In some automotive standards this is referred to as having a "minimum risk maneuver" that puts a vehicle in a "minimum risk condition," although whether a "minimum risk" is actually acceptable needs to be argued in the context of overall item-level risk rather than assumed.

8.6.4.5 CONFORMANCE:

Conformance is checked via inspection of design, V&V evidence, and demonstration.

8.7 Prediction

8.7.1 Prediction functionality shall have acceptable performance.

8.7.1.1 MANDATORY – N/A

8.7.1.2 REQUIRED:

a) Description of strategy and algorithms for prediction
b) Strategy, calculation approach, and design of motion prediction algorithms
c) Characterize risk presented by inaccurate prediction
d) Argue that prediction performance is acceptable
    1) Characterization of prediction performance requirements
    2) Characterization of prediction performance results
    3) Argue that performance metrics and results are acceptable

8.7.1.3 HIGHLY RECOMMENDED:

a) Use of field engineering feedback to monitor prediction performance with respect to performance requirements
b) Use of field engineering feedback to identify rates of incidents resulting from inaccurate prediction and to update risk and prediction models accordingly.

8.7.1.4 RECOMMENDED – N/A

8.7.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

8.7.1.6.1 Note: In some items prediction might be performed entirely or partially by a machine learning or other “AI” approaches. In such items prediction functions are subject to Section 8.5.

8.8 Item trajectory and system control

8.8.1 Trajectory and system control shall have acceptable performance.

8.8.1.1 MANDATORY:

a) Description of trajectory computation and following approach
b) Description of system control approach
c) Characterization of system controllability limits
    1) Considering the entire span of environmental conditions in ODD
    EXAMPLES: Maximum braking ability for worst case conditions in ODD, maximum curvature (minimum turn radius) for worst case conditions in ODD; accounting for road surface conditions, slopes, etc.; all of these worst cases at the same time
    2) Considering the entire span of system conditions
    EXAMPLES: Accounting for tire wear, cargo positioning, occupant weight distributions

8.8.1.2 REQUIRED:

a) Description of interaction between planning and trajectory following limitations
EXAMPLE: Approach for mitigating the risk of a planner commanding a trajectory that will result in item rollover on a tight, high-speed turn in unfavorable road conditions.
b) Description of interaction between trajectory limitations and control limitations
EXAMPLE: Approach for mitigating risk of a trajectory commanding the item to perform a maneuver beyond the physical limits of the item taking into account a potentially heavy cargo load, potentially degraded operational state (e.g., wet tires or overheated brakes), and unfavorable road conditions
c) Define strategies for managing described interactions involving planning, trajectory following, and control limitations.
EXAMPLE: If the planner produces an infeasible plan, the trajectory follower follows a close approximation of the plan within trajectory limits while notifying the planner that it is deviating from the intended plan. (This is just one possible approach.)
d) Trace strategies to risks and hazards.

8.8.1.3 HIGHLY RECOMMENDED – N/A

8.8.1.4 RECOMMENDED – N/A

8.8.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

8.8.2 The argument shall describe the item trajectory and control interface.

8.8.2.1 MANDATORY:

a) Description of autonomy to item equipment interface
EXAMPLES: Interface to engine controller, interface to steering, interface to brakes

8.8.2.2 REQUIRED:

a) Describe additional sensing and actuation components utilized in the control loop
EXAMPLES: Accelerometers, inertial navigation, wheel speed, altimeter
b) Describe operator interface for entry into and exit from autonomous operation
c) Describe item fault detection reporting capability
EXAMPLES: Reading Diagnostic Trouble Codes (DTCs) and Malfunction Indicator Light (MIL) actuations from an underlying conventional item platform
d) Describe design of external control monitoring and takeover mechanisms even if not used during normal operation
EXAMPLES: Teleoperation, remote disable capability
e) Description of item interface to human driver controls

8.8.2.3 HIGHLY RECOMMENDED:

a) Design of human driver controls, including special controls such as for maintenance operations and testing operations, even if not used during normal operation
NOTE: This is relevant for safety related operations that expect a human to exert control

over the item as part of operations that are not normal operational missions. As with the rest of this standard, the safe ability of a human to control and/or supervise is out of scope, but the provision of interfaces and correct item response to applied commands is within scope.

8.8.2.4 RECOMMENDED – N/A

8.8.2.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

8.8.2.6.1 Note: For bespoke autonomous items the interface might be to individual sensors and actuators. For autonomy capabilities added to conventional vehicle platforms the interface might be a connection or some heterogeneous approach.

8.8.3 The argument shall demonstrate that the item interface is acceptable despite faults and interaction effects.

8.8.3.1 MANDATORY:

a) Description of fault response to equipment faults
EXAMPLES: Tire blowout, ECU failure, turn indicator failure
b) Description of response to item behavioral fault or other unplanned item action
EXAMPLES: Vehicle, vehicle pushed or impacted by other vehicle
c) Description of response to defective, exceptional, or unusual autonomy commands
EXAMPLES: Out of range command value, autonomy command that violates assumed slew rates for controls originally designed for human use, autonomy command that would result in vehicle rollover or spin

8.8.3.2 REQUIRED:

a) Consideration of attempted autonomy control of vehicle in ways beyond the scope of underlying vehicle V&V and component V&V
EXAMPLE: Command sequences a human driver is unlikely to present to vehicle such as a step function rather than ramped input into accelerator pedal position sensing circuitry cause a latent software defect in the vehicle code to be activated.
EXAMPLE: Premature wear-out of safety related components due to high speed cycling of input values under automated control that were assumed in component design to be under slower human control
b) Response to takeover operation, including potential item control anomalies during the transition
EXAMPLE: The transition in and out of autonomy mode may cause anomalous control inputs values for which the baseline item was not designed.
NOTE: The item-level safety of a human driver provided takeover operation command is out of scope for this standard; however, any issue with the item incorrectly executing such a command is within scope.
c) Methods to detect and mitigate loss of control loop closure at the trajectory level.
EXAMPLE: The system deviates significantly from the commanded path.

NOTE: There may be more than one cause of control loop failure (e.g. brake system failure vs. ice on the road). Mitigations should take into account that the same action might not be appropriate in all circumstances.

8.8.3.3 HIGHLY RECOMMENDED:

a) Interaction between autonomy item and any installed ADAS items (if any are installed)
EXAMPLES: Automated Emergency Braking (AEB) or Electronic Stability Control (ESC)

b) **Pitfall:** Reliance upon ADAS items to prevent incidents is prone to overlooking implicit assumptions in the underlying ADAS safety case based on a presumption of human driver responsibility for overall item safety.
EXAMPLE: An ADAS collision prevention item might have a high false negative rate in order to achieve a low false positive rate based upon engineering reasoning that a human driver should avoid collisions in the first place and a concern that false positive detection rates will lead to loss events such as unnecessary rear end collisions. This might make such an ADAS feature a useful defense in depth measure, but not result in sufficient collision risk mitigation as a primary collision avoidance system for fully autonomous item operation.

8.8.3.4 RECOMMENDED – N/A

8.8.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

8.8.4 Explicit and implicit item operator notifications shall be handled safely.

8.8.4.1 MANDATORY – N/A

8.8.4.2 REQUIRED:

a) Identify safety related explicit notifications to the item that would be handled by a human in the absence of autonomy
EXAMPLE: Out-of-specification tire pressure notification

b) Identify safety related implicit notifications to the item that would be handled by a human in the absence of autonomy
EXAMPLES: Severe handling problem due to loss of wheel, speed change due to uncommanded acceleration
NOTE: This is intended to address situations in which a competent human item operator would be reasonably expected to notice that something regarding item operation needs attention (e.g., sudden torque on steering wheel, rough ride, and other symptoms of a blown out tire)

c) If the item is based upon a modification or augmentation of a vehicle with a conventional human driver interface, handling of safety related driver notifications in a manner that supports the underlying driver notification safety objective.
EXAMPLE: For US vehicles, FMVSS 138 tire pressure warnings are intended to provoke tire pressure corrective action, not simply display a tire pressure warning

d) Define strategy for handling existing human-oriented safety related notifications that are disabled or ignored by the addition of autonomy so as to handle the underlying condition that triggered the notification
EXAMPLE: If an indicator warning light is missing due to removal of a vehicle dashboard display, the item still detects the underlying condition that generated the warning and takes appropriate risk mitigation action.
e) Define strategy for handling the underlying condition for each safety related system behavior monitored, even if no corresponding explicit electronic based alert mechanism is present in a conventional system.
EXAMPLES: Substantive reduction in braking capability, audible brake pad wear mechanical indicator, visible tire wear indicator

8.8.4.3 HIGHLY RECOMMENDED:

a) Inclusion of indications and warnings that would otherwise be displayed to physically present vehicle operator presented as part of teleoperation displays, if applicable
b) Inclusion of indications and warnings that would otherwise be physically detectable to physically present system operator presented as part of teleoperation displays, if applicable
EXAMPLE: Ignition status, lateral acceleration rate, significant vehicle vibration

8.8.4.4 RECOMMENDED – N/A

8.8.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

8.8.4.6.1 Note: Operator notifications include explicit notifications such as warning lights, warning buzzers, and other designed communication mechanisms that transfer fault handling responsibility to a human driver in a conventional item. Operator notifications also include implicit notifications such as engine failing to start or loud vehicle noises that the human operator would be assumed to notice and correct in a conventional vehicle. This clause can still apply to bespoke items to the extent to which they incorporate conventional vehicle components that produce operator notifications.

8.9 Actuation

8.9.1 Actuator faults shall be detected and mitigated.

8.9.1.1 MANDATORY:

a) Defined capability characterization and fault model for each actuator
b) Analysis showing coverage of actuator faults according to relevant fault models
c) Analysis showing that higher level control approaches are compatible with actuation fault models and failure rates.
Example: A human driver may be expected to use alternate methods to control vehicle speed in the event that braking fails (e.g., down-shift, activate parking brake, steer onto an uphill roadway, steer into a sand or gravel runaway vehicle ramp, steer into an

energy absorbing barrier in preference to collision with other vehicles, shift to neutral if uncommanded acceleration is suspected, or even roll the vehicle over in preference to suffering a head-on collision with an oncoming vehicle). Such controllability may be factored in to brake failure rate acceptability for a baseline vehicle. However, an autonomous algorithm can only engage in these actions if designed to do so.

8.9.1.2 REQUIRED:

a) Monitoring for loss of control loop closure
EXAMPLES: Actuator deviates from commanded position for a significant length of time, actual braking force fails to provide full commanded braking force potentially indicating braking system degradation

8.9.1.3 HIGHLY RECOMMENDED – N/A

8.9.1.4 RECOMMENDED – N/A

8.9.1.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

8.9.1.6.1 NOTE: Safety related functionality of actuators encompasses significant scope beyond what is covered in this standard. For example, ensuring acceptable vehicle handling and braking capability taking into account tire deformation characteristics, suspension, road surface conditions, road slope, braking mechanism condition, and so on is a complex topic. This clause is intended to act as an interface to whatever argument beyond the scope of computer-based items is necessary to assure acceptable actuator capability is present.

8.10 Timing

8.10.1 Timing performance of autonomy functions shall be acceptable.

8.10.1.1 MANDATORY:

a) Timing analysis of significant autonomy components and total end-to-end latency from environmental changes to item reaction, including:
    1) Accounting for latency of entire computational chain from sensing an object/event all the way through to taking responsive action
    2) Violation of ODD parameters to system response
    3) Degradation of functionality or equipment status to corresponding mitigation response

8.10.1.2 REQUIRED:

a) Timing analysis of other item components and services regarding safety related total end-to-end latency including:
    1) Detecting and responding to sensed object departure from predicted behavior
    2) Control loop stability analysis
b) Violation of ODD subset parameters to transition to new ODD subset, including safing ODD subsets

c) Timing analysis and V&V of each major autonomy and other major safety related item components

8.10.1.3 HIGHLY RECOMMENDED:

a) Validation of timing budgets via simulation and testing
b) V&V of fault management response via injected timing faults
c) Analysis and validation of timing involving communication to and from human interfaces and human factors assumptions used for teleoperation and/or remote driver supervision
NOTE: Expectations regarding reasonable human factors assumptions and designs are outside the scope of this standard, but any such information is taken into account when setting timing budgets.

8.10.1.4 RECOMMENDED – N/A

8.10.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

See also: Section 10.7, System Timing.

9 Software and System Engineering Processes

9.1 Development process rigor

9.1.1 The argument shall demonstrate that the item design quality and development process quality conform to relevant best practices for producing an acceptably safe item.

9.1.1.1 MANDATORY:

a) Defined and acceptable process model (See Sections 9.1.2-9.1.5)
b) System quality (See Section 9.2)
c) Defect data (See Section 9.3)
d) Development process quality (See Section 9.4)

9.1.1.2 REQUIRED – N/A

9.1.1.3 HIGHLY RECOMMENDED – N/A

9.1.1.4 RECOMMENDED – N/A

9.1.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

9.1.2 The item development process shall be defined and mapped onto a credible and acceptably high criticality development process model.

9.1.2.1 MANDATORY:

a) Defined process activities encompass all substantive steps and artifacts in an identified reference process model of suitably high criticality.
   EXAMPLE: Evidence is provided that all elements of the IEC 61508 defined V model are included by the defined process, including all associated activities and all defined design artifacts. (Alternately, the same for ISO 26262.)
   NOTE: Acceptable reference process models include those defined for an acceptable domain safety standard, and need not correspond to IEC 61508, which is used solely as an example.
b) Each development process activity identified as a defined task with distinct entry points, exit points, and criteria for transitioning among activities.
   NOTE: This does not mean that activities must be carried out sequentially, nor does it prohibit phased transitioning, iteration, and other structuring of activities. However, it this prompt element does imply that it is possible to audit whether there actually is a task definition, and whether the activity is being carried out in accordance with the task definition.
c) Each defined development process activity produces defined, auditable work product artifacts.

d) All safety related activities and work products are designated as such and made available to assessors.
NOTE: This includes aspects of development process and item quality that even partially include safety related aspects of the item.
e) Work products include technical artifacts
f) Process activities encompass at least:
    1) Item level
    NOTE: This includes quality measures that apply to data sources, service feeds, and other software and systems outside the scope of the vehicle but within scope of the item.
    2) System level
    3) Software
    4) Electrical and electronic hardware
    5) Safety
    NOTE: Whether safety activities are incorporated into other processes or are a separate set of processes is flexible. However, independence is required by Section 17.3.
    6) Cybersecurity (See Section 10.8)

9.1.2.2 REQUIRED – N/A

9.1.2.3 HIGHLY RECOMMENDED:

a) The set of defined process activities encompasses all substantive steps in an application-relevant safety standard if one is available.
NOTE: More than one such standard might be applicable and acceptable for different portions of the item. It might be that no such additional standard is acceptable for use for some aspects of the item.
b) Set of defined process activities encompasses security in accordance with the Security Plan.
c) Work products include meeting minutes, analysis results, test results and other formal records not otherwise used as evidence for argument.
d) **Pitfall:** Use of development process models that are not specifically intended for critical system development or are not intended for the product domain is prone to providing unacceptable evidence for a safety case.

9.1.2.4 RECOMMENDED – N/A

9.1.2.5 CONFORMANCE:

Conformance is checked via inspection of item level and software development plan.

9.1.2.6.1 Note: Mapping to a “V” process defined in a safety standard does not mean that a V process must be used. Rather, the requirements can be met if an alternate process (such as an Agile process) is implemented in a way that it contains equivalent activities to a defined safety critical V process. The mapping requirement is intended to ensure that no substantive steps are

skipped and is not intended to force any specific execution order, detailed content, naming, or other aspects of those steps.

9.1.2.6.2. Note: Some aspects of autonomy, such as use of machine-learning based functionality, do not conform to traditional expectations for some process steps such as requirements decomposition. However, the development process for such components must still be defined and traced to a relevant critical development process. For example, the design and execution of a data gathering plan might map to requirements definition.

9.1.3 The overall item system and software development process shall incorporate and adhere to domain-relevant best practices.

9.1.3.1 MANDATORY:

a) Identification of best practices that have been incorporated into each process activity and work product artifact
NOTE: This clause is not limited to safety related aspects of the product. It applies to the entire product including both the item and any impinging non-safety-related aspects of the product.

9.1.3.2 REQUIRED – N/A

9.1.3.3 HIGHLY RECOMMENDED:

a) Traceability to a source for best practices
EXAMPLES: IEC 12207, IEC 61508 part 7, SEBOK, SWEBOK, MIL-STD-498, ISO 26262, DO-178C
b) Arguments of acceptable rigor for process activities and work products for which best practices have not been identified
c) **Pitfall:** Domain-relevant best practices for novel and/or immature technologies are prone to falling short of the needs of high criticality items.
EXAMPLE: Best practices based on traceability to requirements are arguably insufficient for machine-learning based items if requirements have not been established for traceability.
NOTE: Even if high level system requirements have been established, the use of technologies such as machine learning that do not provide a causal chain of traceability between requirements and ultimate system performance. This can degrade the validity of a backward traceability argument between system level testing and requirements, because there is a broken traceability link in the forward direction. Alternate, additional assurance approaches are advisable.

9.1.3.4 RECOMMENDED – N/A

9.1.3.5 CONFORMANCE:

Conformance is checked via inspection of item level and software development plan.

9.1.3.6.1 Note: “Best” practice identification need not be provably optimum, but rather should be at least commercially reasonable good practices supported by standards, common practice,

and/or scholarly literature. The term “best” is used rather than “accepted” in part to avoid an argument strategy of claiming that software in a particular application area is traditionally of poor quality (e. g., potentially unsafe in the absence of a human operator that can help mitigate design defects) and therefore poor quality software is an “accepted” practice.
REFERENCES: SWEBOK: https://www.computer.org/web/swebok; SEBOK: https://www.sebokwiki.org **See also** references in Section 9.1.3.3(a).

9.1.4 The defined system and software development process shall incorporate a minimum set of required best practices for safety related components.

9.1.4.1 MANDATORY:

a) Defined item level safety requirements
b) Effective peer reviews for defined safety requirements, models, designs, implementations, and test plans
   NOTE: “Effective” means that evidence supports that peer reviews actually find a substantial fraction of all defects found during V&V.
c) Configuration management and version control processes and practices defined and evaluated for effectiveness
d) Quality assurance processes and practices are defined and evaluated for effectiveness
   NOTE: This includes both quality assurance for developed artifacts (e.g., testing), and quality assurance for processes (SQA, including audits of process execution).

9.1.4.2 REQUIRED:

a) Item level testing to verify that testable safety related requirements have been met.
   NOTE: Fulfillment of any untestable requirements must be validated in another way
b) Review of defect closeouts by someone other than the person doing the defect correction. This includes decisions to defer defect correction or otherwise not correct a defect before the next item release.
c) Account for differences between development environment and deployment environment.
   EXAMPLES: Different levels of numeric precision between development systems and deployed systems, timing differences due to removal of test equipment, differences between simulated environment and real-world environment for systems operated in a test chamber.
d) Record and justify deviations from identified best practices
   1) All deviations from identified best practices approved by agreement by at least two different people involving a non-trivial review and decision process
   2) Blanket, repetitive, and other systematic deviations from identified best practices are not permitted for safety related components and functions.
      NOTE: Deviations from identified best practices are expected to be as a result of a unique, truly one-off situation, and not simply used as a way to bypass inconvenient but identified best practices or indefinitely defer correction of issues.

e) Identification of deviation from a best practice as a contributing factor to an incident or mishap results in revocation of deviation approvals for all existing deviations of that practice unless and until those deviations are individually re-reviewed and re-approved.
f) **Pitfall:** Deviation justifications that amount to saying deviation is customary practice rather than based on the merits of the specific deviation situation at hand are prone to resulting in degraded software item and process quality.
EXAMPLE: An unacceptable deviation approval rationale might be that a deviation from a particular best practice has been approved for other cases on the project, without analysis as to the acceptableness of the deviation for the particular situation in question.

9.1.4.3 HIGHLY RECOMMENDED:

a) Unit testing to a defined, acceptable level of software structural coverage.
b) Identify other best practices that are incorporated into the software process.

9.1.4.4 RECOMMENDED:

a) Activities described in IEEE 1012-2012 – IEEE Standard for system and software verification and validation.
b) Blanket deviations from best practices are strongly discouraged, with deviations performed on a per-item basis based on argument as to the acceptableness of the deviation.
c) Agile methods may be used so long as they produce objective, auditable documented evidence of quality and conformance to identified best practices.

9.1.4.5 CONFORMANCE:

Conformance is checked via inspection of item level and software development plan, design artifacts, and process quality documentation.

9.1.4.6.1 NOTE: The word “effective” means that the technique’s effectiveness is supported by objective evidence of effectiveness.

9.1.4.6.2 NOTE: Independent defect closeout can be done internal to the design team, but is performed by an individual (or group) who was not involved in creating the defect, and also not involved in correcting the defect or otherwise performing the corrective action being reviewed. A balance is important between acceptable technical expertise to do a responsible evaluation with acceptable management chain independence to minimize pressure to do cursory reviews due to deadlines or approve unsatisfactory corrective actions. A root cause analysis responsive to an incident that reveals unsatisfactory independence of defect closeout reviews as a contributing factor might need to result in corrective actions to increase independence and significant re-review of existing defect closeouts.

REFERENCE: Boehm et al., Balancing Agility and Discipline: A Guide for the Perplexed, 1st Edition, 2003.

9.1.4.6.2 NOTE: (Informative) Configuration management obligations are potentially imposed by at least the following prompt elements:

- Safety case (Section 5.1.1.1)
- ODD (Section 8.2.4.1)

- Machine learning data (Section 8.5.3.2)
- Safety related components (Section 9.1.4.1)
- Tool Chain (Section 13.3.3.2)
- Build data (Section 14.3.4.3)
- Field self-modifications (Section 14.6.1.2)
- SPI Data (Section 16.3.1.2)
- Conformance package (Section 17.2.1.2)

9.1.5 Acceptable item quality and item development process quality shall be ensured for safety related components.

9.1.5.1 MANDATORY:

a) Objectively evaluable evidence that item quality is acceptable for the required level of rigor or other risk mitigation approach employed.
b) Evidence of peer reviews and peer review effectiveness
c) Evidence of acceptable item level and software level test results
d) Evidence of acceptable conformance to development processes
   EXAMPLE: SQA audit records showing conformance to development process

9.1.5.2 REQUIRED:

a) Evidence of conformance to a defined coding style standard
b) Evidence of acceptable source code analysis results with a defined analysis profile
   EXAMPLES: MISRA C conformance.

9.1.5.3 HIGHLY RECOMMENDED:

a) Measurement of quality metrics
   EXAMPLE: Defect escape rates from each process activity
b) Measurement of artifact quality
   EXAMPLE: Review records of test plans, requirements that assess completeness, correctness, and conformance to project-specific format templates
c) Use of accepted coding standards that emphasize safety and/or security.
   EXAMPLES: MISRA C, MISRA C++
d) Key steps in the process should be evaluated to determine if they are actually being performed, and whether the activities are effective.

9.1.5.4 RECOMMENDED – N/A

9.1.5.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

9.2 Software quality

9.2.1 Software quality acceptance criteria shall be defined for safety related software.

9.2.1.1 MANDATORY:

a) Identify artifact quality acceptance criteria
EXAMPLES: Specified level of MCDC unit test coverage, traceability from test plan to requirements, no software with more than X identified defects per 1000 lines of source code at time of release (implying that modules with high defect densities have been redesigned and rewritten)
NOTE: The validity of the examples given will depend upon the availability of objective evidence of relevance. Arguments might be based on historical predictive power for the development team or conformance to domain-specific standards requirements.

b) Acceptable quality of purpose-built software
    1) Underlying code for autonomy functions included in software quality activities
    EXAMPLE: The quality of run-time engine software for executing a neural network with its learned weight data set can be subjected to conventional software quality processes

9.2.1.2 REQUIRED:

a) Identify process-based software quality acceptance criteria
EXAMPLES: Peer review effectiveness rate (e.g., more than 50% of defects before release found via peer review), peer review coverage rate (e.g., 100% of new code peer reviewed), process completion rate (e.g., percentage of required artifacts spot-checked by SQA)

b) Acceptable quality of re-used and third-party software
EXAMPLE: Open source frameworks and libraries used to support machine learning applications.
See also Section 13.

c) **Pitfall:** Code construction metrics alone are prone to missing potential issues related to other aspects of quality.
NOTE: Code quality metrics in general can be helpful, but favorable metrics do not necessarily indicate acceptable overall software quality.
NOTE: Quality of behaviors based on data values is not generally assessable via conventional code quality metrics. For example, the quality of neural network weights.

9.2.1.3 HIGHLY RECOMMENDED:

a) Other software quality acceptance criteria

9.2.1.4 RECOMMENED – N/A

9.2.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

9.2.2 Item quality acceptance criteria shall be defined for safety related components, subsystems, and the item as a whole.

9.2.2.1 MANDATORY – N/A

9.2.2.2 REQUIRED:

a) Acceptable quality of software
    1) Underlying code for autonomy functions included in software quality activities
       EXAMPLE: Run-time engine for executing results of machine learning development activities
    2) Other software
b) Acceptable quality of computing hardware
c) Acceptable quality of sensors, actuators, and other items
d) Acceptable quality of third-party components, including at least:
    1) Operating system, if used
    2) Libraries incorporated in the final item, if used
    3) Other COTS/SOUP and legacy components
       NOTE: See Section 13.4.
    4) Remote software functionality, if used
       EXAMPLE: Infrastructure data sources, other-item data sources, teleoperation systems
    5) On-line services, if used
       EXAMPLE: Cloud-based map data, weather report feeds
e) Quality of safety related components supported via at least one of:
    1) Independently assessed conformance to this standard
    2) Independently assessed conformance to another domain relevant safety standard
       EXAMPLES: ISO 26262, MIL-STD-882E
       NOTE: Arguments based on “proven in use” or other approaches for software which was not originally created for safety related functionality must still be done in conformance of this or another relevant safety standard.
f) **Pitfall:** COTS components might be used to perform safety related functionality but are prone to challenges in obtaining acceptable evidence to support safety arguments.
   NOTE: See Section 13.4.

9.2.2.3 HIGHLY RECOMMENDED:

a) If more than one approach for determining quality is used, traceability to approach on a per-component basis.
b) Data subject to relevant aspects of software quality activities, including configuration data and machine learning data.

9.2.2.4 RECOMMENDED – N/A

9.2.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

See also: Tool Qualification, Section 13.

9.3 Defect data

9.3.1 Defect data shall be collected, analyzed, and used to improve products and processes.

9.3.1.1 MANDATORY:

a) Defined process step or other event for start of recording failure data for each type of artifact.
See 9.3.1.3(a) for a specific example
b) Defined root cause analysis procedure for development phase and deployment phase defects.
c) Root cause analysis procedures explicitly include the possibility that defects are indicative of an underlying defect in the safety case, processes, and/or safety culture and support correction of such underlying defects.

9.3.1.2 REQUIRED:

a) Defect and failure data recorded, analyzed for root cause, and tracked to closure.

9.3.1.3 HIGHLY RECOMMENDED:

a) The start of defect recording occurs with the first commit to a project repository or the start of the first peer review, whichever occurs first.
b) Statistical measures used to monitor for weaknesses in the safety related development, V&V, safety case, and other processes.
c) Defect and failure data procedures followed for software components, including third party and legacy components.

9.3.1.4 RECOMMENDED – N/A

9.3.1.5 CONFORMANCE:

Conformance is checked via inspection of item level and software development plan as well as design and V&V evidence.

See also: Verification, Validation and Test – Run-Time Monitoring, Section 12.5, for data collection and reporting.

9.4 Development process quality

9.4.1 Development process quality shall be acceptable.

9.4.1.1 MANDATORY:

a) Organization and processes of the software quality assurance activities defined and evaluated for effectiveness.

b) Organization and processes of the safety assurance activities defined and evaluated for effectiveness.
c) Software Quality Assurance (SQA) processes and practices defined and include at least the following for the areas of software development and safety:
    1) Defined development, deployment, and field engineering feedback processes
    2) Training on the defined process
    3) Process conformance audits
    4) Documented (and/or validating) technical skill competence for assigned tasks

9.4.1.2 REQUIRED – N/A

9.4.1.3 HIGHLY RECOMMENDED:

a) SQA management and reporting chains as independent as is practicable from management and reporting associated with product engineering and software engineering.
b) Use of a reference process model and/or process maturity model.
   EXAMPLES: SEI CMM(I), Automotive SPICE

9.4.1.4 RECOMMENDED:

a) The organization and processes of the security assurance activities defined and evaluated for effectiveness.
b) Allocating a target percent of total development effort to be spent on SQA activities.
   EXAMPLE: Allocating 5% to 6% of total effort on SQA based on experience with embedded system development company experience.

9.4.1.5 CONFORMANCE:

Conformance is checked via inspection of process plans and evidence of effective execution of processes.

9.4.1.6.1 NOTE: This clause deals not with software and hardware design quality (lack of defects), but rather with process quality (effective execution of processes). This area is commonly known as Software Quality Assurance (SQA) for software development, although the scope of this clause goes beyond software to the entire item design process.

9.4.1.6.2 NOTE: The emphasis in this section is that there is a way to ensure that processes are actually being executed and that execution is effective. It is generally necessary to have checks and balances used to ensure that this happens.

REFERENCE: SEI, “+SAFE, V1.2: A Safety Extension to CMMI-DEV, V1.2” https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8219

10 Dependability

10.1 General

10.1.1 The argument shall demonstrate that the item is acceptably dependable to support the safety case.

10.1.1.1 MANDATORY:

a) Degraded operations (See Section 10.2)
b) Redundancy (See Section 10.3)
c) Fault detection and mitigation (See Section 10.4)
d) Item robustness (See Section 10.5)
e) Incident response (See Section 10.6)
f) Item timing (See Section 10.7)

10.1.1.2 REQUIRED – N/A

10.1.1.3 HIGHLY RECOMMENDED – N/A

10.1.1.4 RECOMMENDED – N/A

10.1.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.2 Degraded operations

10.2.1 Degraded mission capabilities shall provide acceptable support for item-level safety.

10.2.1.1 MANDATORY:

a) Defined handling of catastrophic faults (sets of faults which cause item to be unable to satisfy the Minimum Equipment List (MEL) of any other defined operational mode)
NOTE: It is understood that a catastrophic fault might result in a loss event. This clause is intended to ensure that reasonable efforts have been made to reduce the risk presented by such faults as a defense in depth measure.
EXAMPLE: Loss of both redundant computing elements for vehicle control might, depending upon which elements were lost, result an in-lane stop, stop while maintaining last known good trajectory, or application of mechanical brakes with best-effort trajectory control.

10.2.1.2 REQUIRED:

a) **Pitfall:** Not making provision for best-effort safety for catastrophic item failures because they are shown to be “impossible” is prone to resulting in catastrophic loss events when an unforeseen gap in the impossibility argument emerges in real world operation.

b) Identify hazards related to and risks increased by entering a degraded operational mode.
EXAMPLE: Performing an in-lane stop in response to a fault can increase the risk of being hit by another vehicle.
c) Degraded operational mode concept description. This includes at least:
    1) Description of degraded operational modes, if any, including mission parameters
    2) Role in fault mitigation
    3) Role in safety argument
    EXAMPLES: Limp-home mode; as a result of a partial sensor failure, the ODD is restricted to permit operation only in favorable weather
d) Traceability of each degraded operational mode to Minimum Equipment List (MEL) descriptions.
e) Argue that item is acceptably safe when the MEL is met for each operational mode.
f) Argue that item is acceptably safe when each MEL lower threshold is crossed, including the lowest defined MEL (i.e., safety must be argued including the case when there is not enough operational equipment to meet any defined MEL).
g) **Pitfall:** Undocumented degraded operational modes in Commercial-Off-The-Shelf components or subsystems are prone to providing a false indication of full operational capability or un-annunciated degradation.
h) Annunciation of operational and other restrictions associated with a degraded operational mode when entered:
    1) To humans interacting with item
    2) To any maintenance and/or monitoring capabilities
    EXAMPLE: Activating 4-way flashers and generating a maintenance request record to annunciated restricted ego vehicle speed due to low tire pressure, sensor failure, etc.
i) Identification of hazards associated with degraded operational modes.
EXAMPLE: The use of a “minimal risk condition” of an in-lane vehicle stop could incur hazards associated with being struck by another vehicle.
NOTE: As with other identified hazards, the contribution to net system level risk from these hazards is considered in the safety case.

10.2.1.3 HIGHLY RECOMMENDED:

a) Limited length diversion mission due to unacceptable redundancy for full operation when appropriate.
EXAMPLES: Pull to nearest safe roadside position, drive to nearest exit ramp.
b) Urgent termination of mission if no MEL is satisfied.
EXAMPLE: In-lane stop.

10.2.1.4 RECOMMENDED – N/A

10.2.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

10.2.1.6.1 NOTE: Classical fault tolerance often maintains the same level of operational capabilities despite faults (e.g., using installed redundancy and spares). In contrast, degraded mode operation involves continued operation with reduced capabilities due to failed equipment, failed sensors, actuators, computing elements, networks, etc., but still satisfying an MEL for the degraded mode. At least one catastrophic failure operational mode is defined to specify actions when no degraded mode MEL is satisfied to transition the item to a safe rest state. Behaviors of degraded modes might be dependent upon context and operational history. Degradation can include reduced performance (e.g., accommodating increased braking distance due to partial failure of braking item, reduced maximum speed), removed capability (e.g., inability to operate in reverse direction, inability to operate in portions of the ODD such as in rain), or combinations. Degradation can also include graceful truncation of a mission (e.g., divert to comparatively safe area to await repairs) and less graceful truncation of a mission (e.g., operate very slowly or come to a stop in a non-ideal location). It is up to the safety case to describe the lattice of degraded capabilities and their role in managing overall item risk.

10.2.1.6.2 NOTE: Catastrophic failure modes should make a best effort to ensure safety, although it is realized such efforts might not be able to prevent all loss events. Such failure modes should attempt to minimize the severity of a loss (potentially avoiding the loss sometimes) if such a failure mode occurs. However, the safety argument should ensure that entering such a condition is so improbable that the item is acceptably safe without such a mode. In other words, catastrophic failure modes should be a defense in depth approach to handle surprises, requirements gaps, and other unanticipated situations.

10.2.2 Degraded mission capabilities shall provide acceptable redundancy and diversity.

10.2.2.1 MANDATORY – N/A

10.2.2.2 REQUIRED (if degraded operational modes are used):

a) List of permitted and prohibited mode transitions that encompasses all possible mode transitions.
   NOTE: It is acceptable to have a list of permitted transitions with the default of all unlisted transitions being prohibited.
b) Acceptable redundancy in case of component and other partial item failures.
c) Diversity that provides acceptable operation in case of component and other partial item failures.
   EXAMPLE: If using LIDAR, radar, and vision, argue that LIDAR and radar alone provide acceptable diversity for operation (potentially in a degraded mode) upon loss of vision.
d) **Pitfall:** Taking unacceptable credit for redundancy and diversity is prone to resulting in over-claimed item dependability, and in particular taking fully independent failure credit for:
   1) A mode pair in which a single fault can cause the failure of a primary mode and its related failover mode

2) Probable multi-component failure, coincident failure, or common cause failure shared between both a primary mode and its related failure mode.
3) Degraded modes during operation if there is a potentially unmitigated fault (latent or otherwise) in the mode switching mechanism
4) Any mode pair in which a single fault (or acceptably probable multi-fault scenario) can cause a failure of both the primary mode and the mode switching mechanism

e) **Pitfall:** An undiagnosed failure in the mode switching mechanism is prone to resulting in an item failure due to an accumulation of faults when the MEL for an operational mode fails to be satisfied.

10.2.2.3 HIGHLY RECOMMENDED:

a) Consideration of failures that affect reconfiguration or mode change process
EXAMPLE: Failure of mode change functionality before or during reconfiguration
b) Alerts, alarms, warnings for activation of a degraded mode
EXAMPLES: Within vehicle; to other road users; to fleet operator; to regulators; to law enforcement
c) To the extent that a degraded mission capability is used in an item redundancy argument, shared faults are considered for any component or function that is shared by both the primary un-degraded and degraded item functionality
d) **Pitfall:** A failover mode having similar software to the primary mode is prone to common cause failures due to algorithmic faults.
EXAMPLE: Primary and failover both use similar algorithmic approach and both fail the same way when encountering exceptional input values.
e) **Pitfall:** A failover mode having similar or shared sensors with the primary is prone to common cause failures due to sensor shortcomings.
EXAMPLE: A sensor type is prone to certain types of false negatives, false positives, or misclassifications in some situations and causes both the primary and failover mode to fail
f) **Pitfall:** Latency introduced while switching to (or recovering from) degraded mode is prone to limiting the safety effectiveness of degraded functionality.

10.2.2.4 RECOMMENDED – N/A

10.2.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

10.2.2.6.1 NOTE: A “primary” mode can be normal operation or mode that is less than completely operational. For this clause the relative “primary” and “failover” mode nomenclature refers to two modes for which the “primary” has more functionality, and the “failover” mode is intended to serve as a reduced capability mode that provides safe operation in the event the primary mode must be exited, e.g., due to equipment failure. The “primary” in a particular mode pair might itself be the “failover” when compared to some other, more capable mode, forming a lattice of degraded modes.

10.2.2.6.2 NOTE: A fault in any mode switching mechanism counts as a first fault in an accumulation of faults. This means in practice that if the switching mechanism fails (due to a first fault), then a failure of the currently active operating mode (due to as second fault) could result in item failure, since the capability to switch to a degraded mode has also failed.

10.2.3 Hazards and risks related to operational mode changes shall be identified and mitigated.

10.2.3.1 MANDATORY:

a) Identification of item operational modes
   NOTE: For some items there might be only one such mode
   NOTE: To the extent that ODD subsetting is used, operational modes might encode the current ODD subset in addition to other potentially relevant modal information such as degraded item configuration.

10.2.3.2 REQUIRED:

a) Identification of item operational modes for at least:
   1) Nominal operational modes
   2) Emergency safety maneuver
      EXAMPLE: Move disabled vehicle off train tracks
   3) Parked
   4) Transport
      EXAMPLE: Vehicle delivery, being towed
   5) Refuel/recharge
   6) Maintenance
   7) Power-on/Self-Test
   8) Unsafe to start new mission
   9) Failures that result in item not satisfying any mode MEL while in operation
   10) Degraded modes
   11) Catastrophic failure mode(s)
   12) Shutdown/Power-off
   13) Post-incident
   14) Safe state mode
   15) Life cycle states
      EXAMPLE: End of line manufacturing test
   16) Loss of external data feeds
      EXAMPLE: Loss of alerts of map status changes such as newly erected construction zones
   17) Loss of external navigation information
   18) Any other modes
      EXAMPLE: Modes used to address different ODD subsets
b) Concept of operations for each identified mode including at least:
   1) Item behaviors and limitations

    2) Response to fault in or failure of mode changing mechanism
c) Criteria for entering and exiting each degraded mode, including:
    1) Per-degraded mode MEL
    2) Operational constraints of each mode
    3) Triggering events that cause transitions into and out of mode
    4) Strategy for determining if corresponding MEL is met before transitioning into a mode
    5) Prohibiting entry into a mode previously exited due to degradation until positive confirmation has been made that the cause for degradation has been resolved
d) Safety during mode transition, including failures that occur during transition process
    1) Safety if fault in mode changing mechanism activates during mode transition process
    2) Safety if an additional failure occurs during mode changing
    3) Changes to item state and/or item state requirements for entering and exiting each mode safely
e) Each mode's role in item-level fault mitigation, and role in safety argument
f) Definition of initialization state for each mode that can be entered
   NOTE: Defined initialization typically has a goal making the item acceptably safe within the newly entered mode.
g) **Pitfall:** Transitioning from a degraded mode to a more capable mode is prone to unmasking suppressed vehicle behaviors.
   EXAMPLE: Exit from incident response mode or power-off mode could unmask a previously suppressed full engine power command could result in unexpected acceleration.

10.2.3.3 HIGHLY RECOMMENDED:

a) Identification of item operational modes, including at least (if supported):
    1) Reduced capability, restricted missions
    2) Reduced capability, limp-home
    3) Best effort handling of catastrophic faults
       EXAMPLES: Stop in lane; stop while maintaining last known good trajectory
    4) Long term storage
    5) Recovery from power loss
    6) Other manual operation
b) Creation of a mapping showing correspondence between item operational modes and ODD subsets (if used) associated with each such mode.
c) Item mode changes initiated in response to faults or failures preclude entry into that same or other modes potentially affected by the initiating fault or failure until positive remediation confirmation has been made.

10.2.3.4 RECOMMENDED – N/A

10.2.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence, as well as demonstration.

10.2.3.6.1 NOTE: Degraded mode operation involves continued operation with reduced equipment, failed sensors, actuators, computing elements, networks, etc., but still satisfying an MEL for that mode. Catastrophic failure modes might be defined to specify actions when no degraded mode MEL is satisfied.

10.3 Redundancy

10.3.1 The item shall have acceptable redundancy, isolation, and integrity.

10.3.1.1 MANDATORY:

a) Definition of mission model for item
b) Definition of item physical architecture
c) Definition of item logical architecture and its mapping onto the physical architecture
d) Identify approach to redundancy, isolation, and integrity with respect to ODDs

10.3.1.2 REQUIRED:

a) As appropriate for the mission model:
    1) Mission length profile used for computing reliability
    2) Approach to diagnosis:
        i. Pre-mission
        ii. During-mission
        iii. Post-mission diagnosis
        iv. During repair
    3) Degraded mission profiles
        EXAMPLE: Diversion mission after significant component failure
b) If redundancy is used, identify fault containment regions (FCRs) for safety related functions and their mapping onto the physical architecture.
c) Identification of safety related redundancy

10.3.1.3 HIGHLY RECOMMENDED – N/A

10.3.1.4 RECOMMENDED – N/A

10.3.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

See also: Section 6.2 Hazards, Section 6.4 Risk Mitigation.

10.3.2 The item shall have an acceptable amount of redundancy and failure mode diversity.

10.3.2.1 MANDATORY:

a) Arguments that redundancy and failure mode diversity is acceptable. This includes consideration of potential:
    1) Hardware faults
    2) Software faults

3) Sensor faults
4) Actuator faults
5) Faults in other item components
   EXAMPLES: Motors, mechanical failsafes, wiring, power supplies

NOTE: For some items an argument might justify that no safety related redundancy and failure mode diversity is required. Nonetheless, a detailed argument is required rather than a safety case deviation based on “not applicable.”

See also: Section 6.5.3.

10.3.2.2 REQUIRED:

a) Redundancy acceptable to achieve required reliability, encompassing all operational modes
b) Consideration of hardware infrastructure and environmental aspects of redundancy and failure mode diversity, including at least:
   1) Power supply
   2) Thermal issues
   3) Component design and manufacturing issues
   4) Shared sensors
   5) Shared actuators
   6) Shared computing components, including multi-core processing chips
   7) Shared wiring harnesses
   8) Shared network connections
   9) Shared zonal location
   10) EMI and EMC
   11) Common cause and other correlated failures
      EXAMPLES: Vibration, temperature cycling, corrosive environment, item aging effects
c) Consideration of software infrastructure aspects of redundancy and failure mode diversity, including at least:
   1) Compilers and other tool chain elements
   2) Libraries and other third-party software components
   3) Software update mechanism, bootloader, and other deployment infrastructure
   4) Timing and coordination
   5) Redundancy management mechanisms and protocols
d) **Pitfall:** Claiming the use of parallel computing paths without a defined redundancy strategy as providing redundancy is prone to overstating fault tolerance benefits.
   EXAMPLE: While typical a neural network uses many parallel paths in its computation, it is not normally intended to provide fault tolerance at the component level.
e) **Pitfall:** Use of purportedly diverse software is prone to common mode and common cause defects. Evidence beyond simply diverse supply chain sources is required to support claims of independent failure of purportedly diverse software and diverse hardware design faults.

NOTE: Multiple trained neural networks can still have common cause defects such as, for example, biases in shared training data.

f) **Pitfall:** Use of redundant identical hardware components is prone to failure due to hardware component design defects.

g) **Pitfall:** Conflicting diversity and redundancy design claims are prone to overstating item reliability.
EXAMPLE: Operating in dust is claimed feasible because of sensor diversity between cameras and radar; however, redundancy is claimed due to having one camera and one radar even though the camera is ineffective in dust, resulting in operating with a single non-redundant sensor when in dust, invalidating other claims of redundant sensors providing fault tolerance.

10.3.2.3 HIGHLY RECOMMENDED:

a) Traceability of redundancy to integrity level requirements for each component and function

10.3.2.4 RECOMMENDED – N/A

10.3.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

10.3.2.6.1 NOTE: Diverse failure modes are ones that do not have a common cause, common mode, design defects, or other expectation of correlated and coincident failures beyond random independent failure assumption.

See also: Minimum Equipment List, Section 10.3.5.

10.3.3 Redundant components and functions shall have acceptable isolation.

10.3.3.1 MANDATORY – N/A

10.3.3.2 REQUIRED:

a) Identification of safety related Fault Containment Regions (FCRs)
b) All components and functions within each FCR designed in accordance with the highest integrity requirement of any component or function in that FCR
c) Integrity analysis of data flows in to and out of each safety related FCR
d) Common mode and common cause fault analysis and avoidance for redundancy
e) Zonal fault analysis and avoidance for redundancy
f) Sufficiency of isolation within any single hardware component that hosts multiple FCRs
EXAMPLE: A multi-core processor chip must have acceptable isolation between cores and support resources for each core to support multiple FCRs.
g) **Pitfall:** Self-diagnosis of an FCR is prone to missing faults that affect both the operational functionality and the diagnosis function, and is prone to missing latent faults.
NOTE: A single fault or accumulation of faults can affect the self-diagnosis capability itself.

EXAMPLE: A first fault disables the self-diagnosis capability of an FCR. A later or coincident fault in that FCR then goes undetected.

h) **Pitfall:** External diagnosis is prone to missing latent faults, including faults that cause incorrect reporting self-test functions triggered by the external diagnosis.

10.3.3.3 HIGHLY RECOMMENDED:

a) Use of an arbitrary failure model
NOTE: An arbitrary fault model assumes that a component or function at a lower integrity level is assumed to behave in a fail active, semi-malicious manner that attempts to undermine the integrity of any higher integrity level component.
b) High integrity monitors and checkers robust to exceptional and malformed data provided to them by lower integrity components and functions.
c) Malicious attacks (i.e., cybersecurity issues) between FCRs considered in keeping with a security plan.

10.3.3.4 RECOMMENDED:

a) Interdisciplinary examination of isolation and fault propagation that includes electronic hardware, power, mechanical items, and structural aspects.

10.3.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.3.3.6.1 Note: Isolation might be used for isolating integrity levels, reliability, availability, and other purposes to ensure non-interference. The FCR analysis clearly states what purpose(s) each FCR serves with regard to the specific dependability property being provided.
EXAMPLE: As an illustration of potential isolation vs. common cause issues, consider this sequence of events: a charging algorithm defect leads to battery fire; fire then spreads to affect other proximate batteries leading to loss of redundant power supplies to redundant component pairs that control network hubs and diagnosis nodes for independent hydraulic pumps; loss of diagnosis node causes protective hydraulic pump shutdown; loss of network hubs causes loss of drive-by-wire electric actuation capability; result: loss of supposedly diverse hydraulic and drive-by-wire control capabilities.

10.3.4 The safety case shall document the design intent for redundancy.

10.3.4.1 MANDATORY – N/A

10.3.4.2 REQUIRED:

a) Design intent documentation specifies the purpose of each redundant fault containment region
EXAMPLES: Fault detection, integrity isolation, availability (hot standby, warm standby, cold standby)
b) **Pitfall:** An architectural pattern with replicated software is prone to software design defects forming a common cause failure.

10.3.4.3 HIGHLY RECOMMENDED:

a) Use of accepted practice for redundancy patterns rather than purpose-created architectural patterns
REFERENCE: Hammet, Design by extrapolation: an evaluation of fault-tolerant avionics, IEEE Aerospace and Electronic Items, 17(4), 2002, pp. 17-25.
b) **Pitfall:** Voter-based patterns such as triplex modular redundancy are prone to the voter being a single fault location that results in failure.
c) **Pitfall:** Redundancy for which credit is taken as simultaneously serving multiple different purposes is prone to resulting in an overestimate of dependability
EXAMPLE: A two-FCR region in which credit is taken for both availability and fault detection is prone to ambiguity in diagnosing which of the two FCRs is good after a disagreement between them has occurred.

10.3.4.4 RECOMMENDED – N/A

10.3.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.3.4.6.1 NOTE: Redundancy includes redundancy relevant to the safety case argument, both at an item and component level.

10.3.4.6.2 NOTE: Pools of redundant resources, such as a set of GPUs, can be treated in an aggregated manner if used for the same redundancy purpose.

10.3.4.6.3 NOTE: Components with uncommitted redundancy, such as GPUs, can specify potential uses and limitations upon uses for redundancy, with higher level arguments including the as-configured redundancy uses within a specific item.

10.3.5 A Minimum Equipment List (MEL) shall be defined for each autonomous operational mode.

10.3.5.1 MANDATORY:

a) Sensor capabilities
EXAMPLES: Minimum number and position of LIDARs, radars, and cameras required for operation
NOTE: Sensors might be impaired by equipment malfunctions, but also might be impaired by adverse environmental conditions.
b) Required maintenance is current
EXAMPLES: Inspection, cleaning, consumable inventories, operating hour-based maintenance
c) Actuator capability requirements
EXAMPLES: Propulsion, brake, steering, etc.
NOTE: Actuators might be impaired by equipment malfunctions, but also might be impaired by adverse environmental conditions.
d) Computing capabilities
EXAMPLES: Processing capability, storage availability, etc.

e) Vehicle status
EXAMPLES: Vehicle weight with payload, tire condition, battery condition, lights, communication system status, other factors
f) Software update freshness, valid configuration, and integrity checks
g) Software functionality
NOTE: It might be that software functions are inoperative even on defect-free hardware due to, for example, a software defect that causes a function to crash in particular operational conditions

10.3.5.2 REQUIRED:

a) MEL includes requirements for redundancy, including any operational hot and cold standby units that are required
b) Calibration validity
EXAMPLES: Acceptable operating hours or other use metric since last calibration, self-calibration
c) MEL below which the item must completely disengage
d) MEL for each degraded mode

10.3.5.3 HIGHLY RECOMMENDED:

a) Analysis supporting that MEL capability is checked frequently enough

10.3.5.4 RECOMMENDED – N/A

10.3.5.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V.

10.3.5.6.1 NOTE: In aerospace the term MEL tends to refer to hardware items that are assumed provide associated functionality. While this standard uses that familiar term, the scope is intentionally expanded to include availability of software, sensing, and actuation functions that might have been compromised even with defect-free hardware due to software defects, exceptional environmental conditions, or other factors. Thus, MEL in this standard refers to the system's ability to perform functions required in a specified, potentially degraded, operational mode and configuration.

10.3.5.6.2 NOTE: In items with multiple operation modes there can be a different Minimum Equipment List (MEL) for each operational mode. If the MEL is the same for multiple operational modes they can be aggregated into an equivalence class for the purpose MEL analysis.

10.4 Fault detection and mitigation

10.4.1 The item shall have acceptable ability to detect and mitigate component and item faults and failures that can contribute to identified risks.

10.4.1.1 MANDATORY:

a) Quantification and justification of self-diagnosis coverage.
b) Reintegration strategy after permanent faults corrected via maintenance.

10.4.1.2 REQUIRED:

a) Self-diagnosis coverage between missions
b) Self-diagnosis coverage during missions
c) Ability to identify which safety related FCRs are working, have activated faults, and have failed
d) Avoid accumulation of faults over time, especially accumulation of latent faults and latent coincident faults
e) **Pitfall:** Enabling, disabling, or changing the behavior of self-diagnosis, logging, data recording, data reporting, and other similar functions is prone to changing the behavior of the item.
   EXAMPLE: Logging enabled during testing is disabled when shipping production items, resulting in timing-based item malfunctions that only occur with logging disabled.

10.4.1.3 HIGHLY RECOMMENDED:

a) Logging of detected faults and failures, including transient events.
   See also: requirement to log incidents (Section 10.6.8).
b) Logging and management of deferred maintenance
   EXAMPLE: Extended operations occur in degraded mode above MEL but with fewer than all components functional due to operational demands, budget limitations, or scarcity of spare parts
c) Temporal and data storage isolation between item functions and data logging items.
d) Reintegration strategy after:
   1) Transient faults
   2) Intermittent faults
   3) Faults that occur during a mission
   4) Faults that occur between missions
   5) Non-operational faults including short term and long-term storage
   6) Faults that occur during maintenance
e) **Pitfall:** Automatic reintegration of components that have recovered from a fault is prone to latent fault accumulation and coincident fault accumulation
   EXAMPLES: Intermittent faults (latent fault accumulation); multiple components accumulating faults that cause them to have matching failure behaviors (coincident fault accumulation) over the course of multiple missions.

10.4.1.4 RECOMMENDED – N/A

10.4.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.4.1.6.1 NOTE: Faults and failures covered by this clause are intended to be expansive. They cover but are not limited to component faults (e.g., RAM bit flip), a fault containment region failure (e.g., failover to standby, detection of multi-channel disagreement), and failsafe activations (e.g., watchdog timer reset)

See Also: Section 6.2 Fault Models.

10.4.2 Fault detection capabilities shall be acceptably effective and timely.

10.4.2.1 MANDATORY:

a) Identification of safety related fault detection capabilities, including for each capability at least:
   1) Component or function covered
   2) Specific portion of relevant fault model covered, with justification
   3) Fault detection latency, with justification
b) Traceability of fault detection capabilities (including coverage) to MEL

10.4.2.2 REQUIRED:

a) Inclusion of Built In Self-Test (BIST) capabilities executed with justified frequency
b) Justification of adequacy of BIST coverage.
c) Detection of:
   1) Power failure
   2) Thermal faults
      EXAMPLE: Clock throttling due to high temperature causes missed real time deadlines; intermittent faults due to exceeding design temperature range limits
   3) Unauthorized safety related equipment modifications, including unauthorized software and configuration data
d) **Pitfall:** High latency fault detection is prone to permitting an accumulation of faults
e) **Pitfall:** Low coverage fault detection is prone to permitting an accumulation of faults
f) **Pitfall:** Self-diagnosis is prone to providing only partial test coverage
g) **Pitfall:** The presence of an architected BIST, monitoring, or redundancy capability is prone to overstatement of effectiveness if fault coverage is not supported by evidence
   NOTE: A BIST capability that only achieves low coverage of a component might not provide acceptable fault detection. Simply having BIST capability does not automatically ensure acceptable fault detection coverage.

10.4.2.3 HIGHLY RECOMMENDED:

a) Use of the following fault detection methods as appropriate for the item:
   1) Built In Self-Test (BIST) capabilities between during missions
   2) Built In Self-Test (BIST) capabilities executed during missions
   3) Built In Diagnostics (BID) capabilities executed between missions
   4) Built In Diagnostics (BID) capabilities executed during missions
   5) Justification of BID coverage
   6) Use of runtime monitoring
   7) Use of redundant component cross-checks
   8) Use of diagnostic service tools for screening for latent faults
   9) BIST and monitor capabilities acceptably isolated from the components being tested to avoid correlated faults
   10) BIST and monitor capabilities themselves tested to ensure they are working properly
   11) Data integrity and sanity checks
   12) Timing failure checks and sequence failure checks

10.4.2.4 RECOMMENDED:

a) Use of proof tests with justified frequency and coverage
NOTE: Proof tests, including automatically performed proof tests, can be useful to ensure that seldom-used mechanisms and functions have not accumulated latent faults.
EXAMPLE: Exercising parking brake periodically if not normally used in operational service and counted upon as a last-ditch braking mechanism.

10.4.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.4.3 Fault diagnosis capabilities shall be acceptably effective.

10.4.3.1 MANDATORY:

a) Identification of fault diagnosis strategies
b) Identification of safety related fault diagnosis capabilities, including for each capability at least:
    1) Component or function covered
    2) Identification of relevant fault model
    3) Specific portion of relevant fault model covered, with justification
    4) Fault diagnosis performance
    EXAMPLE: False positives, false negatives
    5) Fault diagnosis granularity
    EXAMPLES: Subsystem, field replaceable unit (FRU), FCR, other component

10.4.3.2 REQUIRED:

a) Traceability of fault diagnosis capabilities (including coverage) to defined MEL(s)
b) Traceability of fault diagnosis capabilities (including coverage) to defined FCRs
c) Validation of identified fault diagnosis capabilities
d) Identification of fault diagnosis timeliness requirement, if any
NOTE: To the extent that fault diagnosis is used for risk mitigation during item operation, timeliness of diagnosis is likely to be a relevant factor.
e) **Pitfall:** Incorrect or inaccurate fault diagnosis results is prone to permitting an accumulation of latent faults
f) **Pitfall:** False positives that degrade available components below the minimum safe MEL during operation are prone to causing unsafe item behavior due to shedding of resource redundancy.

10.4.3.3 HIGHLY RECOMMENDED – N/A

10.4.3.4 RECOMMENDED:

a) Stress testing to characterize unintended fault diagnosis triggering and false alarm rates.

10.4.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.4.3.6.1 NOTE: While as a practical matter high-performing fault diagnosis is essential for maintainability, for safety assessment the emphasis is more likely to be on ensuring that any required diagnosis is accurate rather than the extent of coverage of the diagnosis capability so long as BIST has high coverage. False negative fault detection/diagnosis can impair safety by reintegrating faulty components as if they were fault-free.

10.4.3.6.2 NOTE: This clause is intended to cover equipment, not engineering design process issues. See the Section 9 Software and Item Processes for those issues.

10.4.4 Fault mitigation capabilities shall be acceptably effective and timely.

10.4.4.1 MANDATORY:

a) Identification of safety related fault mitigation capabilities, including for each capability at least:
    1) Component or function covered
    2) Fault mitigation coverage (i.e., what portion of fault model is mitigated)
    3) Fault mitigation latency, with justification
b) Traceability of fault mitigation to net fault model coverage
c) Traceability of fault mitigation capabilities (including coverage) to MEL

10.4.4.2 REQUIRED:

a) **Pitfall:** Fault mitigation via reboot is prone to repeated reboots if a permanent fault has occurred but the reboot mechanism assumes all faults are transient.
   EXAMPLE: This Pitfall might be avoided by setting a limited number of reboots before hard failure to detect repeated intermittent faults
b) **Pitfall:** Experimentally determined latencies are prone to overlooking infrequent worst-case latencies unless backed by real time analysis
   EXAMPLE: Use of rate monotonic analysis to ensure latency deadlines will be met.
c) **Pitfall:** High mitigation latency is prone to permitting mission critical item malfunctions when operational time constants are shorter than the mitigation latency
d) **Pitfall:** Fault mitigation techniques are prone to failure if at least one additional fault occurs during a recovery interval unless this is specifically considered design of the recovery mechanism

10.4.4.3 HIGHLY RECOMMENDED:

a) Fault masking
b) Failover capability
   EXAMPLES: Hot standby, warm standby, cold standby
c) Failsafes and other safety functions
d) Functional safety analysis regarding use of failsafes and other safety functions
e) Reboots for transient faults with mechanism to confirm faults are not permanent
f) Component reintegration after fault when component diagnosis indicates it is fault-free
g) **Pitfall:** Fault masking techniques are prone to hindering fault detection capability of faults that have been masked
   EXAMPLE: A failed unit in a two-out-of-three voting arrangement can be masked by two

good units outvoting it if the failure is not annunciated, leading to a later accumulation of coincident faults in which a second failed unit pairs with the first failed unit to out-vote the remaining good unit

h) **Pitfall:** Failover capability is prone to malfunction if spare resources have latent faults.

10.4.4.4 RECOMMENDED – N/A

10.4.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.5 Item robustness

10.5.1 The item shall be acceptably robust.

10.5.1.1 MANDATORY:

a) Definition of robust design elements, associated robustness thresholds, and expected robust item responses

b) Ability to detect and manage safety related activated faults and failures in ego vehicle
EXAMPLES: mechanical failure, uncommanded behavior

10.5.1.2 REQUIRED:

a) Detection of unexpected operational data to degree practicable
EXAMPLES: Distributional shifts, surprises

b) Detection of violations of assumptions made in safety case

c) Ability to react to and mitigate robustness-associated failures

d) Detection of incorrect confidence values (if used)
EXAMPLES: Erroneous classification confidence

e) Detection of incorrect prediction values (if used)
EXAMPLES: Erroneous motion prediction

f) Detection and reporting adverse events for which risk was previously “unknown”

g) Detection and reporting of adverse events for which risk was previously “accepted”

h) Supporting evidence records and accumulates assumption violations even if no change in the safety case has (yet) been required.
NOTE: This is expressly intended as a countermeasure to prevent repeated dismissals of assumption violations as “one off” events in denial of an accumulating pattern of violations.

i) Detecting and reporting negative consequences of changes
EXAMPLES: Fixes, retraining, updates

j) Detection of perception robustness deficiencies
See also: Perception, Section 8.4.

k) Ability to compensate for errors and misbehaviors of ego vehicle and other vehicles, pedestrians, and other objects
EXAMPLES: Sensor failures, infrastructure failures, surprise object, surprise event, behavioral rule violations

l) Ability to manage faulty behavior by passengers and cargo
EXAMPLES: Passengers not wearing seatbelts, passenger climbing out window while moving, unsecured cargo, cargo spill
m) Detection of ambiguous data, inconsistent data, commands, operational modes across subsystems
n) Field data on faults experienced to improve fault model
o) **Pitfall:** Arguments based on a statement that there is low risk of “surprises” that attempts to justify little or no monitoring for surprises is prone to missing real-world surprises due to unanticipated changes in the operational environment.
NOTE: Even if evidence contains an overwhelming amount of field data for which surprises have been aggressively monitored, the risk to such an argument is that the surprise will be an unanticipated change in the operational environment.

10.5.1.3 HIGHLY RECOMMENDED:

a) Ability to deviate from normal operational rules in an acceptable manner
EXAMPLES: Circumnavigating lane blockage, safe roadway departure to avoid collision with wrong-way other vehicles

10.5.1.4 RECOMMENDED – N/A

10.5.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.5.1.6.1 NOTE: The ability to detect “surprises” represented by the required elements is limited in practice by various factors including inherent limitations of the item to sense its internal state and environment. It is relevant to consider the criticality of each type of detection to the safety case overall. The more uncertainty there is as to completeness of evidence or other argument that the item is not brittle, the more critical it is to detect robustness issues.

10.6 Incident response

10.6.1 The item shall be able to detect and react acceptably to incidents and loss events.

10.6.1.1 MANDATORY:

a) Detection of loss events
b) Incidents detected to the degree that detection is practicable

10.6.1.2 REQUIRED:

a) Reporting of detected incidents and loss events (See Section 12.5)
b) Recording of relevant data
c) Tracing of incidents and loss events to identified hazards, resulting in safety case analysis (See Section 12.6.1)
d) **Pitfall:** Arguments that a loss event is the fault of some other system or other external cause are prone to resulting in an item that unnecessarily puts itself in risky situations or

behaves in a way that sheds blame onto others.
EXAMPLE: An ego vehicle that cuts into a too-small space between other vehicles and then panic brakes to avoid a collision might be hit from behind, shedding blame for an unsafe cut-in onto the trailing vehicle that hit the ego vehicle from behind during the panic stop

10.6.1.3 HIGHLY RECOMMENDED:

a) High coverage of hazard to incident detection traceability (i.e., hazard mitigation failures that manifest as incidents can be detected even if there is no loss event)

10.6.1.4 RECOMMENDED – N/A

10.6.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.6.1.6.1 NOTE: One specific type of incident of note is a failure of a primary subsystem that results in activation of a backup subsystem or a failure that causes a switch to a degraded operational mode, even if no loss event occurs. (Note that intentional switches to a backup or degraded operational mode according to reasons such as a designed response to ODD changes, periodic diagnosis, and the like are not “failures” in this sense.) Non-limiting examples of incidents that are reported when practicable are:

a) Activation of a backup capability due to a problem with a primary capability. (Note that diagnosis might reveal this is an expected random failure within the tolerance of the safety argument, but this cannot simply be assumed without analysis of the event and/or analysis of the failure rate.)
b) Close call vehicle near-collision (e.g., vehicles passes closer than minimum designed safety distance to pedestrian, obstacle, or other vehicle).
c) Pedestrian jumps out of the way of a vehicle that would otherwise have resulted in a close call or impact.

10.6.2 The argument shall demonstrate that the item can detect loss events.

10.6.2.1 MANDATORY:

a) Ability to detect when item has plausibly been involved in a fatality, or significant human injury, even if any physical impact force would not otherwise be considered substantial
    1) Includes pedestrians, occupants, other road users
    2) Includes non-contacting events
    EXAMPLE: An abrupt ego vehicle maneuver is associated with an adjacent car swerving off the road to avoid impact with an unsafely behaving ego vehicle, resulting in a crash of that adjacent car. “Blame” might be unclear, but a reasonable human driver might be expected to stop at the scene when realizing that such a crash has occurred. It is conceivable there might be some instances (but certainly not all instances) in which a human driver would not realize that a crash occurred.

NOTE: While such detection might be difficult to achieve in a purely automated way, it is still required to avoid a potentially involved vehicle leaving the scene of a serious loss event for which the ego vehicle might be burdened with a share of the blame.

10.6.2.2 REQUIRED:

a) Detect when item has been involved with a fatality
b) Detect when item has been involved with a significant human injury
c) Detect when item has been involved with non-trivial property damage
d) Detect when item has been involved with non-trivial environmental damage
e) Detect when item has had an impact with an obstacle, other vehicle, or other objects that can reasonably lead to damage to either the vehicle or damage to the object impacted

10.6.2.3 HIGHLY RECOMMENDED:

a) Detect when vehicle has violated an assumption or argument in the safety case, even if that violation does not result in a loss event

10.6.2.4 RECOMMENDED:

a) Use of disagreement between redundant sensing and perception items to detect incidents that might have escaped designed incident detection capabilities
b) Lack of a detected incident when other available information reveals a problem with item performance treated as a potentially substantive lack in monitoring capability
c) Consider assumption violations to be incident precursors

10.6.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.6.2.6.1 NOTE: A primary intent is to ensure that the item is not involved in the analogy of a hit-and-run loss event involving either human victims or property damage.

10.6.2.6.2 NOTE: Incident and loss event reporting will be limited in practice due to sensor capability. In particular, if an incident takes place due to an undetected object, then the item might not have a way to detect that incident actually occurred. It is expected that such reporting will involve false positives and false negatives depending upon whether the item correctly or incorrectly resolved potentially conflicting data during operation. Nonetheless, a high false negative rate might mask missed incidents that are strongly predictive of high severity future loss events.

10.6.2.6.3 NOTE: The ability to detect assumption violations will be limited in practice, but can be a component in a feedback item that encompasses detection of safety case argument and evidence defects by using vehicle capabilities and other methods.

See also: incident metric recording and analysis information in Metrics and Item Safety Performance Indicators (SPIs), Section 16.

10.6.3 The item shall detect and respond to impending loss events.

10.6.3.1 MANDATORY:

a) Defined best-effort response to reduce the expected severity of an unavoidable but detected impending loss event.

10.6.3.2 REQUIRED:

a) Defined response is effective in reducing severity of impending loss event
b) **Pitfall:** Arguments that a particular type of loss event is impossible are prone to being incorrect due to unstated or incorrect assumptions
REFERENCE: https://www.britannica.com/topic/Titanic accessed 24 June 2019.
c) **Pitfall:** Arguments that some "no win" situations are impossible to avoid as support for weak impending loss event detection is prone to understating the degree of mitigation that is achievable in practice.

10.6.3.3 HIGHLY RECOMMENDED:

a) Consideration of ethical issues in defining an impending loss event severity mitigation approach.
EXAMPLE: If a collision is impending and no alternate path can be identified that will avoid a collision between the ego vehicle and some object, the current path is taken with maximum braking force applied and deployment of external pedestrian impact mitigation technology (e.g., pedestrian air bags).
NOTE: This is not a requirement for embedding ethical decision making logic in the item. Nor is it a requirement to solve controversial ethical dilemma thought experiments such as the "Trolley Problem." It is, however, a recommendation to consider whether the chosen strategy reasonably considers societal norms and ethical considerations, and a recommendation to have a defined approach.

10.6.3.4 RECOMMENDED:

a) Prediction of risky situations to reduce the chance of being placed in a no-win situation

10.6.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.6.3.6.1 NOTE: While not all loss events will be avoidable, it is important to ensure that reasonable efforts have been taken to avoid putting the item into an excessively risky situation in the first place (so as to avoid entering a situation that is prone to creating then-unavoidable loss events) and also to attempt to minimize the severity of a loss event.

10.6.4 The item shall react acceptably to incidents.

10.6.4.1 MANDATORY:

a) Define an incident taxonomy
b) Define incident response strategies and argue acceptability
c) Validate incident response strategies

10.6.4.2 REQUIRED:

a) If incident handling operational modes are used:
    1) Define incident handling operational modes and trace to incident taxonomy
    2) Define entering and exiting conditions for each incident handling mode
    3) Define behaviors and other aspects of each incident handling mode
    4) Justify acceptability of each incident handling mode for identified incident scenarios
b) Incident data reporting to first responders (dispatch; on-scene)
c) Triggering first responder cooperation functions
d) Incident data reporting to other on-scene humans
e) Ensure that defined behaviors consider safety of on-scene humans, including first responders
f) Incident data reporting to central engineering function for field engineering feedback
g) Triggering vehicle safing functions
h) Triggering vehicle egress functions
i) Triggering vehicle internal and external display functions
j) **Pitfall:** Arguments that assumes that post-crash vehicle functionality relating to post-crash safety is unimpaired by the crash are prone to overlooking the crash itself as a common cause of failures, especially for severe crashes that compromise multiple vehicle fault tolerance isolation zones
    EXAMPLES: A high energy collision can compromise redundant electrical power supplies, redundant sensors (e.g., door closed switches), and redundant actuators (e.g., door release actuators) even if physically placed in different zones for purposes of more general zonal redundancy.

10.6.4.3 HIGHLY RECOMMENDED – N/A

10.6.4.4 RECOMMENDED – N/A

10.6.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.6.4.6.1 NOTE: The scope of an “incident” includes failures to acceptably mitigate at least one hazard whether it results in a loss event or not. For example, a vehicle might suffer an equipment problem that causes it to violate traffic regulations (e.g., running a red light). There might not have been a collision, but the situation should still be treated as if a crash had occurred in terms of field engineering feedback, and potentially other ways.

10.6.4.6.2 NOTE: Electrical safety (e.g., battery design, post-crash high voltage safety) is beyond the scope of this standard. However, to the degree such items rely upon an accurate incident detection capability from the item (e.g., to de-energize power buses), providing that accurate detection is within the scope of this standard.

10.6.4.6.3 NOTE: An example of a crash causing damage that compromises post-crash failure is an item which is designed to immobilize the vehicle when a door is open. Assuming first responders are told a vehicle cannot move if a door is open, a hazard could be created if crash

damage has impaired that function. Consider if the door is open but the door open sensor (or associated cabling) has been damaged in a crash. This could (if engineered countermeasures have not been taken) provide a false door-closed signal that leaves the vehicle able to move when emergency responders are in close proximity (e.g., tending to an injured victim who has been ejected to a location in front of the vehicle). Even multiple door closed signals might have a common cause failure if a side impact has compromised all door switch zones for that door.

10.6.5 Item hazards and risks related to post-incident status shall be mitigated.

10.6.5.1 MANDATORY:

a) Identify post-incident operational modes and corresponding safety related behaviors. This includes:
    1) After crashes, regardless of vehicle role in causing crash and crash severity
    EXAMPLES: Significant crashes and fender benders
    2) After detected non-crash incidents

10.6.5.2 REQUIRED:

a) Post-incident operational modes are effective at mitigating risks
b) Vehicle immobilized as appropriate responsive to involvement in a significant loss event
    1) Immobilize vehicle motion
    2) Immobilize auxiliary equipment
    3) De-energize electrical items
    4) Consideration of situation surrounding vehicle
    5) Consideration of emergency responders
    6) Consideration of passengers
    7) Consideration of potential non-passenger victims

    EXAMPLE: Post-crash vehicle immobilization to provide increased safety to first responders and potential victims even if degraded mode MEL is available.

    NOTE: Unconditional immobilization of vehicle and other item shutdown after a crash may be acceptable if vehicle damage and environmental situation cannot be reasonably assessed
c) Notify first responders of loss event
d) Identify post-incident support features
    1) Control and operational feature bypass to facilitate passenger egress and rescue
    2) Annunciation of item operational mode and degree of immobilization
    3) Capability to transition into maintenance mode as necessary
    EXAMPLE: Drivetrain switched to “neutral” by qualified personnel to facilitate extrication and towing
    4) Mechanism supporting positive confirmation of fitness to operate before resuming service
e) Argue acceptable risk mitigation by and for post-incident operational modes and features

10.6.5.3 HIGHLY RECOMMENDED:

a) Vehicle incident handling capability after interactions with other road users or other objects that can reasonably be expected to have provoked or contributed to a loss event
EXAMPLE: Ego vehicle aggressively cuts off another vehicle and that other vehicle crashes immediately afterwards. Ego vehicle stops at scene and renders/summons assistance as possible.
b) Mechanism for permanent vehicle immobilization
NOTE: “Permanent” could be with regard to a crash scene and recovery. Such a mechanism could be over-ridden or reset during maintenance if deemed appropriate by qualified maintenance personnel.

10.6.5.4 RECOMMENDED:

a) Other situations in which the ego vehicle should alter operations as a result of a proximate crash, loss event, or incident even if the ego vehicle did not actually hit anything.

10.6.5.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

10.6.5.6.1 NOTE: This section is intended to encompass risks that occur related to a crash or other incident after which the vehicle should reasonably be expected to cease normal operations. For example, the ego vehicle might barely miss a cyclist or pedestrian, with a reaction that the at-risk road user loses balance and falls. Or the ego vehicle might interfere with a human-driven vehicle operation in a way that prompts the other vehicle to crash even though no actual contact has been made. A reasonable human driver would (arguably) be expected to stop as if an actual crash had occurred since the ego vehicle’s interaction was potentially a factor in the crash. This clause deals with the need to behave in a different way at a crash, accident, or incident scene compared to normal operations. That behavior starts at the time of the incident and ends either when the vehicle transitions to a maintenance mode (e.g., for transport) or back to normal operations. Blame is not considered a factor in determining whether to enter an incident response mode, and indeed blame might not be readily assignable at the time of the incident. Violation of this clause can potentially result in a “hit and run” type incident. It is up to the developer to identify and implement a strategy for this clause.

10.6.6 Post-incident hazards shall be identified.

10.6.6.1 MANDATORY:

a) Hazards due to post-incident conditions, including damage to or malfunction of risk mitigation mechanisms, including at least:
    1) Unexpected vehicle motion
    2) Unexpected activation of emergency equipment
    EXAMPLE: Airbag deployment after crash sequence has ended
    NOTE: Airbag deployment might be handled by a subsystem completely

independently of the item. However, the safety case needs to establish this independence if true.

10.6.6.2 REQUIRED:

a) Hazards due to post-incident conditions, including damage to or malfunction of risk mitigation mechanisms, including at least:
   1) Unexpected motion of vehicle components
      EXAMPLES: Door opening, startup of hybrid vehicle internal combustion engine
   2) Laser safety
      EXAMPLE: Beam stops scanning for a laser that is argued eye-safe in part because of scanning
   3) Radar safety
      EXAMPLE: Non-eye-safe radar activation near human head in an incident response scenario
   4) Other active emitter safety
   5) Compromise of high voltage shutoff features
      EXAMPLE: Crash damages high voltage shutoff contactor, leaving high voltage supplies energized without fault annunciation during emergency responder extrication attempts

10.6.6.3 HIGHLY RECOMMENDED:

a) Hazards due to incorrect understanding of item operation and ambiguities in item state by occupants, bystanders, and first responders, including for example:
   1) Vehicle “safe” mode activation
      EXAMPLE: Lack of vehicle movement is mistaken for a disabled vehicle when in reality the vehicle state is waiting for the next ride hail event to start moving.
   2) Incorrect vehicle identification for remote control and diagnosis
      EXAMPLE: The wrong vehicle remotely disabled due to confusion or remote operator error in identifying involved vehicle(s) at a crash scene
   3) Vehicle occupants unaware that they should evacuate after an incident
      EXAMPLES: Sleeping occupants, non-native language speakers, children, adults heavily under the influence of alcohol do not evacuate from an unsafe vehicle.
   4) Vehicle occupants unaware of safety features
      EXAMPLE: Mechanical emergency egress release is located behind an unmarked speaker grill, requiring knowledge of procedure to remove a particular speaker grill to activate emergency egress functionality for a passenger who is not familiar with or not capable of activating that feature.

10.6.6.4 RECOMMENDED – N/A

10.6.6.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence.

10.6.7 Post-incident risk mitigation behaviors shall be identified.

10.6.7.1 MANDATORY:

a) Identify item behaviors, requirements, and other aspects of item design relevant for mitigating each identified post-incident risk in each post-incident operational mode

10.6.7.2 REQUIRED:

a) Include scope of at least:
    1) During-incident occupant protection features
    2) Post-incident occupant protection features
    3) Occupant egress features
    4) Occupant education and direction for performing any actions assumed by safety case
    5) Any required occupant knowledge of item state
    6) First responder access to vehicle and occupants
    7) First responder education regarding instructions and procedures required for safe handling of incidents
    NOTE: One approach in support of this is just-in-time delivery of vehicle information at a crash scene. However, general familiarity before responding to a crash can also be desirable, especially with potentially non-standardized aspects such as battery safety procedures and safe extrication cutting locations
    8) First responder knowledge of item state
b) Define fault model for safety related post-incident behaviors and requirements

10.6.7.3 HIGHLY RECOMMENDED:

a) Incident scenarios include at least the following:
    1) Passenger trapped inside vehicle unable to egress from undamaged vehicle
    EXAMPLES: Children, injured humans, incapacitated humans, pets
    2) Access to and egress from stable damaged vehicle
    3) Access to and egress from unstable damaged vehicle
    EXAMPLES: Battery fire, engine fire, vehicle disabled due to flooding, vehicle immersion, vehicle partially over a cliff edge, vehicle in a treetop
b) Fault model includes potential compromise of zonal isolation, redundant sensors, etc. due to catastrophic crash damage

10.6.7.4 RECOMMENDED – N/A

10.6.7.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence as well as demonstration.

10.6.8 The item shall report item status, operational parameters, faults, incident, and loss event data with acceptable forensic validity.

10.6.8.1 MANDATORY:

a) Define approach to incident and loss event data recording and reporting

b) Define approach to data retention
c) Defined incident and loss event data recording and reporting sufficient to enable reconstruction
    1) Ego vehicle item status
       EXAMPLES: Operational mode, equipment status, operational parameters, hardware configuration, software configuration
    2) Perception pipeline state
       EXAMPLES: Object list, confidence measurements, prediction values, planning information, trajectory information
    3) Timing information
       EXAMPLE: Time stamps for sensor samples and object trajectories

10.6.8.2 REQUIRED:

a) Sufficient data available to reconstruct the events surrounding an incident or loss event so as to perform root cause analysis.
   NOTE: It is acknowledged that the vehicle can only provide its own internal sensor and state information, which is not necessarily a complete reconstruction of objective ground truth. It is also likely that events will occur for which data recording is found to be inadequate in an unforeseen way, in which case data recording is improved based upon feedback in response to that event.
b) Data dictionary and data format definition of data reported that is relevant to fault detection, fault diagnosis, incident reporting, and incident reporting
c) Measures to ensure that the accuracy, precision, and integrity of reported data is defined and assured
d) Information to diagnose faults in safety related machine learning and other nontraditional algorithmic functions
e) **Pitfall:** Reporting the outputs of software-based items that have malfunctions is prone to producing erroneous output data that reflects the state of faulty software execution rather than the actual state of the item.

10.6.8.3 HIGHLY RECOMMENDED:

a) Definition and reporting of minimal post-incident data with the same level of integrity as the item-level hazard
   NOTE: If the sensor is wrong, the software reading the sensor is wrong, or memory holding sensor readings is corrupted, the report will be wrong. Incorrect reporting can impair the operation of safety process feedback loops, degrading or negating the validity of argument based on the effectiveness of feedback loops in identifying and correcting previously unrecognized hazards.
   EXAMPLE: Data required to establish the root cause of a fatal loss event should have the same criticality as life critical item functions.
   EXAMPLE: Vehicle status is reported from a non-life critical subsystem X that is convenient to the data logger. However, that subsystem X has a defect that in some cases misreports dangerous values of life critical operating parameters as benign.

Incidents occur that could be diagnosed with accurate information regarding that life critical operating parameter. Incident investigations use the logger data and incorrectly believe that a defective life critical function is non-faulty, when in fact both the value produced by the defective function was faulty and subsystem X's report of the value was itself faulty. This results in a life critical defect being undiagnosable because of a low integrity reporting item and potentially blamed on some other cause. (A similar problem can occur if the data logger itself has insufficient integrity.) For an historical example, see the discussion of ion chamber saturation with regard to the Therac 25 in: Leveson & Turner, "An investigation of the Therac-25 accidents," IEEE Computer, July 1993, pp. 18-41.

b) Periodic logging of status and health of significant item components, including sensors, actuators, and computational elements
c) Time-stamped data
d) Recorded sensor feeds
e) Feedback from incident investigations as to data ambiguities, inadequacies, and other issues using reported data is credibly attributed a root cause, then tracked to resolution
f) **Pitfall:** Undersampled data is prone to supporting incorrect diagnosis conclusions
NOTE: Consider meeting Nyquist sampling criteria (or better) as adapted for the specifics of signal characteristics
EXAMPLE: Vehicle control data logged every 1000 msec by a pre-crash data logger is not able to detect physically realizable changes in control commands.
g) **Pitfall:** Low integrity data logging and reporting is prone to resulting in incorrect root cause analysis of potentially safety critical item defects.

10.6.8.4 RECOMMENDED:

a) Ensure tamper evident via strong cryptographically secure data integrity checks
EXAMPLE: Provide robust chain of evidence integrity tracing back to a crash event
b) Ensure nonrepudiation of data
c) Ensure that fault attribution data is recorded at the highest level of item criticality
EXAMPLES: Sensor data recorded does not pass through unacceptably low criticality components or has sufficient integrity protection to provide evidence of integrity
d) Address privacy concerns in accordance with security plan
e) Record nondeterministic item state to aid in behavior reconstruction
EXAMPLE: Log pseudo-random seed values and local time stamp values periodically if used for non-deterministic algorithms
f) Consider regulatory, legal, and first responder considerations that affect reporting content and timeliness requirements.

10.6.8.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.6.8.6.1 NOTE: A specific example of an unacceptable data reporting item in conventional vehicles is an Event Data Recorders (EDR) which captures accelerator pedal position. In at least some historical vehicles what is really being captured is not a high integrity recording of the pedal position, but rather the result of low integrity software pedal readings, low integrity

data storage operations, and low integrity data reporting software. The value reported is not even (necessarily) the same data source as the pedal position being used by the high integrity portion of the item. Moreover, EDRs on conventional vehicles typically sample data only once per second, while the time constants of human pedal operation are an order of magnitude faster. Therefore, an EDR report of “foot on accelerator” does not mean that the human driver actually had foot on accelerator, but rather that a potentially defective piece of low integrity software thought that was the situation. Similarly, an EDR report of “foot off brake for 1 second” might miss that the foot was actually on the brake (due to incorrect data) or that the driver had a foot actually on the brake for 900 msec between data samples.
See also: Metrics and Item Safety Performance Indicators (SPIs), Section 16.

10.6.9 A post-incident analysis activity shall be defined and executed.

10.6.9.1 MANDATORY:

a) Define approach to collecting data from incidents (including loss events)
b) Define approach to analyzing data and initiating safety case updates (see Section 12.6)
NOTE: In general this corresponds to the notion of an “accident investigation” process.

10.6.9.2 REQUIRED:

a) Effectiveness of approach to data collection
b) Effectiveness of data analysis and safety case update approach
c) Retention of analysis results for life of item cohort
d) Effective execution of approach in response to incidents
e) Update of hazard log in response to identified hazards

10.6.9.3 HIGHLY RECOMMENDED:

a) Automation support for routine incident processing and triage
NOTE: Quality control must be exercised over any automation to minimize the risk of a high criticality defect going unnoticed
b) **Pitfall:** Waiting for statistical evidence that a field anomaly is high severity before taking action is prone to accumulating an unacceptable number of loss events before correction.

10.6.9.4 RECOMMENDED:

a) Identification of and conformance to any legal and/or regulatory reporting requirements.

10.6.9.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

10.7 System timing

10.7.1 Real time requirements of the item shall be met.

10.7.1.1 MANDATORY:

a) Item timing analysis that addresses time constants, deadlines, and any built-in timing engineering margins
b) Defined real time scheduling approach

10.7.1.2 REQUIRED:

a) Each function in item meets its defined real time requirements (if any)
b) Timing analysis includes at least:
    1) Time constants of environment that place timing requirements upon the item
    EXAMPLES: Maximum vehicle speeds, time to implement trajectory correction before crash
    2) Time constants of the vehicle
    EXAMPLE: Time to brake, time to execute a steering command
    3) Cached and buffered data effects
    EXAMPLE: Map data freshness impaired by stale cached data in on-line data distribution system
c) Timing requirements for control stability

10.7.1.3 HIGHLY RECOMMENDED:

a) Use of at least one of:
    1) Rate monotonic analysis for safety related functions (includes deadline monotonic analysis)
    2) Time triggered design techniques for safety related functions
b) **Pitfall:** Design approaches not based on mathematically proven real time scheduling properties are prone to missing deadlines during unusual operational conditions
EXAMPLES: Use of earliest deadline first approaches, ad hoc mixed event-based and periodic items with high priority events, or prioritization based on perceived data importance rather than period and/or deadline
c) **Pitfall:** Item components not specifically designed for real time operation are prone to missing deadlines during unusual operational conditions
EXAMPLE: Use of a desktop operating system without an underlying real time scheduling layer
d) **Pitfall:** Experimental timing validation at the item level (i.e., by observing whether an entire item meets its overall timing goals) is prone to missing individual function timing misbehaviors that can contribute to item malfunctions in unusual operational conditions or heavy workloads

10.7.1.4 RECOMMENDED:

a) **Pitfall:** Timing approaches that leave no timing slack are prone to failure when some component experiences a transient timing anomaly

b) **Pitfall:** Event-based items are prone to real time constraint violations when encountering faults
EXAMPLE: “Event showers” due to component failures can cause resource overloads

10.7.1.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

10.7.1.6.1 NOTE: The requirements of this Section 10.7 are also intended to apply to autonomous item functions (See Also: Section 8.10 Timing).

10.7.2 Violation of real time requirements shall be detected and mitigated.

10.7.2.1 MANDATORY:

a) Defined detection and mitigation approach to item-level real time faults
EXAMPLE: Overloaded resources, missed deadlines, loss of control loop closure due to computing latency, timeouts

10.7.2.2 REQUIRED:

a) Effectiveness of real time fault detection and mitigation approach
b) Detection and mitigation of timing faults on a per-function basis for safety related functions
EXAMPLES: Detecting a missed deadline, hung task
c) Fault model that includes slow computing process, hung computing process
d) Proper use of watchdog timers and other timing monitors

10.7.2.3 HIGHLY RECOMMENDED:

a) Proper use of resource monitors
EXAMPLES: Free memory exhaustion, stack overflow detection, CPU overload
b) Fault model that includes resource starvation
c) Fault model that includes communication congestion and other real time latency faults
d) Software stress testing to validate timing margins

10.7.2.4 RECOMMENDED:

a) Techniques that statically allocate resources
EXAMPLES: Static allocation rather than dynamic allocation of memory, disable dynamic allocation after item startup

10.7.2.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

10.8 Cybersecurity

10.8.1 Hazards and risks related to cybersecurity shall be mitigated.

10.8.1.1 MANDATORY:

a) Reference a cybersecurity plan
NOTE: The cybersecurity plan can be maintained independently of the safety case. Some of the information required by this clause is supplied by that plan.

b) Identify hazards and risks related to cybersecurity, including topics related to:
   1) Confidentiality
   2) Integrity
   3) Availability

NOTE: As with other identified hazards and risks, other clauses in this standard require mitigation. Some risk mitigation might be completely argued in the safety case, but other risk mitigation is likely to depend upon the cybersecurity plan as discussed in Section 10.8.1.3.
See also Section 10.8.2.

10.8.1.2 REQUIRED:

a) Cybersecurity plan covers safety related threats and risks
EXAMPLE: A Threat Analysis and Risk Assessment (TARA) includes safety related threats that are linked to safety case hazard log.

b) Trace mitigation of cybersecurity related hazards and risks to cybersecurity plan contents
EXAMPLE: Hazards related to malicious software defects trace to the portion of the cybersecurity plan that covers software update integrity

c) Compatible safety and cybersecurity goals
   1) Identify cybersecurity goals that are potentially related to or conflicting with item-level safety goals
   NOTE: Conflict analysis might need to be done periodically in response to changes in the cybersecurity plan over time.
   2) Argue that the item as described in the safety case does not violate cybersecurity goals
   NOTE: This is only possible as a result of having compatible safety and cybersecurity goals, which will likely involve compromises on both sides while still achieving acceptable overall item risk for safety and security.
   3) Argue that cybersecurity risk treatments do not invalidate the safety case
   NOTE: Cybersecurity risk treatments can include a cybersecurity concept and cybersecurity specification.

e) Timely detection of software and item integrity failures
EXAMPLES: Periodic cryptographic integrity check of software images, intrusion detection

10.8.1.3 HIGHLY RECOMMENDED:

a) Co-design of safety and cybersecurity goals
NOTE: The needs of safety and security can conflict. However, the safety case and the cybersecurity plan will need to be compatible with each other, resolving any potential conflicts to create an item that is both acceptably safe and acceptably secure.

b) Reference risk treatment portion of cybersecurity plan using a SEooC interface. (See Section 5.7.3.)
NOTE: This permits the cybersecurity plan to provide evidence of security-related hazard mitigation under assumptions fulfilled by the contents of the safety case. The cybersecurity plan might impose additional argument interface requirements.

10.8.1.4 RECOMMENDED:

a) Ability to restore system to “factory default configuration”
NOTE: This can help recover from a cybersecurity attack, but raises issues regarding need to obtain and install updates before operation, and using a restore as a way to exploit vulnerabilities present in the factory default configuration but patched in later versions.

10.8.1.5 COMPLIANCE:

Compliance is checked via inspection of safety case, the cybersecurity plan, and evidence that the cybersecurity plan has been prepared by personnel qualified to execute a cybersecurity engineering program for the item considering its design and ODD.

10.8.1.6.1 NOTE: Defining a complete approach to security is out of scope for this standard. However, security is a significant concern with regards to safety. The requirements in this section (10.8 overall) are intended to assist with selecting an adequate security approach without being overly constraining.

10.8.1.6.2 NOTE: Assessment considers the existence of a cybersecurity plan and the aggregate coverage of identified prompt elements. However, assessment of the completeness, validity, and other aspects of the cybersecurity plan itself are outside the scope of this standard.

10.8.1.6.3 References: The following informative references may be useful in considering cybersecurity: SAE J3061, ISO/SAE 21434, BSI PAS 1885.

10.8.2 Fault models shall include malicious faults.

10.8.2.1 MANDATORY:

a) Include malicious type of faults and malicious component failures in identified fault models (See Section 6.2)
NOTE: The term “malicious” is used to evoke the notion of a non-random adversarial attacker who has knowledge of the weaknesses of a system. While faults indistinguishable from malicious faults might occur by chance, a malicious fault model makes it more difficult to argue that faults, assumption violations, and correlated events that can be intentionally caused by a motivated attacker are unlikely to occur by chance as might otherwise be done in a safety case.

NOTE: Mitigation for some malicious faults might rely upon assurances provided by the cybersecurity plan.

10.8.2.2 REQUIRED:

a) Alteration of the environment
EXAMPLES: Defaced signs, optical illusions drawn on roadway, alterations of road markings

b) Alteration of objects in the environment
EXAMPLES: Anti-face recognition makeup and hair styles, use of camouflage, intentionally unusual behaviors, adversarial attack images applied to clothing and objects

c) Malicious road user human behavior
EXAMPLES: Pedestrian group intentionally blocks vehicle, other vehicles attempt to run ego vehicle off road

d) Alteration of data feeds
EXAMPLES: Spoofed severe weather warnings, spoofed V2x transmissions

e) Data infrastructure attacks
EXAMPLES: Malicious alteration of map data, maintenance records, vehicle status information

f) Training data poisoning
EXAMPLES: Intentionally skewing distributions of objects, events, or other characteristics when training data is being collected

g) Supply chain attacks
EXAMPLES: Malicious insertion of code into components, accessories, and data loggers connected to vehicle; malicious compromise of hardware; malicious compromise of non-electronic components, supplies, and materials; cryptographic key material leaks

h) Installation of unauthorized components
EXAMPLES: Alternate supplier replacement components unwittingly installed that bear malicious software, wireless network connection devices added by vehicle owner or passenger, removable storage media with malicious payloads

i) Attacks via connected devices
EXAMPLES: Passenger electronic devices connected to system wired or wireless networks

j) Physical attacks on sensors
EXAMPLES: Paint gun used to blind camera, metalized balloons released on roadway

k) Physical attacks on information systems
EXAMPLES: Breaking off side view mirror to access vehicle network

l) Vehicle takeover attempts
EXAMPLES: Remote access via computer network, via local access by passenger, access to passenger voice interface, compromise of central dispatching infrastructure

m) Alteration of software images
EXAMPLES: Malware inserted into software updates, unauthorized update code intentionally installed by vehicle owner

10.8.2.3 HIGHLY RECOMMENDED:

a) Malicious access to data
EXAMPLES: stalkers, targeting of public figures

10.8.2.4 RECOMMENDED – N/A

10.8.2.5 COMPLIANCE:

Compliance is checked via inspection of safety case and cybersecurity plan.

10.8.2.6.1 NOTE: The prompt elements in this clause are primarily intended to cover security-related hazards that are specific to autonomous systems, including both physical attacks on the item's computing system and more indirect cybersecurity attacks. Some or all security prompt elements might be addressed by the cybersecurity plan. Other additional cybersecurity hazards are likely to be provided by the cybersecurity plan and are added to the hazard log if safety related.

11 Data and Networking

11.1 General

11.1.1 Risks related to data storage, data handling, and data transmission shall be acceptably mitigated.

11.1.1.1 MANDATORY:

a) Data Communications and Networks (see Section 11.2)
b) Data Storage (see Section 11.3)
c) Operational Infrastructure Support (see Section 11.4)
d) Cybersecurity (see Section 10.8)

11.1.1.2 REQUIRED – N/A

11.1.1.3 HIGHLY RECOMMENDED – N/A

11.1.1.4 RECOMMENDED – N/A

11.1.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

11.1.1.6.1 NOTE: A primary goal of this section is to ensure that the potential contributions of data network, data storage, and data processing failures to risk are acceptably considered.

11.1.1.6.2 NOTE: The emphasis of this standard is on a stand-alone autonomous item's safety. While such items can be an element in a system-of-systems context, argument regarding issues such as emergent properties of multiple autonomous products interacting beyond normal operational interactions is out of scope for this standard.

See also: Section 6.2.6 Data Fault Model.

REFERENCE: A source for general guidance on data safety is: [SCSC-127C] Data Safety Guidance (Version 3.0) by the SCSC Data Safety Initiative Working Group [DSIWG]

11.2 Data communications and networks

11.2.1 Item hazards and risks related to data transmission shall be mitigated.

11.2.1.1 MANDATORY – N/A

11.2.1.2 REQUIRED:

a) Identify data transmission related hazards
b) Mitigate data transmission contributions to risks

11.2.1.3 HIGHLY RECOMMENDED:

a) Remote updates to software, firmware, configuration data, and other safety related data performed in a secure and reliable manner
b) Conformance with the Standard for Safety for Remote Software Updates, UL 5500, or equivalent

11.2.1.4 RECOMMENDED – N/A

11.2.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

11.2.2 Data flows related to the item shall be identified.

11.2.1.1 MANDATORY:

a) Identify safety related data flows (if none, so state)
   NOTE: See below elements for scope of identification

11.2.1.2 REQUIRED:

a) Identify the presence of communication data flows for the item, whether deemed safety critical or not, including:
   1) Wired Networks
      EXAMPLES: Wired networks running Ethernet, CAN, FlexRay, MOST protocols
   2) Communication links including but not limited to: serial buses, multiplexed wiring links, dedicated serial transmission links
      EXAMPLES: RS-232, RS-485, SPI, I2C, LIN
   3) Radio communications
      EXAMPLES: V2x, WiFi, Bluetooth, 3G, 4G, 5G, other mobile communications, key fob data link, tire pressure monitoring item
   4) Non-radio wireless communications
      EXAMPLE: IrDA
   5) Human interfaces
      EXAMPLES: Screens, keyboards, driving controls
   6) Role of other sensors to receive encoded data values
      EXAMPLES: Video sensor used to receive data encoded as a bar code
   7) Other external interfaces to equipment
      EXAMPLES: Service tool interface, smartcard interface, dial-up connection, SMS data packet interface, OBD-II

   NOTE: The above prompt elements have overlap and cover both physical media and protocols. Precise categorization will depend upon sub-domain common terminology. Each data flow need only be included in one category.
b) For each identified interface (including both REQUIRED and any identified HIGHLY RECOMMENDED interfaces) describe:
   1) Components, functions, parties, etc. that are directly connected.

i) Communication participant management approach
ii) State if complete list of communication participants is not necessarily known
EXAMPLE: Broadcast radio signals sent or received might not have defined lists of network participants

2) Safety-related data that is sent or received on the data flow, if any.
3) Safety-related functions that directly or indirectly consume any aspect of the data flow
NOTE: A function can indirectly consume data if it consumes the results of a computation based on data received via a communication channel. In practice this can require a type of taint analysis with at least a non-malicious fault model to ensure that the effect of communication faults and failures are considered for safety related functions.
EXAMPLE: A hypothetical indirect failure scenario: time of day is received via GNSS and fed into a non-safety related software service. However, an anomalous time value causes that purportedly non-safety related service to hang. A safety related function calls that service to retrieve a time value, but hangs waiting for a response, causing a failure of the safety related function.

c) **Pitfall:** Interfaces not managed for safety and security are prone to creating unexpected avenues of failure and attack, even if entirely internal to the item.
d) **Pitfall:** Safety related functions that indirectly consume data flows are prone to being overlooked in data flow analysis.

11.2.1.3 HIGHLY RECOMMENDED:

a) Identify the presence of any of the following types of communication data flows for the item, whether deemed safety critical or not, identifying which are believed to be safety critical:
1) Remote access devices
EXAMPLES: Keyless entry, anti-theft devices, teleoperation devices
2) Charging infrastructure connectivity
3) Storage access ports
EXAMPLES: USB interface, SD card interface
4) Contact closures
EXAMPLES: Contact closure interface wires, switches, buttons, dials, key switches, jumpers
5) Analog data inputs
EXAMPLES: Potentiometers, analog interface wires
6) Other internal interfaces to equipment
EXAMPLES: TPM interface, daughter boards, JTAG interface
7) Connectivity to infotainment and internet service devices
8) Remote updates
EXAMPLES: Software, data, configuration

9) Live mission-related data flows
   EXAMPLES: Map data, traffic data
10) Connections to third party devices
   EXAMPLES: Occupant cell phones and computers
11) Other communications
   EXAMPLES: Reflective memory, memory bus to shared memory, inter-processor communication buses, dual-ported memory
12) Configuration interface
   EXAMPLES: Board jumpers
13) Teleoperation, including driving commands and/or remote supervision functionality, if present

b) Identify safety related outbound data flows
   EXAMPLE: Outbound traffic signal control over-ride device for an emergency vehicle, outbound safety related V2X signals

11.2.1.4 RECOMMENDED – N/A

11.2.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, design documents, and inspection of item.

12.2.1.6.1 NOTE: This clause supports both safety and security analysis. It is important to identify data flows so that correct categorization of safety and security relevance can be assessed.

12.2.1.6.2 NOTE: The distinctions in terminology between networks, communication links, “mixed” wires, etc. are flexible. The important net result is that all communication links are considered.

12.2.1.6.3 NOTE: Communication and data storage outside the boundaries of the vehicle can contribute to risk. This standard is written from the point of view of a single vehicle, so those risks are aggregated into the risk that an inbound data flow contributes to item risk.

11.2.3 The safety case shall identify risk mitigation mechanisms and techniques applied to identified data flows.

11.2.3.1 MANDATORY – N/A

11.2.3.2 REQUIRED:

a) Specify for each data flow identified responsive to Section 11.2.2:
   1) Fault model relevant to each data flow (see Section 6.2.5 which discusses communication fault models)
   2) Safety criticality of data flow
   3) Fault containment region boundaries crossed by each dataflow
   4) Description and analysis of effectiveness of fault and failure mitigation approaches

b) Data integrity approach, with description of specific integrity function used.
EXAMPLES: Parity, checksum, CRC, cryptographic integrity function, redundant transmission

11.2.3.3 HIGHLY RECOMMENDED:

a) Data logging
b) Span of data integrity approach
EXAMPLES: Hop-by-hop, end-to-end on communication link, precomputed integrity check values
c) Data authentication approach
EXAMPLES: Insecure hash (e.g., CRC), secure hash, digital signature
d) Timing and sequencing assurance
EXAMPLES: Nonces, sequence numbers, time stamps
e) Data secrecy approach in accordance with security plan
EXAMPLES: Encryption including specific algorithm used
f) Conflict resolution between data flows
EXAMPLE: Different subsystems generate different commanded positions for actuators; remote teleoperation control commands conflict with local autonomy control commands

11.2.3.4 RECOMMENDED:

a) Anomalous data detection and reporting
b) Protocol versioning
EXAMPLE: Protocol version transmitted as part of message

11.2.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence and design documents.

11.2.3.6.1 NOTE: Data flows are often associated with security requirements. Arguments that data flow integrity and other safety related data flow properties is likely to be closely tied to the security approach. **See also** Section 10.8.

11.2.4 Risk mitigation shall address hazards associated with each identified data flow.

11.2.4.1 MANDATORY:

a) State risk mitigation required and method of risk mitigation for each identified data flow.

11.2.4.2 REQUIRED:

a) For each data flow that crosses between a lower integrity portion of the item and a higher integrity portion of the item, argue that that:
    1) The operation of safety related functions cannot be impaired by data faults from the lower integrity portion, applying the union of the fault model from the lower integrity portion of the item and the fault model of the higher integrity portion of the item to this analysis.
    2) Inputs to safety related functions cannot be compromised in an unsafe way by the lower integrity portion of the item.

3) Outputs of the safety related function cannot be compromised in an unsafe way by the lower integrity portion of the item.
4) Consider external item interfaces to be equivalent to a lower integrity portion of the item.
   EXAMPLE: the interface between a safety related item function and an external Bluetooth device might consider the Bluetooth channel to be a lower integrity portion of the item. If an argument is made that the Bluetooth channel is in fact of high integrity, then argument must be extended along that channel until a lower integrity boundary is eventually reached as if that extended path were a part of the item.
4) External sensors are considered to be an interface to a lower integrity real world.

b) V2X safety
   1) Degree to which vehicle safety depends upon V2X communications
   2) V2X data timeliness, integrity, accuracy, availability
c) GNSS safety
   1) Degree to which vehicle safety depends upon GNSS position data, time, or other factors
   2) Hazards cause by potential GNSS spoofing, degradation, and outages

11.2.4.3 HIGHLY RECOMMENDED:

a) Timing, network loading, and other non-data-value faults caused by non-safety related components and external interfaces
b) Malicious attacks on internal and external data connections to the degree mandated by the security plan

11.2.4.4 RECOMMENDED – N/A

11.2.4.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence and design documents.

11.2.5 Risks related to the use of remote operator data connectivity shall be mitigated.

11.2.5.1 MANDATORY – N/A

11.2.5.2 REQUIRED:

a) Identification of role of remote operator, including at least which of the following roles is supported by the item:
   1) Continuous teleoperation (i.e., remote control)
   2) Remote takeover in response to automatic alerts
   3) Remote continuous supervision when in autonomous mode
   4) Remote supervision in response to automatic alerts
   5) Remote takeover in response to continuous supervision
   6) Teleoperation (remote control) in response to planned ODD departure
   7) Teleoperation (remote control) in response to unplanned ODD departure

8) Teleoperation (remote control) in response to autonomy failure
9) Command interfaces for vehicle repositioning

EXAMPLES: maintenance operations, transport load/unload features, and operations using a manual controller to reposition a vehicle under human control

b) Authentication of remote operator/supervisor authority to interact with the item
c) Loss of connectivity, including correlated and coincident faults, for potentially extended lengths of time.
d) Unavailability of connection for on-demand connectivity during a mission if safety related
e) Integrity of remote-control interfaces provided to infrastructure
EXAMPLE: Externally imposed speed limit enforcement
f) Integrity of remote-control interfaces provided to law enforcement
EXAMPLE: Destination change, “kill switch”
g) **Pitfall:** Arguing that connectivity will not be lost due to diverse connections is prone to neglecting infrastructural single fault vulnerabilities
EXAMPLES: Shared cell towers, shared cell tower machine rooms, shared cell tower power supplies, shared backhaul data facilities, shared backhaul conduits, unlicensed radio transmitters, geographic obstacles such as tunnels. Generally any argument that correlated radio frequency link loss to all control links will not occur should be extremely thorough in considering common cause failures.

11.2.5.3 HIGHLY RECOMMENDED:

a) Degraded data rates, congestion, or other inability to meet bandwidth or latency requirements
b) Integrity of remote operation/supervision software and infrastructure
c) Malicious attacks in accordance with security plan
EXAMPLES: Spoofing, relay attacks, denial of service

11.2.5.4 RECOMMENDED – N/A

11.2.5.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, demonstration.

11.2.5.6.1 NOTE: The human factors involved with remote operations and supervision if used (e.g., whether a remote operator can effectively ensure safety) are critical to safety, but are beyond the scope of this standard.

11.3 Data storage

11.3.1 Safety related data storage shall be identified.

11.3.1.1 MANDATORY:

a) Identify data storage devices and safety related data functions

11.3.1.2 REQUIRED:

a) Consider types and locations of data
    1) Fixed storage devices in item
       EXAMPLES: Hard disks, solid state storage, etc.
    2) Removable storage devices
       EXAMPLES: SD cards, flash drives, etc.
    3) Remote storage devices
       EXAMPLE: Cloud storage, network attached storage devices
    4) Engineering data storage locations and archives
b) Safety related data for:
    1) Program instructions (including boot loaders, drivers, and application code)
    2) Nonvolatile data
    3) Volatile data
    4) Configuration and calibration data for software images
    5) Machine learning related data and configuration information
    6) Vehicle equipment configuration and status data
    7) Vehicle field engineering feedback data
    8) Engineering design data repositories
    9) Data logs of faults, failures, incidents, mishaps
    10) Software image update data
       EXAMPLES: Post-production updates, factory configuration reset data
    11) Crash-survivable event recorders

11.3.1.3 HIGHLY RECOMMENDED:

a) Other data logs
b) Other locations associated with data relevant to data storage risk mitigation (Section 11.3.2.)

11.3.1.4 RECOMMENDED – N/A

11.3.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence and design documents.

11.3.1.6.1 NOTE: In many cases one physical data storage device will have multiple data functional aspects, such as a flash memory that stores both program instructions and configuration data. All safety related aspects of storage data integrity are relevant, but arguments can be consolidated within reason.

11.3.2 Risks related to data storage and data handling shall be mitigated.

11.3.2.1 MANDATORY:

a) Risk related to identified data storage locations
b) Data handling related to identified data storage locations

11.3.2.2 REQUIRED:

a) Data used for engineering design activities

b) Training data and other collected data used in design process
c) Design validation data
EXAMPLES: Test sets, vehicle performance data
d) Data used for manufacturing and field service activities, including at least the following:
    1) Item software image integrity
    2) Item software update integrity and freshness
    3) Maintenance data completeness, integrity, and freshness (procedures, requirements, vehicle status)
e) Manufacturing and production data storage
    1) Engineering data repository
    2) Manufacturing data repository
    3) Configuration management data repository
f) Update data storage
    1) Data storage and transportation between manufacturer and vehicle
    2) Intermediate data storage if used
    EXAMPLES: Local dealership server, service tool storage
g) Operational data
    1) Map data
        i) Accuracy
        ii) Features identified
        iii) Expiration date/time
    2) Weather data and other environmental data
    3) Mission-related data
    EXAMPLE: Map routing
    4) Remotely stored vehicle data
    EXAMPLES: Configuration data, operational history, maintenance history
    5) Vehicle status data
h) Post-crash and incident-related recorded data
i) Data dependability and freshness
    1) Cloud data
    2) Infrastructure data
    3) V2X data
    4) Map data
    5) Navigation
    6) Vehicle pose
    7) ODD change and violation
    8) Weather prediction and other environmental factors

11.3.2.3 HIGHLY RECOMMENDED:

a) Authenticity of data identified responsive to this clause
b) Integrity and authenticity of data used for field engineering feedback
    1) Technical validity and provenance of data
    2) Supports acceptably unambiguous root cause analysis

11.3.2.4 RECOMMENDED:

a) Forensic validity of data used for incident and mishap analysis
    1) Chain of custody
    2) Tamper evidence
    3) Unmitigated fault sources that can compromise data
    4) Suitability for insurance claim handling and risk assessment

REFERENCE: see DO-200B & DO-201 for non-normative guidance

11.3.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence and design documents.

11.3.2.6.1 NOTE: In some cases the effects of this Section will need to reach well into an IT infrastructure data safety case for the engineering and lifecycle support functions, while this standard is concerned primarily with the safety of the autonomous product. Nonetheless, IT system-resident data potentially plays a significant role in item safety. Acceptable risk mitigation is argued from the point of view of mitigation to the risk that an individual item's safety has been compromised by an issue with IT system-resident data. Design tradeoffs to simplify safety argument might include, for example, choosing to store some data inside the vehicle to reduce the criticality requirements placed upon external storage.

11.4 Infrastructure support

11.4.1 Infrastructure assumptions, dependencies, and hazards scope shall be identified.

11.4.1.1 MANDATORY:

a) Identify infrastructure assumptions and dependencies with regard to ODD scope
   NOTE: This results in considering the degree to which items listed for this clause are within ODD, outside ODD, inside ODD only under some limited conditions, or required to be present for the item to be inside its ODD.
b) Travel surface design constraints
   EXAMPLES: Assumed limitations on slope, curvature, friction coefficient, coloration, including roadways, curbs, and relevant aspects of sidewalks;
   Road smoothness, including potholes, pavement heaves, pavement changes
   Limitations on speed bumps or other traffic calming mechanisms
   Landing surfaces for aircraft
c) Infrastructure assumptions and dependencies
   EXAMPLE: Assumption that reflective road striping is used rather than paint, assumption of GNSS accuracy, required location accuracy of markers
d) Traceability to hazards and functions/components within item that directly and indirectly depend upon that data
   EXAMPLE: Road surface markings are used for detailed positioning information directly by localization module and indirectly by planning module.

11.4.1.2 REQUIRED:

a) Navigational infrastructure
   EXAMPLES: GNSS, differential GPS signals, officially designated navigational aids (e.g., markers, street signs, fiducial markers), street signs, landmarks
b) Signage and other safety related informational devices
   EXAMPLES: Traffic regulation signage, informational signage such as highway exit information
c) Augmentations to human-compatible infrastructure
   EXAMPLE: Machine-readable 2-d bar codes superimposed on signs
d) Infrastructure markings
   EXAMPLES: Boundary markings, travel lane markings, magnetic markers, paint, crosswalk stripes, other surface and environmental marking materials, colors, and textures
e) Mitigation for dangerous road conditions
   EXAMPLES: Marking of open construction pits, metal plate coverings for idle construction zones
f) Special roadway situations
   EXAMPLES: Markings for non-signalized one-lane two-way bridge, markings for low clearance underpasses including garage clearance
g) Emitters
   EXAMPLES: Lights, radio beacons
h) Passive markers
   EXAMPLES: Corner reflectors, optical travel boundary markers, painted identification information (e.g., numbers painted on travel surface), dock numbers
i) Found item infrastructure characteristics used but not necessarily under control of any infrastructure
   EXAMPLES: Navigational use of house numbers, commercial signage, fences, landscaping features
j) Manual operated signals, including hand signals
   1) Construction zones
   2) Police activity
   3) First responder activity
   4) School crossing
   5) Ad hoc traffic control
      EXAMPLE: Civilian assisted truck maneuvering, good Samaritan traffic management at crash scenes
k) Special vehicle signaling
   1) School buses
   2) Yield to emergency vehicle
   3) Comply with police pull-over signaling
   4) Railroad grade crossing (signalized and non-signalized)

11.4.1.3 HIGHLY RECOMMENDED:

a) Other road conditions
    1) Surface coefficient of friction improvements
       EXAMPLES: As improved by road treatments, pavement milling
    2) Maximum grade, camber
    3) Fresh pavement
       EXAMPLES: Recent oil and chip application, repaving with below-normal specification temporary road markings
    4) Winter road treatment
    5) Snow plow interaction
    6) Surrounding smoke, fire, heavy fog
b) Unusual road conditions
    1) Metallic bridge components or road surfaces
       EXAMPLES: Bridge joints, steel grid bridge deck
    2) Dynamic roadway features
       EXAMPLES: Grade crossing barriers, drawbridges, moveable lane barriers
    3) Wooden roadway and bridge components
    4) Significantly uneven road surfaces
       EXAMPLE: Excessive camber on one-lane dirt road, boundary of milled road surface in repaving construction zones
    5) Passenger and cargo loading zone configuration
    6) Other infrastructure requirements

11.4.1.4 RECOMMENDED:

a) Other relevant aspects of infrastructure such as:
    1) Parking lots and garages
    2) Charging stations/refueling stations
    3) Off-road and ad hoc parking areas
       EXAMPLE: parking in hay field during a holiday festival

11.4.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

11.4.1.6.1 NOTE: Infrastructure properties might be relied upon for safe operation of the item in terms of either providing support infrastructure or enabling assumptions about what types of conditions can be assumed within a particular ODD. Therefore, an infrastructure hazard is often not the existence of an identified aspect, but rather the deviation of an identified aspect from expectations and assumptions made by the item and its design.

11.4.2 Identified infrastructure hazards related risks shall be mitigated

11.4.2.1 MANDATORY:

a) Identify infrastructure related hazards in accordance with identified infrastructure fault model (See Section 6.11)

b) For each identified contribution to risk or hazard, identify risk mitigation strategy
NOTE: Risk mitigation strategy might be “accept” for low risk items
c) For each risk mitigation strategy, argue acceptable risk mitigation has been achieved

11.4.2.2 REQUIRED:

a) Include mitigation of risks due to infrastructure not meeting assumptions and/or requirements.

11.4.2.3 HIGHLY RECOMMENDED – N/A

11.4.2.4 RECOMMENDED – N/A

11.4.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, and demonstration.

12 Verification, Validation, and Test

12.1 Verification, Validation (V&V), and test approaches

12.1.1 V&V approaches shall provide acceptable evidence of acceptable item risk.

12.1.1.1 MANDATORY:

a) Identify V&V methods and extent used (See Section 12.2)
b) V&V Coverage (See Section 12.3)
c) Testing (See Section 12.4)
d) Run-Time Monitoring (See Section 12.5)
e) Safety Case Updates (See Section 12.6)

12.1.1.2 REQUIRED – N/A

12.1.1.3 HIGHLY RECOMMENDED – N/A

12.1.1.4 RECOMMENDED – N/A

12.1.1.5 CONFORMANCE:
Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

12.1.1.6.1 NOTE: Testing is a type of V&V, but is explicitly named because of its prominence in V&V activities for these items.
12.1.1.6.1 NOTE: Traditionally, V&V provides acceptable evidence of requirements compliance. To the extent that traceability that provides a causal link between requirements, implementation, and test results is present (e.g., using a V model), requirements compliance may be an acceptable argument. (This assumes that requirements are also argued to provide acceptable item risk.) However, for arguments that do not rely upon forward design process traceability (e.g., perception systems based upon machine learning that use statistical arguments based primarily on testing data), V&V approaches may need to directly address risk acceptability.

12.2 V&V methods

12.2.1 The safety case shall identify specific V&V methods used.

12.2.1.1 MANDATORY:

a) Identification of V&V approaches used, including for each approach at least:
    1) Each type of V&V approach
    EXAMPLES: Peer reviews, static analysis, unit test, simulation, item test, formal proof, inspection, analysis by reviewer
    2) Description of how activity is carried out and what work products it produces

3) Identify coverage metric(s)
   EXAMPLES: Peer reviews on new code and code modifications, unit test of modified code
4) Traceability strategy
   NOTE: This item requires identifying how the V&V activity relates to other design activities and, when appropriate, performance of the end item. This is not a requirement that each V&V technique must be highly realistic in terms of deployed item operations, but rather a requirement to state what property or condition is being contributed to the overall V&V activity. In some cases the relationship to final item operation might be indirect, such as ensuring that an implementation meets its design objectives.

b) Physical item testing
   EXAMPLES: Closed course testing, HIL testing, public road testing
   NOTE: Physical testing can serve at least two roles. One is validation of the item. Another is collection of additional data that may contain unexpected operational environmental data. These are two separate purposes and in some cases argument can be improved by addressing those two purposes separately. A specific intent is that everything including any software, data, configuration, calibration, or hardware update will not be deployed to items without some form of confirmatory physical testing at the item level.
   NOTE: Public road testing presents unique risks in terms of exposure of non-participants to the effects of potential item malfunction. Acceptable testing safety approaches are essential, but beyond the scope of this standard.
c) Argue that identified V&V methods provide acceptable V&V coverage.

12.2.1.2 REQUIRED:

a) Peer reviews
b) Static analysis
   1) Identify static analysis techniques
      NOTE: This can be in the form of identifying tools and tool capabilities.
   2) Justify static analysis rigor
      NOTE: This includes justifying that tools selected and tool configurations used are acceptable
      EXAMPLE: Adding the flag “-Wall” to a Gnu C compiler provides comparatively weak static analysis despite the flag name, because it does not enable a large number of often relevant static analysis capabilities (e.g., potentially those included in “-Wextra” and other configuration flags).
c) Software unit test
   1) **Pitfall:** Unit testing of excessively large software units is prone to missing defects due to limitations on controllability and observability.
d) Robustness and/or stress testing
e) Software Qualification Test
   EXAMPLE: Software requirements verified as in IEEE 12207

f) Item Qualification Test
EXAMPLE: Item requirements verified as in IEEE 12207
g) Failure Modes and Effects Testing
h) Functional and component testing with environmental condition variation consistent with industry best practices for ODD
EXAMPLES: EMI, Shake & Bake, temperature cycling, accelerated life testing
i) Pre-release regression tests for any updates
j) Per vehicle commissioning tests
k) Closed course item testing
EXAMPLES: Dedicated test facility, controlled access use of public spaces
l) Log analysis of deployment data to supplement before-release V&V

12.2.1.3 HIGHLY RECOMMENDED:

a) Automated test frameworks
b) Continuous integration
c) Dynamic analyses
d) Integration testing
e) Formal methods
f) Other analytic methods
g) Software-In-the-Loop (SIL) testing
    1) With recorded environmental workloads
    2) With simulated environmental workloads
    3) With live environmental workloads
h) Hardware-In-the-Loop (HIL) testing
    1) With recorded environmental workloads
    2) With simulated environmental workloads
    3) With live environmental workloads
i) Stress testing
j) Item testing
    1) With recorded environmental workloads
    2) With simulated environmental workloads
    3) With live environmental workloads
    EXAMPLE: Closed course testing
k) Public road testing with continual human safety supervision
NOTE: Assuring acceptably safe human supervision crucial but yet potentially difficult, and raises potential ethical concerns regarding exposure of the general public to test items. Addressing issues of effective human supervision is beyond the scope of this standard.
l) Public road testing with less than continual human safety supervision
NOTE: Assuring acceptably safe human supervision crucial but yet potentially difficult, and raises potential ethical concerns regarding exposure of the general public to test items. Accomplishing this is beyond the scope of this standard.
m) Pilot public road deployments

n) Run-time monitoring of any form of testing or deployment (specify which)
o) Diagnosis testing to replicate field issue reports
p) Site testing with any adaptation data
q) Field vehicle in-service tests
   EXAMPLE: Annual inspection capability and performance test
r) Any other types of testing performed
s) **Pitfall:** Use of manual breakpoint debugging for unit test is prone to inconsistent test results and limited scope of testing.
   NOTE: Breakpoint debugging typically involves using a debugger to manually set up variable values, observe flows of control, and observe computational results of a unit within a fully compiled item image. In practice it is difficult to ensure repeatable results, and testing scope is limited due to the time and expense of non-automated regression testing inherent in a manual approach.

12.2.1.4 RECOMMENDED – N/A

12.2.1.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

12.2.1.6.1 NOTE: Finer grain categorization of types of tests is encouraged so long as all categories in the required list are covered (document coverage with traceability analysis if any required category is not explicitly included).

12.2.1.6.2 NOTE: As a practical matter many of the recommended types of testing will need to be employed to create a satisfactory safety case. Their inclusion as recommended rather than required is to provide flexibility in the overall testing approach. In particular, it is generally appropriate to use a wide variety of V&V techniques for life critical aspects of the item.

See Also Section 12.4.6.

12.2.2 The safety case shall document the contribution of evidence provided by each V&V method.

12.2.2.1 MANDATORY:

a) Consider effects of potentially nondeterministic component and item behavior on V&V results. (If none, so state.)
   EXAMPLE: Statistical significance (or other approach) using multiple approaches to ensure that nondeterministic item behavior has been characterized by a testing process.

12.2.2.2 REQUIRED:

a) For each V&V method documented in support of Section 12.1, results tied to specific argument in the safety case.
b) Effects of statistical nature of test data and operational environment on V&V results.

12.2.2.3 HIGHLY RECOMMENDED – N/A

12.2.2.4 RECOMMENDED – N/A

12.2.2.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

12.3 V&V coverage

12.3.1 V&V shall provide acceptable coverage of safety related faults associated with the design phase.

12.3.1.1 MANDATORY:

a) Systematic design defects
b) Design consideration of faults, corruption, data loss, and integrity loss in sensor data
c) Requirement gaps/omissions and requirement defects
d) Response to violation of requirement assumptions
   EXAMPLE: Response to exceptional operational environment
e) Identification and description of the intended ODD
f) Acceptable mitigation of aspects of the defined fault model for each component and other aspect of the item

12.3.1.2 REQUIRED:

a) Maintenance procedure definitions
   NOTE: While maintenance occurs during the lifecycle, the definition of procedures needs to correspond to design requirements and assumptions made in design regarding maintenance
b) Operational procedure definitions (including startup and shutdown) and operational modes
c) Faults, corruption, data loss, and integrity loss in data from external sources
d) Faults and failures associated with exceptional conditions that impair risk reduction functionality
e) Hardware and software errata and other third-party component design defects
f) Other faults in safety related functions, component designs, and other designed properties

12.3.1.3 HIGHLY RECOMMENDED – N/A

12.3.1.4 RECOMMENDED – N/A

12.3.1.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence.

12.3.1.6.1 This clause is intended to encompass the correctness and completeness of requirement, design, implementation, and mitigation of design cycle related faults which can affect safety related functionality.

12.3.2 V&V shall provide acceptable coverage of safety related faults associated with the construction of each item instance.

12.3.2.1 MANDATORY:

a) Conformance of item instance to design
b) Capability to execute safety related functionality
c) Effectiveness of risk mitigation functionality and approaches
d) Configuration data faults
   EXAMPLES: Incorrect calibration data, corrupted calibration data, missing calibration data
e) Faults and failures in components integrated into the item
f) Faults and failures that compromise the integrity of programmable components

12.3.2.2 REQUIRED:

a) Incorrect or incompatible versioning of components, data, manufacturing procedures
b) Supply chain deviations from component requirements
   EXAMPLES: Quality fade, incompatible components, counterfeit components, excessively aged components

12.3.2.3 HIGHLY RECOMMENDED – N/A

12.3.2.4 RECOMMENDED – N/A

12.3.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

12.3.3 V&V shall provide acceptable coverage of safety related faults associated with the item lifecycle.

12.3.3.1 MANDATORY:

a) Impairment of safety related functionality
b) Faults and failures that are capable of affecting safety related aspects of the intended operation of the item
c) Coverage of specified fault models during item operational lifetime (see Section 6.2)

12.3.3.2 REQUIRED:

a) Accuracy of reliability and end-of-life estimates used for maintenance scheduling
b) Faults and failures during:
   1) Manufacturing-associated operation
   2) Transport
   3) Storage
   4) Sales and business-related operations
   5) Corrective maintenance
   6) Mid-life upgrades
   7) Crash and other damage repair

12.3.3.3 HIGHLY RECOMMENDED – N/A

12.3.3.4 RECOMMENDED – N/A

12.3.3.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.3.4 V&V shall provide acceptable coverage of the ODD.

12.3.4.1 MANDATORY:

a) Coverage of identified ODD (see Sections 8.2.1 and 8.2.2)
b) Coverage of ODD violations (see Section 8.2.3)
c) Arguments that coverage is acceptable

12.3.4.2 REQUIRED:

a) Coverage of defined ODD subsets, if used.

12.3.4.3 HIGHLY RECOMMENDED – N/A

12.3.4.4 RECOMMENDED – N/A

12.3.4.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.3.5 V&V shall provide acceptable coverage of the item structure and intended operations.

12.3.5.1 MANDATORY:

a) Coverage of safety related item hardware components
b) Coverage of safety related item software components
c) Coverage of safety related system interfaces
   EXAMPLES: Sensors, actuators, human/computer interfaces, electronic communication interfaces
d) Coverage of safety related item functions

12.3.5.2 REQUIRED:

a) Coverage of safety related extra-functional properties, including:
    1) Real time performance
    2) Software stability
    3) Performance margin
    4) Dependability

12.3.5.3 HIGHLY RECOMMENDED – N/A

12.3.5.4 RECOMMENDED – N/A

12.3.5.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4 Testing

12.4.1 Testing shall be conducted with acceptable rigor and coverage.

12.4.1.1 MANDATORY:

a) Test Plans (See Section 12.4.2)
b) Testing oracles (See section 12.4.3)
c) Testing coverage (See section 12.4.4)
d) Traceability of test results to safety argument (See Section 12.4.5)
e) Regression testing (See Section 12.4.6)
f) Fault injection testing (See Section 12.4.7)

12.4.1.2 REQUIRED – N/A

12.4.1.3 HIGHLY RECOMMENDED:

a) Defined test strategy
   NOTE: The test strategy describes overall philosophy, approach and overarching aspects (e.g., definition of test rigs). This is supplemented by test plans, which describe the steps and expected results associated with each individual test case. Collecting repetitive and general information in a test strategy document can promote uniformity and reduce repetitive documentation.

12.4.1.4 RECOMMENDED – N/A

12.4.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

12.4.1.6.1 NOTE: Testing is one form of verification and validation. To the degree that testing does not cover the entire fault model for each aspect of the item, other aspects of V&V are used to complete V&V coverage.

12.4.2 Test plans shall be documented and followed for test data relied upon as evidence.

12.4.2.1 MANDATORY:

a) Methodical approach to capturing hardware, software, and other configuration information for components of the item under test
b) Acceptable test plan documentation:
   1) Description of each test procedure
   2) Description of test setup, test environment and test instrumentation
   3) Independent derivation of expected test results (See Section 12.4.3)
   4) Description of pass/fail criteria
   5) Documentation of as-performed test runs, including any deviations from test plan with justification
   6) Traceability of each safety related test to argument of test efficacy

7) Traceability of each safety related test to associated requirement(s) or risk mitigation approach
8) Consideration of nondeterministic aspects of item behavior

c) Coverage of safety related aspects of item
   1) Argument of test plan sufficiency
   2) Safe operation of normal functionality
   3) Safe transition through startup, sequences of operational conditions, shutdown, and other transient functionality
   4) Component and subsystem fault and failure responses
   5) Coverage of ODD, including at least:
      i) Operational environments
      ii) Objects and events
      iii) Maneuvers
      iv) Item level fault and failure responses
d) Consideration of brittleness of software-based functionality
   1) Stress test response to exceptional conditions
   2) Randomized or otherwise varied operational parameters and scenarios
   3) Evaluation of autonomy brittleness
e) Factors that can compromise test validity and/or representativeness, including:
   1) Environmental conditions
   2) Equipment condition
   3) Sensitivity of item to small changes in initial conditions

12.4.2.2 REQUIRED:

a) Peer review of test plans
b) **Pitfall:** Tests with ambiguous or ad-hoc success criteria are prone to failing to detect defects
   NOTE: A contributing factor is confirmation bias when testers look for reasons to declare that a test has passed.
c) **Pitfall:** Test execution with multiple varied or undocumented item configurations or parameters is prone to invalidating test validity and test reproducibility
   NOTE: Tests run without acceptable documentation of item version under test and whether test conditions adhere to the test plan do not provide sufficient evidence to meet testing requirements.
d) Consideration for ensuring testing repeatability
   EXAMPLES: Initial item conditions, timing, test apparatus calibration
e) Description of monitoring methods and procedures to identify source(s) of unexpected test results
f) Evaluation of test results and root-cause analysis of anomalous results
   1) Errors originating in test monitoring tools
   2) Errors in test conduct
   3) Test oracle defects
   4) Test setup errors

5) Test procedure defects
6) Incorrect observation and recording of test results
7) Faulty derivation of expected test results

g) **Pitfall:** Software defect correction during a test campaign is prone to invalidating prior test results from that campaign
NOTE: This means that already-passed tests are re-run after a bug fix performed partway through a test campaign, potentially subject to limitation as a result of change impact analysis.
h) **Pitfall:** A single test of a nondeterministic function is prone to passing due to chance rather than as a confirmation of correctness.

12.4.2.3 HIGHLY RECOMMENDED – N/A

12.4.2.4 RECOMMENDED – N/A

12.4.2.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4.2.6.1 NOTE: Tests that are not relied upon as evidence (e.g., efficiency or ride comfort tests) do not need traceability to arguments, but by the same token are disregarded in evaluation of the safety case.

12.4.3 The test oracle for each test shall be documented.

12.4.3.1 MANDATORY:

a) Test setup, procedure, and sequence of test cases acceptable for the test oracle
b) Description of pass/fail criteria
c) Method of defining pass/fail criteria
NOTE: Description related to creation of automated oracle results and/or manually generated expected test results

12.4.3.2 REQUIRED:

a) Argue oracle correctness, if an automated oracle is used
b) Test oracle defined before test is conducted
c) **Pitfall:** Defining test pass criteria after testing is prone to rationalizing incorrect results as test passes instead of testing failures.
d) **Pitfall:** Using previous execution results of the software under test as an oracle is prone to creating incorrect test pass/fail criteria that accept the results of any software defects as valid.
NOTE: Using previous execution results might be acceptable practice for regression testing if other functionality tests have been defined that also encompass the defect correction that is the subject of the regression test.
e) Tools that automatically generate tests including pass/fail criteria based on the code itself are prone to missing functional defects in that code.
EXAMPLE: A tool that automatically generates unit tests to cover all code branches exercises the code, but has no way of determining if the code functions as intended

unless paired with some sort of machine-interpretable design and/or specification information.

12.4.3.3 HIGHLY RECOMMENDED – N/A

12.4.3.4 RECOMMENDED – N/A

12.4.3.5 CONFORMANCE:
Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4.3.6.1 NOTE: A primary purpose of a safety related testing is to provide evidentiary support for safety arguments. The test oracle is created with this in mind. As an example, a conventional software robustness test might have an oracle of “doesn’t crash” rather than detailed data value results for each test executed if the purpose is to generate evidence that software crashes are unlikely to occur. Other informal testing can be performed, but testing that is not performed with an oracle having acceptable criticality is insufficiently supportive of safety argument. In particular, an oracle defect that causes false negative test results of safety critical functionality can create a life critical defect in the safety case.

12.4.4 Each set of safety related testing evidence shall have a defined coverage metric that supports the argument.

12.4.4.1 MANDATORY:

a) Test coverage including:
    1) Planned coverage
    2) Achieved coverage
    3) Coverage of nominal conditions
    4) Coverage of off-nominal conditions
    5) Coverage stated with respect to identified fault models

12.4.4.2 REQUIRED:

a) Use of at least one of the following coverage metrics for each set of test evidence:
    1) Software White box metrics
       EXAMPLES: Code coverage, branch coverage, MCDC coverage
    2) Hardware white box metrics
       EXAMPLES: Exercising each significant function on each hardware component, exercising each IP block on each chip, exercising each interface signal, exercising each gate in an integrated circuit, exercising each bit of a data storage device
    3) Black box metrics
       EXAMPLES: Requirements coverage, traceability to design
    4) Metrics related to the machine learning model in use and its data
    5) Metrics related to the way test inputs cover the ODD
b) Quantified confidence in coverage for nondeterministic functionality
   EXAMPLE: Statistical analysis techniques

c) **Pitfall:** Repeated testing with a fixed set of tests is prone to eliminating only the specific defects that the test plan is designed to find, and does not mean that the resultant software is defect free.
REFERENCE: The Pesticide Paradox [Beizer90]

12.4.4.3 HIGHLY RECOMMENDED:

a) Internal software state information to support validity of nondeterministic test results
EXAMPLE: Test passed because internal self-report of module behavior matches intended test scenario

12.4.4.4 RECOMMENDED – N/A

12.4.4.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4.5 Safety related testing shall trace to safety argument.

12.4.5.1 MANDATORY:

a) Test oracles, setup, and procedures trace to safety argument.
b) Traceability of pass/fail criteria to the evidentiary requirements of the test in the safety argument

12.4.5.2 REQUIRED:

a) **Pitfall:** Arguments based on having performed a large amount of undifferentiated testing without alignment to arguments is, on its own, prone to resulting in insufficient testing evidence.

12.4.5.3 HIGHLY RECOMMENDED:

a) Testing evidence traces to specific argument elements
NOTE: Tests that provide evidence supporting argument of acceptable software quality, functionality, or dependability are designed to specifically address aspects of the fault model.

12.4.5.4 RECOMMENDED – N/A

12.4.5.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.
12.4.5.6.1 NOTE: Tests that do not trace to safety argument can be performed. However, no safety credit can be taken for tests that do not trace to safety argument.

12.4.6 Regression tests and validation testing shall be used to validate item changes.

12.4.6.1 MANDATORY:

a) Regression testing conducted after any change to item
b) Regression testing conducted after any change to regression tests

12.4.6.2 REQUIRED:

a) Each corrected safety related defect traces to at least one test to validate correction in a regression test suite
   NOTE: This is intended to result in a regression test suite over time exists that accumulates tests for all defect corrections to safety related item components.
b) Any change to a safety related fault-containment region results in full testing for safety functions within all affected fault-containment regions
   NOTE: This is likely to result in a full-coverage test plan and testing activity for the entirety of functionality resident in each safety related FCR, including non-safety related functionality that happens to be resident in that FCR. That whole-FCR test plan is executed in response to each change within the relevant FCR, even if the change is not itself safety related.
c) Defect corrections covered by the regression test suite include any defects found in V&V, pilot deployments, and at-scale operation
d) Non-code contributors to defects used as inputs to continuous process improvement activities
   EXAMPLES: Peer review checklist omissive mistakes, test plan omissive mistakes

12.4.6.3 HIGHLY RECOMMENDED:

a) Regression testing informed by impact analysis.
b) Execution of all regression tests regardless of impact analysis.
   EXAMPLE: All regression tests run periodically regardless of impact analysis results for changes, but only run responsive to impact analysis for minor changes between full runs.
c) Regression tests for non-safety related functionality that interfaces to safety related functionality.

12.4.6.4 RECOMMENDED – N/A

12.4.6.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4.6.6.1 NOTE: Non-code contributors to defects do not necessarily result in additional regression tests, but can result in process changes to ensure that process defects do not recur. **EXAMPLE:** A defect caused by a missed requirement has corrective action taken to reduce the probability of other requirement gaps of a similar type. That might result in a change to requirement review checklists and a re-review of at-risk requirements. There might be no point in re-running regression tests if no changes to code and no changes to test plans are made as a result.

12.4.7 Fault injection testing shall be used to provide evidence of acceptable fault mitigation.

12.4.7.1 MANDATORY:

a) Fault injection testing to a justified level of coverage

12.4.7.2 REQUIRED:

a) Cover all aspects of identified fault models (see Section 6.2)
    1) Fault injection where practical
    2) Justification that other aspects of fault models are covered by other techniques
b) For each instance in which fault injection testing is deemed impracticable for an aspect of a fault model:
    1) Justify why fault injection testing is impracticable
    2) Arguments and evidence validating that the relevant aspect of the fault model has been mitigated

    NOTE: All aspects of all faults within identified fault models are covered. Preference is given to actual fault injection testing rather than analysis. Validation is specifically required, indicating that the question at hand is not “is fault mitigation supposed to work,” but rather “does the fault mitigation actually work.”

12.4.7.3 HIGHLY RECOMMENDED:

a) Evaluation and minimization of intrusiveness of fault injection approaches
b) Fault injection with pairs of moderate to high probability faults
c) Fault injection performed in simulation
d) Fault injection testing conducted at unit level
e) Fault injection testing conducted at subsystem level
f) Fault injection testing conducted at vehicle level

12.4.7.4 RECOMMENDED – N/A

12.4.7.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.4.7.6.1 NOTE: Different approaches to injecting faults are likely to be more efficient and effective depending upon the type of fault and its effect on the system. Coverage can be attained via a combination of fault injection strategies, and need not include duplicating specific faults via different fault injection approaches.

12.4.7.6.2 NOTE: Injection of some faults in an operational product can lead to potentially dangerous malfunctions if the fault response is incorrect. This is not a sufficient excuse for neglecting confirmation of safe fault response necessary to avoid loss events during deployment, but does motivate initial confirmation of fault response effectiveness via simulation and actual testing under controlled conditions.

12.5 Run-time monitoring

12.5.1 Run-time monitoring shall be used to detect safety related operational faults and design assumption violations.

12.5.1.1 MANDATORY:

a) Identification of run-time monitoring strategy and capabilities

12.5.1.2 REQUIRED:

a) Occurrence of and correctness of response to safety related operational faults
EXAMPLE: Hardware operational faults
b) Occurrence of and correctness of response to safety related events that could have been caused by design faults
EXAMPLES: Unexpected tripping of watchdog timer, unexpected item resets, unexpected item behaviors
c) Run-time monitoring to detect at least the following:
    1) Validity of assumptions made in the safety argument
    2) Validity of historical data-based evidence used as the basis for the safety argument
    3) Confirmation that system is being used inside the ODD during monitoring
    NOTE: Data from operation outside the ODD does not necessarily provide evidence useful for arguing safety inside the ODD
d) Logging of safety related run-time monitor and fault detections
NOTE: Logging fidelity supports acceptable field engineering feedback. For some items this might be a detailed time-stamped log, while for non-life-critical items it might be acceptable to have a list of most recently activated diagnostic trouble codes.
e) Validation of run-time monitoring capability
NOTE: The implementation of run-time monitoring is subject to software quality considerations as well as data safety considerations (See Section 11).

12.5.1.3 HIGHLY RECOMMENDED:

a) Monitoring traced to the fault model and evidentiary requirements of the safety case rather than simply based on what seems convenient to monitor in the implementation.

12.5.1.4 RECOMMENDED:

a) Run-time monitoring of the occurrence and response to faults to the maximum extent practicable, including non-safety related faults.

12.5.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

12.5.1.6.1 NOTE: Run-time monitoring of items in test and deployment can help ensure that the fault model is complete, that faults happen at expected rates, and that the item handles faults as intended.

12.5.1.6.2 NOTE: A combination of on-item monitoring to trigger reports and off-line analysis of data logs may be acceptable. The tradeoff of data bandwidth vs. on-item processing power is left at the developer's discretion.

12.5.2 The argument shall demonstrate acceptable analysis of results of run-time monitoring to identify and address hazards, design defects, and process defects according to safety argument

12.5.2.1 MANDATORY:

a) Timely data collection and analysis of run-time monitoring logs
    1) Includes logs taken during item-level testing

12.5.2.2 REQUIRED:

a) Analysis intended to identify novel hazards
b) Identification of incorrect safety case assumptions
c) Identification of incorrect analysis of occurrence rate of:
    1) Accepted risks
    2) Mitigated faults
    3) Unmitigated but detectable faults
    4) Unmitigated, undetected faults
    NOTE: This might need to be inferred via observation of incidents, anomalies, and other indirect detection methods.
d) Identification of incorrect object or event classifications
e) Identification of substantively ambiguity, uncertainty, and/or jitter in object/event classifications

12.5.2.3 HIGHLY RECOMMENDED:

a) Monitoring of item performance to detect deviations from safety related design parameter specifications, including for example:
    1) Data network bit error rates
    2) Variance from designed operational behaviors
    EXAMPLES: Distribution of closest points of approach to obstacles compared to intended buffer distance values
    3) Prediction values that differ excessively from actual outcomes
    EXAMPLE: Object behavior predictions
b) Monitoring hazard detection and mitigation performance
    EXAMPLES: Detection and reporting of ODD violation events and item response to those events

12.5.2.4 RECOMMENDED – N/A

12.5.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as demonstration.

See also: Section 16

12.5.3 Any safety related unexpected item behavior detected by observation, run-time monitoring, or any other means shall be considered an incident, even if no loss event has occurred.

12.5.3.1 MANDATORY – N/A

12.5.3.2 REQUIRED:

a) Evaluation of run time monitoring data, test data, and field observation for safety related events
    1) Disagreement between safety case constraints and requirements vs. actual item behavior
    2) Anomalous safety related behavior
b) Identification, root cause analysis, item correction or justification of no correction for each unexpected event
    NOTE: Some unexpected behaviors might result in a change of expectations to encompass and observed behaviors. These might result in changes to the safety case rather than changes to the item implementation.
c) Analysis of information gathered via sources other than run time monitoring for safety related events
d) Tracking incident to closure via updating at least one of following as acceptable in response to each unexpected event:
    1) Requirements
    2) Design
    3) Test plans
    4) Processes
    5) Other argument, evidence or other components of the safety case and/or item artifacts
    6) Item validation (i.e., re-validate item as acceptable)

12.5.3.3 HIGHLY RECOMMENDED:

a) Monitoring of cohort performance information for safety related events
    EXAMPLES: Customer complaints, warranty repair database
b) Monitoring of accident investigation reports for safety related events
    EXAMPLES: Police reports, insurance claims

12.5.3.4 RECOMMENDED – N/A

12.5.3.5 CONFORMANCE:

Conformance is checked via problem report list status and justification.

12.6 Safety case updates

12.6.1 A safety case analysis shall be triggered in response to changes.

12.6.1.1 MANDATORY – N/A

12.6.1.2 REQUIRED:

a) Change to the build package and/or item image
EXAMPLES: Source code change, use of a retrained neural network, configuration and/or calibration data change, changes to libraries, security patches

b) Change to processes and/or tools that affect the item build image directly or indirectly
EXAMPLES: New or updated versions of: compiler, operating system used to generate system image, configuration management tool, remote update management tools, neural network training tools, training data collection items, development process model, development procedural changes, test procedure changes, SQA procedure changes

c) Change to data, processes and/or tools that affect safety related data sources
EXAMPLES: Change of software used to process map data provided to item, change of map data vendor, acquisition by map vendor of third party data incorporated into map database, change of map data provider infrastructure, update to data collection item hardware and/or software, update to training data, update to weather data collection infrastructure, update to remote operation or supervision infrastructure

d) Change to processes and/or tools related to safety analysis and feedback
EXAMPLES: Update to defect tracking tool, update to simulators, update to HIL/SIL tools, update to test procedures, update to test plans, update to analysis tools used to evaluate operational anomalies, update to safety case analysis and maintenance tools, change to different tools.

e) Change of item configuration
    1) Changes of fault containment region boundaries
    2) Reallocation of software to different hardware resources
    3) Addition or deletion of a sensor in the as-built item configuration
    NOTE: Assumes installed sensors are fully operational and is not intended to cover degraded configurations, which are covered elsewhere
    4) Mounting/location change of installed sensors
    5) Component version change, including hardware components, sensors, and actuators
    6) Component substitution
    7) Component supply chain change

f) Change to the intended operational environment
    1) Deployment to new ODD
    2) Modification of ODD
    3) Discovery of novel objects, events, or fault situations that require handling by the item within established ODD

g) The occurrence of any safety-related incident regardless of whether the item has been changed in response or not
    1) Incidents
    2) Loss events
    3) Violation of a monitored safety related threshold and/or assumption
    EXAMPLE: Occurrence of more than expected number of network packet failures, elevated rate of misclassification of a safety related object by a particular type of sensor, violations of safety case assumptions
h) Change that results in a previously non-safety related aspect of the item becoming safety related.

12.6.1.3 HIGHLY RECOMMENDED:

a) Automating identification of safety case analysis triggers when feasible
EXAMPLE: Tracking field failure rates for exceeding predetermined thresholds

12.6.1.4 RECOMMENDED – N/A

12.6.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence as well as subsection conformance.

12.6.1.6.1 NOTE: Changes of parameters and other values that have been pre-enumerated in a build image are not intended to serve as triggers. As an example, a passenger selector of vehicle dynamics that permits “comfort” vs. “sport” handling mode does not trigger safety case analysis when it is changed so long as validation has already considered the possibility of using the associated different algorithms and different machine learning data sets being involved in those different settings in the validated build image.

12.6.1.6.2 NOTE: Changes to documents which are not technically substantive (e.g., non-substantive typographical error corrections) still trigger a safety case analysis, if for no other reason than to determine that the change is in fact not technically substantive. Impact analysis procedures can provide ways to limit the effort required to screen for non-substantive changes.

12.6.2 Impact analysis shall be used to determine the scope of the effect of changes upon the safety case.

12.6.2.1 MANDATORY – N/A

12.6.2.2 REQUIRED:

a) Determine the scope of the change’s effect on the safety case, including at least the following:
    1) Identify whether the change is safety related, even if only indirectly
    2) Identify any change to safety related functionality
    3) Scope of the change’s effect on assumptions, item limitations, and evidence supporting the safety argument
    4) Scope of the change’s effect on tools, procedures, and historical data

5) Scope of the change's effect on the validity of evidence used to support the safety case

b) **Pitfall:** Seemingly "small" changes to software and data are prone to causing potentially catastrophic item failures. The "size" and impact of a change cannot be assumed to be proportional to the number of lines of code or number of bytes of data changed

c) **Pitfall:** Changes to non-critical functions are prone to compromising safety related functions via interference, resource consumption, or other indirect coupling if they share resources or communicate

NOTE: An architectural partitioning that provides strong isolation between safety and non-safety related components can simplify change analysis. To the degree that no assumptions are made about a non-safety related component within the safety case, changes to that component might not have to be analyzed for safety impact. However, any assumption made upon the behavior or other attributes of a purported "non-safety related" change that affect safety case arguments in fact make that component indirectly safety related, and impose a change analysis requirement to ensure that any relied-upon properties hold true.

EXAMPLE: An analysis that acceptable reserve resources are available can be invalidated by a non-safety-related function that consumes too many resources on the same processor.

12.6.2.3 HIGHLY RECOMMENDED:

a) Use of qualified tools to perform impact analysis triage and decision support

b) Coupling of impact analysis to regression analysis and reverification planning to validate that impact analysis is correct and there are no unforeseen consequences from a change

c) **Pitfall:** Use of tools to perform impact analysis is prone to making that tooling safety related.

EXAMPLE: Use of a machine-learning based tool to do impact analysis potentially requires validation of that tool to a life critical level of integrity, which might not be feasible.

12.6.2.4 RECOMMENDED:

a) Automated detection and analysis of changes with no safety related impact when feasible

EXAMPLE: Detection of correction of typographical errors in documentation, addition of evidence that is not linked to safety argument

b) Automated detection and analysis of changes impact according to a set of justified screening criteria

12.6.2.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

See also: FAA Order 8110-49, although this does not address machine learning.

12.6.3 The safety case shall be updated responsive to an impact analysis.

12.6.3.1 MANDATORY – N/A

12.6.3.3 REQUIRED:

a) Update safety case to record and reflect result of impact analysis
b) If impact analysis reveals no safety related change, document that impact analysis was performed
c) If impact analysis reveals safety related change conditionally update to result in an acceptable safety case by adding, deleting, modifying, or updating:
    1) Goals and/or sub-goals
    2) Arguments
    3) Evidence
    4) Assumptions
    5) Traceability

    NOTE: Impact analysis will inform the starting point for updating the safety case. However, the entire safety case must be acceptable after the update, even if ripple effects require changes beyond the scope of the original impact analysis.
d) Re-evaluation of safety case according to scope informed by impact analysis
    NOTE: See Section 17.4.2

12.6.3.3 HIGHLY RECOMMENDED: N/A

12.6.3.4 RECOMMENDED:

a) Notification of stakeholders of safety case change
    EXAMPLE: Government safety regulator notification if appropriate

12.6.3.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

13 Tool Qualification, COTS, and Legacy Components

13.1 General

13.1.1 The item shall be acceptably free of errors caused by use of tools and tool chains, COTS components, legacy components, and associated functionality

13.1.1.1 MANDATORY:

a) Identify tools and tool chains (See Section 13.2.1)
b) Mitigate risks from tools and tool chains (See Section 13.3)

13.1.1.2 REQUIRED:

a) Mitigate risks from COTS and legacy components and functionality (See Section 13.4)
b) Mitigate risks from Item Element out of Context (SEooC) components (See Section 5.7)

13.1.1.3 HIGHLY RECOMMENDED – N/A

13.1.1.4 RECOMMENDED – N/A

13.1.1.5 CONFORMANCE – N/A

13.2 Tool identification

13.2.1 The safety case shall identify safety related tools.

13.2.1.1 MANDATORY:

a) Identify tools, support software, and other software not actually included in the item (collectively: tools) that are potentially safety related for the item software release addressed by the safety case, including at least:
    1) Tool vendor and tool name
    2) Tool version number used and date of that version’s release
    3) Description of use of tool
b) Identify tools used throughout the lifecycle:
    1) Design
    2) Simulation
    3) Data collection
    4) Data analysis
    5) Maintenance
    6) Defect reporting and management
    7) Change control
    8) Training

13.2.1.2 REQUIRED:

a) Development environment

1) Requirements tools
2) Design tools
3) Model based design and analysis tools
4) Coding tools and code generation tools, including compilers
5) Code analysis tools
6) Data management tools, including machine learning tool chains
7) Configuration and build tools, including continuous integration tools
8) Configuration management tools
9) Statistical and Mathematical models
10) Decision process tools
11) Script generation tools
12) Libraries, operating systems, file items
13) Editing tools, file items, document management tools, spreadsheets

b) Verification & Validation environment
   1) Test generators and test planning support
   2) Simulators and emulators
   3) Generation of test results including testing frameworks and regression test tools
   4) Test report generators and test result management tools
   5) Simulators
   6) Defect tracking tools
   7) Field data collection and analysis tools
   8) Statistical and mathematical models
c) Calibration tools
d) Security including:
   1) Vulnerability analysis tools
   2) Cyber defense tools
   3) Cryptographic key management tools

   NOTE: Security tool prompt elements can be delegated to a security plan.
e) Handoff environments, including at least:
   1) Interface description tools
   2) Handoff between design/development team and manufacturing team
   3) Handoff environment between suppliers and OEM
f) Manufacturing environment
   1) Safety related 3D-printing tools
   2) Safety related CAD tools
g) Tools used by suppliers
h) Tools used in software update mechanisms, bootloader, and other deployment infrastructure
i) Tools used for safety case creation and management
j) Consider at least for tools and tool chains:
   1) Correctness
   2) Reliability

3) Availability
4) Diagnosability
5) Provenance

13.2.1.3 HIGHLY RECOMMENDED:

a) Identify tool releases newer than the released being used and justify that substantive defect fixes in these releases do not compromise safety related aspects of the item.
b) Configuration tool used for item line management

13.2.1.4 RECOMMENDED – N/A

13.2.1.5 CONFORMANCE:

Conformance is checked via inspection of tool use, tool design, tool V&V evidence.

13.2.1.6.1 NOTE: The word “tool” is intended to be expansive, and includes any software or data set which could result in a safety related defect in the item. As an example, a file storage item with unacceptable error detection capability could, if a fault were not mitigated by the developer’s procedures and tool use practices, result in corrupted data being included in an item build image.

13.2.1.6.2 NOTE: The REQUIRED tool identification list is not a requirement to actually use a tool in each category listed. Rather, it is a requirement to identify which tools are listed in each category. “None” is an acceptable response for individual categories in which no tools were actually used that can introduce or fail to detect hazards and/or risks.

13.2.1.6.3 NOTE: Other standards have guidance for classification of tools, and tool qualification methods commensurate with the risk to the item so that acceptable confidence could be placed in tool usage. There are also tool qualification packages produced and provided by the tool vendors. Use of such standards and tool qualification packages is encouraged.

13.3 Tool risk mitigation

13.3.1 Safety related risks due to tools shall be identified.

13.3.1.1 MANDATORY:

a) Faults, failures, and defects potentially introduced by each tool
b) Faults, failures, and defects that fail to be detected by tools
   NOTE: Generally refers to tools for which the safety case claims credit for detection of faults, failures, or defects.
c) Unintended behavior of the item potentially caused directly or indirectly by each tool
d) Incorrect data values, missing data values, biased data values, and other data defects caused by tools, including machine learning training tools

13.3.1.2 REQUIRED:

a) Faults, failures, and defects potentially masked or unreported by each tool

b) Common mode and common cause fault analysis and avoidance in combination of tools and tool chains
c) Consideration and mitigation of known errors (tool developer's errata publications and experience in using the tool) for the exact version/revision of the tool used
d) Identification of tool developer usage and limitation instructions
EXAMPLES: Tool is only validated for a particular (somewhat old) version of an operating system that might be different than the OS version actually being used to design the item; tool has a life critical usage disclaimer but is being used in a way that could affect substantive life critical risks.
e) **Pitfall:** Infrastructure tools such as e-mail, spreadsheets, and databases are prone to being taken for granted, but might be used in safety related ways and might not be recognized in the list of tools to be considered
f) **Pitfall:** Deferring tool selection and qualification is prone to resulting in the use of unqualified tools to meet production deadlines.
NOTE: Waiting until just before item deployment to consider tool qualification is not an acceptable safety case deviation justification.
g) **Pitfall:** Taking a narrow view of the effects of tool usage is prone to missing errors introduced by one tool but masked by another tool
NOTE: A later tool change might un-mask that fault, potentially without being detected until after loss events.
h) **Pitfall:** Use of an older or newer version of the tool than the one qualified for use is prone to creating safety related incompatibilities in the design and build process.

13.3.1.3 HIGHLY RECOMMENDED:

a) Security implications of tool usage in accordance with security plan
EXAMPLE: Malware in third party tool chain intended to compromise item safety; malware in tools that enables malicious attacks on item software images (e.g., malicious updates)
b) Traceability of each component and function lifecycle phase to tools/tool chains used
c) Traceability between hazard log and potential tool faults, failures, and defects

13.3.1.4 RECOMMENDED:

a) Treatment of safety related risks at the component level via use of an acceptable fault model.
EXAMPLE: A compiler might create incorrectly compiled code; the fault model can be that software created by that compiler has an arbitrary failure that can result in possible incidents if unmitigated. More specific, restrictive fault models can be used for tools, but such an approach can increase argument complexity.

13.3.1.5 CONFORMANCE:

Conformance is checked via inspection of design, verification, validation, supplier management, and manufacturing evidence.

13.3.1.6.1 NOTE: In classical functional and system safety the distinction is often made between tools that can create or insert a defect in an item vs. tools that fail to detect a defect,

with greater emphasis on the former. However, to the degree that a primary mitigation strategy is based on identifying and mitigating risk based on field feedback, tools that fail to detect a defect increase in importance. Therefore, it is appropriate to argue that the degree of risk from failing to detect a defect is acceptable rather than simply assuming it is comparatively less important than preventing defect insertion.

13.3.2 Hazards and limitations associated with use of simulations shall be identified.

13.3.2.1 MANDATORY – N/A

13.3.2.2 REQUIRED:

a) Simplifications, assumptions, and abstractions in modeling, including:
    1) Sensors
    2) Actuators
    3) Physical characteristics of item
    4) Physical characteristics of environment
    5) Simplifications and abstractions in modeling the interaction between the item and the environment
b) Simplifications, assumptions, and abstractions applicable to simulation workload
    1) Representativeness of ODD
    2) Real time execution considerations
       EXAMPLES: Timing of simulated sensor inputs, task scheduling jitter, loop closure timing
    3) Inclusion of low probability safety related workload elements (i.e., edge cases)
       NOTE: This is not a requirement to include all possible edge cases. Rather, inclusion is supported by argument that the edge cases included result in acceptable risk
c) Issues with tool functionality, including at least:
    1) Translating models into internal simulation objects
    2) Physics simulation accuracy
    3) Representation and management of simulated time
    4) Simulation result reporting, including simulation failure reporting
    5) Performance of simulation monitoring functions
    6) Simulation management tools
d) Issues with workload, including at least:
    1) Incorrect workload data
    2) Corrupted workload data
    3) Missing workload data
e) Issues with experimental design, including at least:
    1) Experimental coverage
    2) Statistical analysis of results
    3) Workload data mismatch with experimental design

f) Hazard mitigation includes comparison of real-world item performance with simulation results
g) Issues addressed in requirement 13.3.1 applied to simulators and simulation tool chain
h) **Pitfall:** Machine learning based algorithms are prone to exploiting artifacts in simulation rendering.
EXAMPLE: Pedestrian clothing is simulated with predictable bitmap texture patches that look pleasing to human observers of simulation renderings. A machine learning algorithm learns to identify pedestrians via recognition of these patches rather than looking at overall object shapes, leading to elevated perception failure rates on non-simulated pedestrians.

13.3.2.3 HIGHLY RECOMMENDED – N/A

13.3.2.4 RECOMMENDED – N/A

13.3.2.5 CONFORMANCE:
Conformance is checked via inspection of tool classification analysis and tool qualification evidence related to simulations.

13.3.2.6.1 NOTE: Simulations, models, workloads, and related tooling can create hazards or contribute to risk if they generate data used in design, are used as the primary means of validating correction of a design defect, or otherwise relied upon in a role in which they can inject incorrect data or give false readings that risk has been mitigated.
EXAMPLE: A machine learning based development process uses biased simulation data to train a neural network. The simulation uses a predictable dithering algorithm for cleaning up image boundaries when superimposing pedestrian images on street scenes. This bias is exploited by a trained neural network, enhancing performance in simulation, but resulting in lower edge detection capability in real images. That in turn results in worse than acceptable pedestrian detection rates on specific types of patterned backgrounds in the real world. While this bias might be found in testing, the simulation can be said to have introduced a hazard.
EXAMPLE: A simulation is relied upon to validate a fix, but the experimental design component of the simulation has biases that overlook an important edge case that are reported as having been covered in the simulation report. Vehicle level testing samples simulation results for confirmation, but does not have budget to reproduce all edge cases purported to be covered by the simulation. This results in higher than argued net risk.

13.3.3 The risks associated with tools shall be acceptably mitigated.

13.3.3.1 MANDATORY:
a) Analysis of acceptability of each tool against identified safety related implications
b) Analysis of confidence in the tool including measures taken for avoidance of errors

13.3.3.2 REQUIRED:
a) Include risks associated with use of simulation
b) Adherence to tool developers usage and limitation instructions

c) Change analysis and requalification of tools after each tool update, including security patches (if any)
    1) Requalification required after any change to tool and/or its operational environment
    2) Extent of requalification informed by impact analysis
d) Configuration management of tool chain associated with each fielded release candidate
e) Root cause analysis to include possible tool related problems
f) **Pitfall:** Over-reliance and unquestioning belief in tool performance based on seemingly trouble-free experience is prone to missing subtle but important safety related tool defects.
g) **Pitfall:** Root cause analysis that does not consider potential tool faults is prone to mischaracterizing faults that may have been caused or missed by tools

13.3.3.3 HIGHLY RECOMMENDED:

a) Analysis of external-to-tool risk mitigation techniques applied to item
   EXAMPLE: Application-provided strong error detection coding used to mitigate risk of undetected file item corruption by a tool that stores an application memory image.
b) Depending upon the safety implications, acceptable measures for avoidance of errors in the item, potentially including:
    1) Restrictive use of tool
    2) Use of service history in establishing tool dependability
    3) Specify design assurance techniques applied to tool
    4) Use of specific safety standards in building the tool
    5) Validation of any assumptions in modeling error prevention and detection
    6) Verification and validation of tool output
    7) Select the simplest fit-for-purpose tool available

13.3.3.4 RECOMMENDED – N/A

13.3.3.5 CONFORMANCE:

Conformance is checked via inspection of tool classification analysis and tool qualification evidence.

13.4 COTS and legacy risk mitigation

13.4.1 Safety related risks from Non-Development Item (NDI) components shall be identified and mitigated.

13.4.1.1 MANDATORY:

a) Identify contribution to hazards from NDI information, functions, components, and pedigree, including both hardware and software aspects of each
   EXAMPLES: LIDAR sensor, RADAR sensor, cameras, antennae, electronic throttle control module, CPU chip, GPU chip, data processing component, logic bearing devices, ECU, real time operating system, event based operating system, network protocol

stacks, map database, data used to pre-train machine learning, other safety related components

NOTE: The term “NDI” is intended to be used expansively, and includes COTS, SOUP, legacy, third party open source software, and other characterizations of components which are not completely assessed on their own merits within the safety case.

NOTE: To the degree that NDI components have complete information available, they can be treated as SEooC components. (See Section 5.7.)

b) Ensure the risk contributions from COTS information, functions, components, and pedigree are mitigated.

13.4.1.2 REQUIRED:

a) Software components, if used
EXAMPLES: Operating systems, library functions, network protocol stacks, autonomy functions, autonomy design frameworks

b) Hardware components
EXAMPLES: CPU, GPU, computing module, logic bearing components, Electronic Control Units (ECUs)

c) Other COTS, and SOUP components

d) Other legacy components for which safety case information is not of comparable scope, quality, and depth to produce acceptable safety case contribution without further work.

e) Remote software functionality, if used
EXAMPLE: Infrastructure data sources, other-item data sources

f) On-line services, if used
EXAMPLE: Cloud-based map data, weather report feeds

g) Identify and argue acceptable risk mitigation dependent upon the correctness and accuracy of third-party information.
EXAMPLES: Data sheets, component safety reports, certification of conformance of a component to a safety standard
NOTE: The intent is to identify places in the safety case where incorrect, incomplete, or misleading information from a third party could invalidate the safety case.

h) Ensure that any argument relying in whole or in part upon third party evaluation provides complete and correct information for the safety case.
EXAMPLE: Using evidence of independent assessment that a component has been assessed as conformant to ISO 26262 ASIL C provides only part of the information needed for an argument. There must still be credible argument and evidence that, for example, the assessment was performed by an independent qualified assessor and covers hazards relevant to the safety case.

i) **Pitfall:** Relying upon a certificate or other finding of conformance of a COTS component to any safety standard (including this one) is prone to overlooking mismatches between the context and scope of that conformance finding and the needs of the safety case for the item that component is embedded within.

j) Mitigate risks related to mismatches between COTS assessment materials and needs of an acceptable safety case, including at least:

1) Hazards in item safety case were not all considered in COTS component assessment
2) Risk mitigation required by item safety case does not match mitigation evaluated by COTS component assessment
3) Risk mitigation required by item safety case does not match mitigation model used for COTS component assessment
   EXAMPLE: Component assessed to ISO 26262 takes credit for assumed controllability of faults that is not actually provided by the item
4) COTS component safety manual (or similar) does not provide all information needed by safety case
5) COTS component is being used in a context or for a function that does not match the context or function for which assessment was performed
   EXAMPLE: Different assumptions about item operational environment

13.4.1.3 HIGHLY RECOMMENDED – N/A

13.4.1.4 RECOMMENDED – N/A

13.4.1.5 CONFORMANCE:
Conformance is checked via inspection of safety case.

13.4.1.6.1 NOTE: The term “NDI” is intended to be expansive, including software not developed within the context of the safety case being assessed. This includes potentially legacy code developed by the same team which does not have sufficient information available to provide an acceptable contribution to the safety case of the current item.

13.4.1.6.2 NOTE: It is not the intent of this standard to create a need for reworking acceptable, existing safety analysis, evaluate and assessment. However, it is essential that any differences between an existing assessment and an acceptably rigorous safety case be identified and reconciled. Mere existence of a certificate of conformance does not presumptively qualify a component for use in the item being assessed. Gaps potentially include non-technical considerations such as independence of assessment. As a practical matter it is desirable for NDI components to either (i) have complete information available to contribute to the safety case (which generally results in a safety case structure equivalent to that which would be expected if developed as part of the item under consideration), or (ii) provide both a credible assessment result to a different standard combined with additional safety case content to fill any gaps left by that credible assessment result.

13.4.1.6.3 NOTE: Once a suitable safety case for a COTS or legacy component has been created, it is reasonable to treat the component as a SEooC if it is advantageous to do so. Creating a SEooC interface might, for example, insulate the main safety case against issues such as the component argument being in a different natural language than the main safety case.

14 Lifecycle Concerns

14.1 General

14.1.1 Hazards and risks related to lifecycle activities and phases shall be mitigated.

14.1.1.1 MANDATORY:

a) Identify lifecycle hazards and risks related to at least the following lifecycle phases:
   1) Requirements/Design V&V (See Section 14.2)
   2) Handoff from design to manufacturing (See Section 14.3)
   3) Manufacturing and item deployment (See Section 14.4)
   4) Supply chain (See Section 14.5)
   5) Field modifications and updates (See Section 14.6)
   6) Operation (See Section 14.7)
   7) Retirement and disposal (See Section 14.8)

14.1.1.2 REQUIRED:

a) Identify hazard mitigation for each identified hazard, including but not limited to:
   1) Hazard mitigation mechanism or activity
   2) Periodicity or triggering event for activating the mechanism or performing the procedure
b) Where hazard mitigation on its own is unacceptable to mitigate risk, identify additional risk mitigation, including at least:
   1) Risk mitigation mechanism or activity
      EXAMPLE: Transition to degraded operational mode if component failures exhaust available redundancy required to maintain current operational mode.
   2) Periodicity or triggering event for activating the mechanism or performing the procedure
      EXAMPLE: Running a proof test every fixed number of operational hours to mitigate the risk of accumulated latent faults that cannot be diagnosed by BIST.
c) Acceptable documentation, procedures, tooling, and other requirements for performing mitigation activities
   1) Acceptable data collection, field engineering feedback, quality checks, and any other relevant activities are in place to ensure required lifecycle risk mitigation activities will be performed acceptably, including at least:
      i. Evidence of completion of data collection, field engineering feedback, and quality checks
      ii. Adherence of these activities to required procedures
      iii. Effectiveness of activities at achieving risk mitigation
      iv. Timeliness of analysis and feedback completion

2) Analysis of collected data to measure/improve performance of risk mitigation activities as necessary to support the safety case

14.1.1.3 HIGHLY RECOMMENDED:

a) Record safety related maintenance and inspections, including automated as well as manual, in an auditable manner
b) **Pitfall:** Failure to monitor performance of maintenance and other life cycle risk mitigation activities is prone to elevating the risk of unacceptable performance of those activities.

14.1.1.4 RECOMMENDED:

a) Account for jurisdiction-specific aspects
EXAMPLE: Mandatory periodic governmental item safety inspection with different requirements in different jurisdictions for a multi-jurisdiction ODD

14.1.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.1.1.6.1 NOTE: The Requirements/Design portion of the lifecycle is the subject of other sections and thus is not explicitly included in this section.

14.1.1.6.2 NOTE: Prototypes (e.g., public road testing and debugging of works-in-progress) require risk mitigation, but present additional risks, such as ensuring human safety supervisor attentiveness, that are beyond the scope of this standard.

14.2 Requirements/design validation

14.2.1 Hazards and risks related to requirements and design V&V activities shall be mitigated.

14.2.1.1 MANDATORY:

a) Identify hazards and risks related to V&V activities and track to closure
    1) Related to performance of tests
    2) Related to the possibility of incorrect item behavior during testing
    NOTE: Correct behavior of risk mitigation measures cannot be assumed if the purpose of a test is to validate that the behavior in fact is implemented properly.
b) V&V Safety Plan including at least:
    1) Identify V&V hazards and risks
    2) Identify V&V risk mitigation approaches
    3) Establish an item for tracking identified and novel risks related to design V&V activities and tracking risk mitigation to closure

    NOTE: This plan covers ensuring that V&V activities are performed safely, which may impose additional requirements on permanent and/or temporary equipment and procedures

14.2.1.2 REQUIRED:

a) Consider safety while performing at least:
    1) Hardware in the loop testing
    2) Fault injection testing
    3) Fault diagnosis testing
    4) Track testing
    5) Public road testing
    6) Other testing
b) Continual updates to risk mitigation associated with V&V activities in response to novel risks.
c) **Pitfall:** Assuming completeness of risk mitigation during requirements/design validation is prone to exposing validation team to undue risk.
    EXAMPLE: A failsafe design might itself be faulty (e.g., fail to activate as intended to mitigate a risk). Therefore, fault injection testing during design validation of the failsafe can expose the item and test humans to potentially unmitigated risks.

14.2.1.3 HIGHLY RECOMMENDED – N/A

14.2.1.4 RECOMMENDED – N/A

14.2.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.2.1.6.1 NOTE: This subsection is intended to cover whether design V&V activities themselves are safe, as opposed to the eventual safety of the item being designed.

14.2.1.6.2 NOTE: To the degree that design V&V might be performed in a way that exposes the public to risk, design V&V risk mitigation is considered in-scope for an independently assessed safety case prior to production system deployment.

14.3 Handoff from design to manufacturing

14.3.1 Hazards and risks related to handoff from design to manufacturing shall be mitigated.

14.3.1.1 MANDATORY:

a) Identify hazards and risks related to item handoff from design to manufacturing and track to closure
b) At time of handoff from design to manufacturing, positive assurance that:
    1) Software build matches validated software version
    2) Hardware configuration matches validated hardware configuration
    3) Item configuration matches safety case version
    4) No corruption to software and data images has occurred during handoff

5) There is no mix-up of components intended for specific lines of manufacturing: component intended for one item configuration was not mixed up and handed off associated with a different another model or version
EXAMPLE: At time of handoff to manufacturing the currently available LIDAR component is a different hardware version or has a different firmware version than the LIDAR component used during design validation.

c) **Pitfall:** Lack of ability to ensure that a deployed item's configuration conforms to a validated configuration is prone to resulting in unsafe deployed items.

14.3.1.2 REQUIRED:

a) Handoff requirements apply to both new builds and updates

14.3.1.3 HIGHLY RECOMMENDED:

a) No adverse security events have occurred during handoff, according to the security plan

14.3.1.4 RECOMMENDED – N/A

14.3.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.3.1.6.1 NOTE: If any hardware, software, or component changes between design validation and release to manufacturing, the safety case is updated with any associated validation informed by impact analysis. That update can be treated either as a pre-release design change or as a field update or otherwise handled in an acceptable manner at the discretion of the developer.

14.3.1.6.2 NOTE: Release to manufacturing occurs both for primary builds and for updates to existing deployed items. The requirements of this section are intended to apply to both. It is noted that commonly updates are applied to a baseline as part of the process of manufacturing items. In the end, all portions of an item (including the original build and any updates) are checked to ensure that the safety case that matches the operational item configuration.

14.3.2 The item build process shall be defined.

14.3.2.1 MANDATORY:

a) A build process including at least the following elements:
    1) Creation of a manifest (i.e., list of hardware and software components with versioning information included)
    2) Define and assure conformance to build process acceptance criteria
    EXAMPLES: Acceptable static analysis results, test suite results, malware check results, software licensing analysis
    3) Perform build package integrity validation
    EXAMPLE: Auditable record of check that item being validated exactly corresponds to the item being deployed
    4) Software configuration management

14.3.2.2 REQUIRED:

a) Coordination of multiple build packages
NOTE: In the event that multiple build processes are used, they need to be coordinated so that the deployed product operates with a defined version of all components that have been subject to an acceptable build procedure.
EXAMPLE: coordination between vehicle control build, infotainment system build, remote database build.

14.3.2.3 HIGHLY RECOMMENDED:

a) Include SQA process considerations
EXAMPLE: Include quality metrics that affect release decision
b) Include any updates that are intended to be applied to a baseline configuration within the item manifest.

14.3.2.4 RECOMMENDED – N/A

14.3.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.3.3 The item build process shall provide acceptable results.

14.3.3.1 MANDATORY:

a) Quality assurance regarding execution of build process

14.3.3.2 REQUIRED:

a) Consideration of build process defect as a root cause when performing failure diagnosis

14.3.3.3 HIGHLY RECOMMENDED:

a) Historical tracking of build process quality

14.3.3.4 RECOMMENDED – N/A

14.3.3.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.3.4 Item configuration shall be managed on builds and release of builds to manufacturing.

14.3.4.1 MANDATORY:

a) An item configuration management process defined including at least:
    1) Software image installed in each item instance
    2) Hardware component manifest for each item instance, including each part number, manufacturer, and part revision
    NOTE: This is intended to be at the “field replaceable unit” level, and is not intended to require identification of lower level subcomponents.

3) Safety case associated with each item instance at time of manufacture

b) Software configuration information and data acceptable to completely recreate the build from archived data, including at least:
   1) Software source, libraries, and other components
   2) Development tool chain
   3) Calibration data and other data files
   4) Data used for V&V
   5) Test plans, procedures, scripts and tooling
   6) Updateable firmware images and other software images for software source code not under developer control for components
      EXAMPLE: Snapshot of the firmware update image for radar sensor that had been applied during validation testing
      NOTE: This is not intended to mandate providing firmware images to the item integrator if a component is not firmware updateable. Rather, it is intended that if it is possible for a component to have more than one firmware image in its lifetime, that firmware image must be kept available in case it is needed for a configuration rollback, diagnosis, or other purposes

c) **Pitfall:** Differences between a build version released to manufacturing and the corresponding build version associated with the relevant safety case are prone to rendering the safety case invalid.

14.3.4.2 REQUIRED:

a) Require component suppliers to update component version number any time there is a change in the component's hardware or software manifest.
b) Automated software build process

14.3.4.3 HIGHLY RECOMMENDED:

a) Disaster recovery capability for stored data images and configuration data to ensure build data information can be recovered at any time for any deployed item instance
b) Configuration management of training and validation data used for machine learning and other techniques
c) Configuration management of per-unit calibration data
   EXAMPLE: The calibration data as well as relevant test equipment calibration information might be stored so that if a systematic factory calibration error is discovered it is possible to determine which units are in need of recalibration.
d) Configuration management of on-line data sources used for validation
   EXAMPLE: Snapshot of map, weather, traffic, and other on-line databases used for item validation, taking into account that if live data is used it will change over time.
e) Configuration management for software or firmware associated with manufacturing process at time of release
   EXAMPLE: Firmware version of device programmer used to transfer software image to components during the manufacturing process

f) **Pitfall:** Inability to document and demonstrate that a build version released to manufacturing corresponds to an acceptable safety case is prone to making the safety case invalid for that build version.

14.3.4.4 RECOMMENDED:

a) Configuration management of internal-to-component builds and configuration information from component suppliers
EXAMPLE: Software and hardware manifests for components are either provided by component suppliers or maintained in case of need by component suppliers

14.3.4.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.3.4.6.1 NOTE: The level of granularity for hardware and software component version tracking is at the discretion of the developer. However, at the item level it is essential that any change in a component results in a change in the component versioning information as reflected in the configuration management system so that the exact version of hardware and software is recorded for each item instance. For items in which each component has unique calibration data, this may result in the serial number for that component also being recorded and an image of the calibration data associated with the applicable safety case version being retained.

14.4 Manufacturing and item deployment

14.4.1 Hazards and risks related to item deployment shall be mitigated.

14.4.1.1 MANDATORY:

a) Identify hazards and risks related to manufacturing and item deployment and track to closure
b) Safety related checks, inspections, and other actions performed on early deployed items
EXAMPLE: Engineering validation deployment, type approval activities
c) Safety related checks, inspections, and other actions performed on each instance of the item
EXAMPLE: End-of line check, dealer preparation, required commissioning activities by item owner of purchased item.
d) Safety related aspects of manufacturing process, including:
    1) Use of approved components
    2) Use of correct version of components (hardware, software, other)
    3) Use of correct assembly processes
    4) Observance of manufacturing process parameter limitations
    EXAMPLES: Storage temperatures, component temperatures during circuit board assembly
e) Pre-sale operations
EXAMPLES: Maneuvering in marshalling and storage areas, placement in showroom or

other display location, ferrying between storage and display locations, customer demonstration drives

14.4.1.2 REQUIRED:

a) Activities, assumptions, and other factors relevant to risk mitigation credit taken
EXAMPLE: Vehicle retailer is expected to notice and initiate repair of any sensors damaged in transport
b) Ensure any changes made since the build release to manufacturing are accounted for in the safety case, including at least changes to:
    1) Software manifest
    2) Hardware manifest
    3) Component versions
    4) Accumulation of additional data that might serve to invalidate assumptions made in the safety case
    5) Changes due to repairs of manufacturing defects
    EXAMPLE: Different version spare part used to correct a faulty component discovered at end of line testing

14.4.1.3 HIGHLY RECOMMENDED – N/A

14.4.1.4 RECOMMENDED:

a) Ensure that any government-required inspections or tests have been performed satisfactorily and results documented as required
NOTE: Government-required inspections or tests for which credit has been taken in the safety case are REQUIRED.

14.4.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.4.1.6.1 NOTE: This clause covers aspects of item safety that can be compromised by manufacturing, post-manufacturing checks, distribution, and commissioning for use. Maintenance and inspection aspects of the safety case itself are treated in a different section

See also: safe item operation during maintenance activities in Maintenance, Section 15.

14.5 Supply chain

14.5.1 Hazards and risks related to the supply chain shall be mitigated.

14.5.1.1 MANDATORY:

a) Identify hazards and risks related to the supply chain and track to closure
b) Component management plan addressing at least the following:
    1) Supply chain and manufacturing quality assurance
    NOTE: Developer is responsible for ensuring acceptable supplier work product quality

2) Unapproved item and component modifications
   EXAMPLES: Substitution with components with reduced operating specifications (e.g., reduced temperature range), salvaged parts that have not been acceptably requalified for use
3) Unapproved spare components or supplies
   i) For manufacturing
   ii) For maintenance

   EXAMPLES: Counterfeit components, use of unapproved substitute sub-components, use of unapproved materials, use of unapproved software image, use of unapproved mechanical item components such as sensor and actuator elements, and other types of Suspected Unapproved Parts (SUP)

14.5.1.2 REQUIRED:

a) Quality fade of supplier work products across manufacturing lots
   EXAMPLES: Reduced quality components, reduced quality execution of processes, reduced quality safety case data from supplier incorporated into item safety case

14.5.1.3 HIGHLY RECOMMENDED – N/A

14.5.1.4 RECOMMENDED:

a) Include supply chain attacks within scope of security plan
   1) Tool chain attacks
      EXAMPLE: Tool chain that inserts malicious code into item images
   2) Software component attacks
      EXAMPLE: Functional defect inserted into open source software
   3) Hardware component attacks
      EXAMPLE: Chip mask modification
   4) Cryptographic key provisioning & TPM provisioning attacks
   5) 3-D printing data attacks
      EXAMPLES: Material substitution, design alteration

14.5.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, handoff processes, evidence and consistency or related quality checks (conformity inspections, manufacturing process inspections etc.), and demonstration.

14.5.1.6.1 REFERENCES:

a) Suspected Unapproved Parts Program Plan, FAA, October 6, 1995.
b) ISO 28000 Supply Chain Security Management
c) SAE AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
d) SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors
e) FAA AC 21-29D – Detecting and Reporting Suspected Unapproved Parts

14.5.1.6.2 NOTE: An “unapproved” part is one that potentially does not provide the same safety related capabilities as an approved part including operational and non-operational characteristics. If component wearout or aging is a safety related consideration, a previously approved part that has been used but is sold as new could be unapproved (e.g., a secondary cell battery with insufficient remaining recharge cycles). Similarly, an otherwise legitimate component that was manufactured earlier than represented could be unapproved (e.g., a primary cell battery with a limited shelf life and fraudulent expiration date). “Approved” does not necessarily mean that any formal inspection has been conducted on the part so long as there is an acceptable level of assurance that the part is fit for purpose.

14.6.1.6.3 NOTE: in this context, the term “component” includes an individual or bundled replaceable units and/or sub-assemblies that may have been produced either in-house or by a supplier. It also includes hardware, software, data, and services as applicable.

14.6 Field modifications and updates

14.6.1 Hazards and risks related to field modifications shall be mitigated.

14.6.1.1 MANDATORY:

a) Identify hazards related to field modifications and track to closure
b) A Field Modification Plan for safety related aspects of the item

14.6.1.2 REQUIRED:

a) The Field Modification plan addresses:
    1) Problem reporting and root-cause analysis
    2) Planned changes
       EXAMPLE: ODD expansion
    3) Unplanned changes
       EXAMPLE: Emergency bug fix, emergency security patch.
    4) Change impact analysis encompassing at least:
        i) Safety and safety case changes
        ii) Functionality changes
        iii) Interface changes
        iv) Process changes
            NOTE: Includes all applicable processes such as design, manufacturing, supplier processes, and quality assurance
    5) Change control, change approval, and update management of item and product families
        i) Problem reporting, triage, tracking of components or software used in multiple items
        ii) Validation across different configurations in deployed cohort
        iii) Approval of release candidate for release (Release Process), including main versions, minor versions, updates, “hot fixes,” etc.

iv) Sunsetting obsolete configurations
EXAMPLE: Disabling of orphaned configurations that are no longer supported by update and validation activities or which no longer have a valid safety case
v) Ensuring changes are reflected in safety case
vi) Define risk acceptance policies
EXAMPLES: Policies for unfixed anomalies, less than complete re-validation, deployment of urgent fixes in parallel with re-validation

6) Field modification and adaptation process safety impacts, including at least:
i) Software updates
ii) Hardware updates and/or upgrades
iii) Calibration data updates
iv) Machine-learning related data updates
v) Other data updates
vi) Update delivery mechanism
EXAMPLES: Over-the-air, USB drive delivery to customer, dedicated technician update tool
vii) Any self-modifications, including configuration management and validation of self-modifications

7) Timely execution of recalls and updates
i) Timely deployment of recalls and updates
ii) Ensure updating process does not reduce operational safety
EXAMPLE: Update triggered while item is in operation that reduces operational safety
iii) Ensure updating process does not reduce non-operational safety
EXAMPLE: Passenger stranded in dangerous environment such as a hot desert or rising flood waters during extended update
iv) Ensure timely completion of non-software recalls
v) Establish item requirements for operation when recall corrections and updates have not been performed in a timely manner
EXAMPLE: Degrade vehicle speed or ODD until necessary recalls and/or updates have been performed
vi) Update integrity per security plan
EXAMPLES: Authenticity, data integrity, configuration compatibility

b) **Pitfall:** Making installation and activation of safety related updates and modifications dependent upon accepting a statement regarding legal obligations or terms of service is prone to dis-incentivizing system owners from installing necessary safety updates.
NOTE: Especially problematic is imposing new unfavorable licensing terms in exchange for providing a safety update. This is not intended to preclude establishing legal terms and conditions for updates at the time of initial item acquisition.

c) Software/hardware updates should follow the same processes as noted in the safety case unless an update to that aspect of the safety case is warranted by change impact analysis
d) Risks related to use of over-the-air update mechanisms, including associated security risks (if used)

14.6.1.3 HIGHLY RECOMMENDED:

a) Change control/approval & update management of product families
    1) Problem reporting and triage across product families
    2) Ensuring resolution of identified issues to components or software used in multiple products
    3) Validation across different configurations in deployed cohort
    4) Ensuring changes are reflected in safety cases for affected product families
b) Support for mixed configuration cohort operation during mid-life hardware upgrade or required hardware upgrade rollout
    EXAMPLE: Period of time during which hardware updates are deployed to a cohort
c) Extended mixed configuration cohort operation
    EXAMPLE: Use of multiple suppliers for safety related components that purport to meet identical specifications but do not have identical implementations, and therefore potentially have different unknown latent defects or other safety related issues
d) Unauthorized aftermarket item alterations and/or added equipment that invalidate the safety case
e) Ensure that non-mandatory changes and updates do not cause reduction in safety margins when not installed

14.6.1.4 RECOMMENDED – N/A

14.6.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.6.2 Hazards and risks related to software and data updates shall be mitigated.

14.6.2.1 MANDATORY:

a) Software Update Safety Plan for ensuring acceptable updates to safety argument and maintenance/operational requirements in response to at least the following:
    1) Software updates
    2) Repair and maintenance procedures
    3) Component updates
    4) ODD definition updates
    5) ODD changes

14.6.2.2 REQUIRED:

a) Execution of applicable processes in Software Update Safety Plan for each software update

b) Update safety impact analysis considering at least the following:
    1) Safety argument changes
    2) Maintenance changes
    3) Operational procedure changes
    4) Calibration data changes
    5) Map & data updates
    6) Behavioral rules
       EXAMPLES: With regard to obeying traffic laws, interaction rules
    7) Infrastructure expectations
       EXAMPLES: Signage types, road marking materials
    8) Repair and maintenance triggering events and/or periodicity
    9) Computer upgrades, sensor upgrades, electromechanical upgrades
    10) Augmentation of training data and re-training of machine learning based functionality
    11) Model and simulator updates
    12) Tool updates
       EXAMPLES: Use of new compiler, new static analysis tool, new build tool
    13) Failsafe updates
    14) Monitor updates
    15) SPI & metric updates
       EXAMPLES: Revisit prototype and models to ensure continued SPI validity; map previous results onto new models if acceptable
    16) V&V methodology updates

14.6.2.3 HIGHLY RECOMMENDED – N/A

14.6.2.4 RECOMMENDED:

a) Compliance with relevant governmental regulations
   EXAMPLE: 49 CFR § 573.6 - Defect and noncompliance information report

14.6.2.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.7 Operation

14.7.1 Hazards and risks related to the operational portion of the item lifecycle shall be mitigated.

14.7.1.1 MANDATORY:

a) Hazard and risk mitigation approaches performed during specific mission phases:
    1) Start of mission checks
       EXAMPLES: Minimum Equipment List (MEL) check, calibration check, configuration check, update check, and self-test

2) During-mission checks
EXAMPLES: Memory image integrity, Built In Self-Test (BIST) status

14.7.1.2 REQUIRED:

a) Other hazard and risk mitigation approaches performed during specific mission phases
b) Risk mitigation via proof tests
EXAMPLE: Activation of backup items and failsafes to ensure fault detection
c) Specify any checks or inspections required of drivers and passengers, including at least:
1) Identify procedure
2) Argue effectiveness
3) Argue that checks and inspections will be done with acceptable quality and frequency
d) Risk mitigation during non-operational and upkeep scenarios, including at least:
1) Refuel/recharges
2) Short term storage
3) Long term storage
4) Equipment protective measures
EXAMPLE: Use of tarps and covers
5) Cleaning
EXAMPLE: Manual and automated car washes
6) Routine servicing
EXAMPLE: Safety during fluid refill operations, tire pressure maintenance, replace wiper blades
7) Routine inspection
EXAMPLE: Safety during tire condition checks
8) Transport and towing
9) Decommissioning/Disposal
e) Risk mitigation during maintenance and inspection operations
1) Calibration operations
2) Inspections
3) Item repair
4) Post-maintenance item testing
f) Account for different potential deployment types
1) Managed fleets
2) Individually owned and maintained units
3) Deployment to different climates and environmental conditions within ODD
4) Deployment with different usage duty cycles
5) Deployment into different roles
EXAMPLE: Mostly freight vs. mostly passenger deployments for same item type
g) **Pitfall:** Assuming that passengers or other untrained humans will perform inspections is prone to resulting in poor conformance
NOTE: Hoping that a passenger or other civilian stakeholder notices an item problem

might be a helpful defense in depth approach, but is only a primary risk mitigation approach if it is specifically and credibly argued to be effective as part of the safety case.

14.7.1.3 HIGHLY RECOMMENDED – N/A

14.7.1.4 RECOMMENDED:

a) Safety of and support for required governmental inspections
EXAMPLE: Brake test on skid plate during annual vehicle inspection, honk horn on demand, activate wipers on demand, activate signals on demand even though operational scenario would not normally involve those operations.

14.7.1.5 CONFORMANCE:

Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.7.2 Hazards and risks related to item operation shall be mitigated.

14.7.2.1 MANDATORY:

a) Identify hazards related to item operation and track to closure
b) Road testing safety
NOTE: Details of how to ensure road testing safety are beyond the scope of this standard. This prompt element may be expected to correspond to a separate process and/or plan for ensuring road testing safety, the details of which are not assessed as part of this standard.
c) External human safety
EXAMPLES: Exposure to laser emissions, radio frequency emissions, collisions
d) Item and component failure safety
EXAMPLES: Vehicle fire, cargo fire, battery fire, explosive gas, toxic gas
e) Item maneuver safety
EXAMPLES: Excessive g force on passengers or cargo, too close to other item with dangerous/loose load, impalement by projection from adjacent item
f) Internal item physical & environmental hazards
EXAMPLES: Toxic fumes, biohazards (e.g. blood), dangerous cabin temperature, sharp edges, pinching hazard (including windows, doors, sunroof, seat adjustment), unsecured cargo, deployed air bags
g) Non-operational item behavioral risk
EXAMPLES: Running combustion engine of a short-term stored vehicle in an enclosed space, emission of explosive gases during charging, fire while charging, unexpected item or component movement in non-operational modes

14.7.2.2 REQUIRED:

a) Identify credit, if any, taken in safety argument for crashworthiness
    1) Vehicle safety mechanisms
    EXAMPLES: Crumple zones, shock absorbing bumpers, seat belts, air bags

2) Pedestrian safety mechanisms
EXAMPLES: Pedestrian air bag, vehicle geometry, operational speeds at/below 20 mph
3) Affects upon passengers, other road users, including dangerous equipment such as propulsion batteries subjected to a non-zero risk of fire after a crash

b) Passenger distress
EXAMPLES: Passenger medical emergency, incapacitated passenger
c) Operation in unsafe environments
EXAMPLES: Flooding, landside, bridge washout, smoke, tornado, hurricane, waterspout
d) Transitioning to other-than-operational modes in unsafe environments
EXAMPLES: Stopping on railroad tracks, parking with a hot catalytic converter in contact with a pile of tree leaves
e) Safety of any support for command override of safety mechanisms

14.7.2.3 HIGHLY RECOMMENDED:

a) Mitigating threats to passengers
EXAMPLES: Robbery via obstructing item, carjacking, ride share inter-passenger violence
b) Transportation of illicit/dangerous cargo
EXAMPLES: Automated bomb delivery, automated drug running, hazardous cargo
c) Unauthorized item operation
EXAMPLES: Improper transport of unaccompanied minors when adult occupant is required by operating rules, vehicle stops in street to block traffic intentionally as part of a protest, unauthorized operation in pedestrian zone, violation of city congestion rules
d) Exceptional authorized operation
EXAMPLE: Permitting authorized deliveries in pedestrian-only zones while recognizing that pedestrians are unlikely to be attentive to vehicles in such a zone, operation on sidewalks when permitted (e.g., for specialty delivery of heavy objects)
e) Test track & validation operation
EXAMPLES: Safety while testing failsafes and fault mitigation capabilities
f) Behavioral requirements if used by police and emergency responders

14.7.2.4 RECOMMENDED:

a) Support for command overrides of risk mitigation
EXAMPLES: Command to exceed speed limit in extreme situations (e.g., life threatening injuries motivate increased speed to an emergency room), escape from wildfire, escape from tornado
b) Remote control interfaces provided to infrastructure
EXAMPLE: Remote speed control commands
c) Remote control interfaces provided to law enforcement
EXAMPLE: Speed control, destination change, remote disable
d) Degraded functionality when under malicious attack in conformance to Security Plan

14.7.2.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.7.2.6.1 NOTE: The human factors involved with remote operations and supervision are essential to safety, but are beyond the scope of this standard.

14.8 Retirement and disposal

14.8.1 Hazards and risks related to component aging and obsolescence shall be mitigated.

14.8.1.1 MANDATORY:

a) Identify hazards related to component aging and track to closure
b) Replacement of worn-out components
EXAMPLE: Tires, wiper blades, batteries, non-volatile memory components that have reached their cycle limit, bearings for rotating sensors

14.8.1.2 REQUIRED:

a) Replacement of aged components
EXAMPLE: Tires, non-rechargeable batteries, one-time programmable non-volatile memory chips that have age-related data degradation, discolored optics lenses

14.8.1.3 HIGHLY RECOMMENDED:

a) Disabling of item which is no longer supported
EXAMPLE: Disable item autonomy when field engineering feedback and patching are no longer being performed, potentially due to developer going out of business.
b) Advance planning for obsolete components
EXAMPLE: End-of-life component purchases, mid-life upgrades in anticipation of component obsolescence
c) Replacement of unreliable components
EXAMPLE: Components which no longer have required reliability (e.g., have aged past the constant-failure-rate portion of the reliability bathtub curve)
d) Replacement of components which are no longer supported
EXAMPLES: Unsupported operating system versions, components for which issue identification, bug fixes and patches are no longer being provided
e) Disabling of item features which are dependent upon components that are no longer acceptably reliable
EXAMPLE: Item should not operate if safety related components that are too old or otherwise unreliable have not been replaced.

14.8.1.4 RECOMMENDED – N/A

14.8.1.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

14.8.1.6.1 REFERENCES:

a) DOT/FAA/TC-15/33 Obsolescence and Life Cycle Management for Avionics

b) Electronic Component Management Plans - IEC TS 62239-1:2015(E)

14.8.2 Hazards and risks related to item retirement and disposal shall be mitigated.

14.8.2.1 MANDATORY:

a) Identify and argue mitigation of retirement-related hazards
EXAMPLE: Degradation and malfunction of item controls due to extended exposure to adverse weather, freezing, or immersion in water requires retirement or major overhaul rather than simple repair due to decrease in overall reliability below acceptable limits

14.8.2.2 REQUIRED – N/A

14.8.2.3 HIGHLY RECOMMENDED:

a) Permanent disablement of item features and components that are deemed irreparable
EXAMPLE: Non-repairable component with failed internal redundancy disabled to prevent entry into supply chain as a counterfeit fully functional component

b) Detection and disablement of item components that have been exposed to unrecoverable environmental extremes
EXAMPLE: Resale of vehicles subjected to hurricane seawater flooding that have compromised electrical item connections

c) Safe procedures for legitimate item access denial to end user
EXAMPLE: Item repossession or disablement that leaves item owner in an unsafe condition such as stranded in a remote location

14.8.2.4 RECOMMENDED – N/A

14.8.2.5 CONFORMANCE:
Conformance is checked by inspection of safety argument, evidence, design documents, maintenance manuals, technician training, operational use-cases, and inspection of item.

15 Maintenance

15.1 Maintenance and inspection

15.1.1 Hazards and risks related to maintenance and inspection shall be mitigated.

15.1.1.1 MANDATORY:

a) Identification of safety related maintenance and inspection activities (See section 15.2)
b) Non-operational safety (See section 15.3)
c) Post-incident item behavior (See section 15.4)
d) Traceability of hazard log entries and risk mitigation to potential maintenance and inspection contributions to risk
   EXAMPLE: A particular inspection activity is part of a risk mitigation approach. That maintenance activity is traced to the risk it is mitigating.
e) Approach to ensuring required maintenance and inspections are performed on operational items (See also section 15.2.3)
   1) Identify approach to ensuring performance
   2) Identify approach to ensuring detection of maintenance and inspection nonconformance
   3) Ensure identified approaches are executed effectively
f) Approach to ensuring that maintenance and inspections do not degrade safety
   EXAMPLE: Damage to item during inspection, forgetting to reset maintenance override mechanisms before return to operation
g) Approach to addressing hazards caused by incorrect and/or incomplete maintenance

15.1.1.2 REQUIRED – N/A

15.1.1.3 HIGHLY RECOMMENDED – N/A

15.1.1.4 RECOMMENDED – N/A

15.1.1.5 CONFORMANCE:

Conformance is checked via consideration of subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

15.1.1.6.1 NOTE: In general this Section 15 is intended to encompass operational inspections and item maintenance. For other lifecycle aspects see Lifecycle, Section 14.

15.2 Required maintenance and inspections

15.2.1 Safety related maintenance and inspections shall be identified.

15.2.1.1 MANDATORY:

a) Identify safety related maintenance requirements. If none, so state.
b) Identify safety related inspection requirements. If none, so state.

15.2.1.2 REQUIRED:

a) Identify a fault model for maintenance and inspection requirements, including at least:
    1) Omitted and/or deferred
    2) Procedure performed incorrectly
    3) Incorrect procedure performed
b) Per-mission inspections and maintenance
   EXAMPLES: Inspection for sensor damage, sensor cleaning
c) Periodic inspections and maintenance
    1) Triggered by item usage
    2) Triggered by clock and/or calendar time
d) On-demand inspections and maintenance
   EXAMPLE: Triggered by condition monitoring or prognosis approach
e) **Pitfall:** Reliance upon a casual human interaction with the item to detect an issue is prone to an unacceptably high rate of undetected issues.
   NOTE: One way to help avoid this Pitfall is to ensure that required inspections and maintenance are performed automatically and/or by designated human inspectors/maintainers.

15.2.1.3 HIGHLY RECOMMENDED:

a) Maintenance and inspections for type deployment
b) Per item instance commissioning maintenance and inspections
c) Decommissioning maintenance and inspections
d) Maintenance and inspection fault model includes performed too often

15.2.1.4 RECOMMENDED – N/A

15.2.1.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence.

15.2.1.6.1 NOTE: It is important to capture the full range of safety related aspects of maintenance and inspection in the safety case to ensure acceptable definition and performance.

15.2.1.6.2 NOTE: If no inspection or maintenance is required for risk mitigation for a particular REQUIRED item, that prompt element can be annotated as “not applicable.”

15.2.2 The procedures for the performance of safety related maintenance and inspections shall be identified.

15.2.2.1 MANDATORY – N/A

15.2.2.2 REQUIRED:

a) Specify and document maintenance and inspections
    1) Procedures
    2) Approved components, materials, equipment
    3) Scheduling and/or conditions that require procedure to be performed (See Section 15.2.3)
    4) Validation of maintenance quality and effectiveness

15.2.2.3 HIGHLY RECOMMENDED:

a) Define minimum technical qualifications for personnel
b) Include expected multi-human checking, post-maintenance inspection, etc.

15.2.2.4 RECOMMENDED – N/A

15.2.2.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence.

15.2.3 The method for prompting and monitoring the performance of safety related maintenance and inspections shall be identified.

15.2.3.1 MANDATORY – N/A

15.2.3.2 REQUIRED:

a) Identify the mechanism, method, or trigger for prompting the performance of each maintenance and inspection item.
b) Include in identification the following factors:
    1) Reliance upon external-to-item scheduling support
    EXAMPLE: Based on calendar reminder system (See Section 13 regarding tool qualification)
    2) Reliance upon external-to-item data analysis
    EXAMPLE: Based on operational history records kept in a third-party database
    3) Item-generated reminders based on time, operational hours, operating history, etc.
    EXAMPLES: Engine maintenance, rotating part maintenance, power sources
    4) Procedural prompting tied to operational situations
    EXAMPLE: Start of mission checklist, daily operational checklist
    5) Conditional trigger based on item status monitoring
    EXAMPLES: Fluid levels, tire pressure, DTCs
    6) Component life limits
    EXAMPLES: Number of operational cycles, aging, nonvolatile memory write cycles, fluid aging, entering ascending portion of reliability bathtub curve

7) Other applicable factors

15.2.3.3 HIGHLY RECOMMENDED:

a) Environmental operational effects on maintenance and inspection scheduling
EXAMPLES: Extreme temperatures, salt exposure
b) Non-operational reliability considerations
EXAMPLES: Battery charge retention during idle periods, periodic movement to maintain lubrication when not in operational status
c) Identify the mechanism used to ensure the timely completion of each maintenance and inspection item, including if applicable:
    1) On-product detection of completion
    EXAMPLE: Sensing of refilled fluid
    2) On-product recording, logging, etc.
    3) Off-product recording, logging, etc.
    4) Audits, procedural enforcement

15.2.3.4 RECOMMENDED – N/A

15.2.3.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence as well as demonstration.

15.2.4 Risk due to maintenance and inspection faults shall be mitigated.

15.2.4.1 MANDATORY:

a) Identify safety related maintenance and inspection procedures

15.2.4.2 REQUIRED:

a) Arguments that any maintenance fault will be either avoided, or detected and corrected
b) Consideration of safety related maintenance faults including:
    1) Incorrectly performed maintenance and inspection procedures
    2) Use of substantively incorrect or unauthorized components or materials
    EXAMPLE: Use of warm weather fluid refill formulation in cold weather conditions that results in safety related frozen fluids
    NOTE: It is up to the safety case to define whether and how mitigation credit is taken for justified component and material authorization mechanisms.
    3) Deferred maintenance and inspections (including not performed at all)
    4) Unauthorized deviations from maintenance and inspection procedures
    5) Unqualified personnel performing maintenance and inspection procedures
    6) Improperly reporting deferred or incorrect maintenance and inspections as having been completed
c) Field engineering feedback collection and analysis of maintenance and inspection nonconformance
    1) Analysis to determine whether nonconformance rates are acceptable

2) Improvement of maintenance and inspection approach to improve nonconformance as required

15.2.4.3 HIGHLY RECOMMENDED:

a) Inclusion of malicious maintenance faults, such as supply chain faults including counterfeit components and materials

15.2.4.4 RECOMMENDED:

a) Periodic audits of field maintenance status of deployed items

15.2.4.5 CONFORMANCE:

Conformance is checked via inspection of design and validation evidence as well as demonstration.

See also: Lifecycle, Section 14, for safety of item during maintenance and inspection operations.

15.3 Non-operational safety

15.3.1 Hazards and risks related to between-mission status shall be mitigated.

15.3.1.1 MANDATORY:

a) Identify hazards related to non-operational safety
b) Mitigate risks related to non-operational safety

15.3.1.2 REQUIRED:

a) Human egress, including children & pets when non-operational
EXAMPLES: Human not locked in car after vehicle transitions to “parked & unattended” standby mode.
b) Recharge/refuel safety, including fume emission while unattended
EXAMPLES: Carbon monoxide emissions from hybrid electric vehicles, Hydrogen emissions from recharging electric vehicles with lead-acid batteries
c) Uncommanded movement, including both passive and active
EXAMPLES: Uncommanded parking brake release; unacceptable propulsion item activation; unacceptable auxiliary item movement
d) Safety during maintenance and other non-operational procedures
    1) Maintenance safety
    EXAMPLES: Disablement of functionality required to be disabled for safe maintenance; Component movement required as part of maintenance procedures
    2) Inspection safety
    EXAMPLE: Safety interlocks to permit safe access for inspection
    3) Towing and product transport safety

15.3.1.3 HIGHLY RECOMMENDED:

a) Safety issues related to long term storage, including

1) Inability to perform safety related software updates due to off-line item status
2) Depletion or aging of safety related materials and components
3) Disabled risk mitigation measures due to depletion of battery charge

15.3.1.4 RECOMMENDED – N/A

15.3.1.5 CONFORMANCE:
Conformance is checked via inspection of design and validation evidence as well as demonstration.

16 Metrics and Safety Performance Indicators (SPIs)

16.1 General

16.1.1 Safety Performance Indicators (SPIs) shall be incorporated into the safety case.

16.1.1.1 MANDATORY:

a) SPI metrics (See Section 16.2)
b) Metric data analysis and response (See Section 16.3)

16.1.1.2 REQUIRED:

a) Demonstrate item improvement responsive to metrics
    1) Metric definition supportive of item improvement
    2) Metric data collection and analysis
    3) Item improvement responsive to metrics
    4) Metric and safety case improvement responsive to field experience

16.1.1.3 HIGHLY RECOMMENDED – N/A

16.1.1.4 RECOMMENDED – N/A

16.1.1.5 CONFORMANCE:
Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.1.1.6.1 NOTE: “SPI” is similar in spirit to a Key Performance Indicator (KPI), but specifically related to safety and can extend beyond process activities.

16.2 Metric definition

16.2.1 The item shall be acceptable according to a defined set of safety metrics.

16.2.1.1 MANDATORY:

a) Define quantified SPIs for the overall item encompassing at least:
    1) Incident rates
       EXAMPLE: Violation of safety margins with no damage
    2) Rule violation rates
       EXAMPLE: Violation of traffic regulations and other rules with no damage
    3) Minor collision rates (property damage only)
    4) Minor injury rates
       NOTE: The division between minor and major injuries is at the discretion of the safety case consistent with use of this division responsive to other clauses.
    5) Major injury rates

6) Fatality rates
NOTE: Life critical metrics are applicable even to an item which is believed to be not substantively life critical. In such a case the target metric might be zero lost lives.

b) Item-level SPIs have a defined target value.
NOTE: A “target” value can be a desired value, or it can be a threshold such as a limit on incident frequency. This target value is set during development rather than after deployment. In some cases a target value might be general improvement over time so long as the initial item is acceptably safe to deploy.

16.2.1.2 REQUIRED:

a) Safety metrics categorized for at least each of the following:
1) By item exposure
EXAMPLES: Per vehicle operational hour, per vehicle kilometer, per vehicle mile, per scenario, per scenario family, per functional class of road
2) By human exposure
EXAMPLE: Per passenger-hour of exposure, per pedestrian encounter, effects of number of vehicle passengers for shared vehicles (e.g., fatality rate is a at least in part a function of number of fatal loss events combined with number of occupants at time of each loss event).
3) Events, incidents, and other field situations contributing to item safety metrics recorded as evidence in the safety case and be diagnosed to root cause

b) Safety metrics categorized by ODD subset, if used
NOTE: This prompt element is intended to address situations in which a vehicle is substantially more dangerous than acceptable in one portion of the ODD space, but that situation remains undetected in aggregate metrics due to counterbalancing above-target safety in a different portion of the ODD space. This is not a requirement for all ODD subsets to have identical risk, but rather a prompt to improve below-target ODD subsets.

16.2.1.3 HIGHLY RECOMMENDED:

a) Categorized by hazard rate occurrence, including mitigated hazards
NOTE: Can help validate assumed pre-mitigation hazard rates to ensure an acceptable level of risk mitigation has been used.

b) Categorized by relationship to item displaying behavior that passengers or road users find unexpected, provocative, or irritating

c) Categorized by demographic of involved parties
NOTE: Intended to identify patterns in mishaps due to biases in machine learning training sets or defects in ODD construction so that they can be corrected.

d) Metrics that address psychological comfort of humans
EXAMPLE: Passing closer than a cultural- and situational-dependent comfort zone might provoke psychological discomfort and/or trigger a human fight/flight response, compromising both perceived safety and potentially actual safety.

16.2.1.4 RECOMMENDED:

a) Categorized by relevant crash characteristics that could inform blame determinations
EXAMPLE: Ego vehicle is hit from behind at a stop sign is by default blamed on the other, trailing vehicle.
NOTE: An elevated rate of not-blamed loss events could still be indicative of safety issues, such as the item behaving in a manner that provokes mistakes by human drivers. It is not the intention of this standard to require assigning blame, nor to determine where the right balance is for such issues. Rather, this prompt element is intended to help uncover potentially unacceptable blame-shedding behavior and other problematic safety related behaviors to ensure that mitigation has been done acceptably.
b) Making data as public as is practical; sharing data with other organizations
c) Include item-level metrics defined via industry collaboration

16.2.1.5 CONFORMANCE:

Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.2.1.6.1 NOTE: It is recognized that the question of “how safe is safe enough” is a complicated societal question. This standard does not seek to set a level of acceptability. However, at some point an item is either safe enough to deploy or it isn’t, with the added complication of potential uncertainty over the safety performance that will be achieved by deployed items. A determination of outcome via a lagging metric of field events is needed to close feedback loops that detect and correct latent shortcomings in the safety case or other aspects of the item.

16.2.2 SPIs shall be defined to detect potentially ineffective risk mitigation.

16.2.2.1 MANDATORY:

a) Identify SPIs for the effectiveness of risk mitigation in the safety case in a quantified manner, including at least:
    1) The occurrence of unmitigated hazards and partially mitigated hazards
    NOTE: These are hazards for which mitigation techniques did not completely succeed as designed.
    2) The occurrence of hazards that have been accepted without mitigation
    3) Violations of assumptions, design goals, and conclusions made based on an evaluation of evidence made in the safety case
    4) Collisions
    5) Incidents that are practicably detectable

    NOTE: Whether SPIs are counts, normalized rates, or otherwise scaled depends upon the specifics of the safety argument.

16.2.2.2 REQUIRED:

a) Safety related detected hardware and software component failures, even if the item was able to successfully mitigate risk

NOTE: This specifically includes failure of redundant components for which the redundancy permits continued operation so as to provide field failure rate data

b) Identify SPIs to ensure continual validation of aspects of the item based upon safety related statistical argument, covering at least:
    1) Misclassification rates for classification algorithms
    2) False negative detection rates
    3) False positive detection rates
    4) Prediction error rates
    5) Correlated fault and failure rates

    NOTE: Alternative designations than this list may be used so long as the designations used fully cover the required listed categories.

    NOTE: While error rates for sensor performance in principle cannot be known with certainty, data can and should be collected based on comparisons between sensors and other data sources that provide redundant data to estimate or bound field error rates.

    EXAMPLE: If an imager does not see a road sign that is in a map database then one of the two data sources is incorrect.

    EXAMPLE: If a LIDAR does not detect an object having a radar classification that should also be detectable by LIDAR, something has gone wrong.
c) Identify SPIs related to the item lifecycle, including at least:
    1) Post-deployment safety related software defect rates
    2) Field failure rates of safety related preventive and periodic maintenance items
    3) Field failure rates of items that are subject to inspection
    4) Field failure rates of life-limited items
    5) Field failure rates of corrective maintenance results
    6) Performance of inspections and maintenance

    NOTE: Can help detect issues with maintenance and inspection procedures and scheduling

16.2.2.3 HIGHLY RECOMMENDED:

a) Identify SPIs to detect item performance and quality issues, including at least:
    1) Software execution fault rate
       EXAMPLES: Watchdog timer activations, task crash rates, item crashes
    2) Real time performance fault rate
       EXAMPLES: Missed task deadlines, CPU overload
    3) Other software and hardware execution faults
       EXAMPLES: Resource allocation failures, non-real-time task hangs, single event upset rate, network packet error rate
    4) Other data supportive of predictive maintenance and component end-of-life predictions
b) Include a combination of item validation metrics, field experience metrics, and process metrics
c) Additional candidate metric types:

1) Security
2) Mission success rate
3) Failure mitigation success rate
4) Failure rates
5) Rate of encountering “surprises” (situations, objects, or other aspects of a potential ODD that are not contemplated by the definition of the intended ODD)

d) Inclusion of leading indicator SPIs such as:
1) Rate of identification of new hazards
2) Rework of safety related item components
3) Identification of software modules with high defect rates

e) Metrics to capture safety process progress, status, and completeness, especially those that take ownership of known current safety process gaps and help to assess the risk impact
EXAMPLES: Count items such as: hazards identified, hazards with a control, controls with a safety requirement, safety requirements with a safety verification, software level of rigor tasks completed vs required, safety verification passed/failed, etc.

f) **Pitfall:** Incidents that cannot be traced to unmitigated hazards are prone to indicating the presence of unidentified hazards and/or invalid risk acceptance decisions.

16.2.2.4 RECOMMENDED:

a) Making data as public as is practical; sharing data with other organizations
b) Incorporating publicly available data

16.2.2.5 CONFORMANCE:

Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.2.2.6.1 NOTE: These are generally leading metrics in that they can serve to provide data for detecting safety issues before severe loss events occur. While leading metrics might not perfectly predict deployment performance, they can be especially useful when they detect issues with the safety case. Some metrics discussed can also be considered lagging metrics when considering less severe loss events. The difference between whether a particular metric is considered leading, lagging, or both will depend upon the specifics of how that metric is used in the safety case.

16.2.2.6.2. NOTE: Aggregate metrics may be permitted within reason so long as coverage of the entire safety case is established and violations and invalidations of individual elements of the safety case are reasonably likely to be detected by the metric set. Relying solely upon item level lagging metrics is not acceptable.

16.2.3 SPIs shall be defined relating to interactions between the item, its subsystems, the defined ODD, and the environment.

16.2.3.1 MANDATORY:

a) Operational failure analysis to determine potential ODD departures, behavioral faults, and other anomalies to be monitored
   EXAMPLE: Identified using Functional Hazard Analysis, FMEA, or other methods as acceptable
b) ODD departures that were not purposefully and safely initiated by the item that violate or invalidate the currently active ODD, including at least:
   1) Environmental conditions
      EXAMPLE: Encountering ice in an ODD or ODD segment that assumes no ice is present; operation outside geo-fence; geo-fence boundaries changed during operation, instantaneously putting ego vehicle outside geo-fence while moving (e.g., while in newly activated construction zone)
   2) Infrastructure faults and exceptions
      EXAMPLES: Unmapped construction zone, unrecognized sign types
   3) Objects
      EXAMPLE: Encountering an object that is not supposed to exist in the ODD, such as a kangaroo in a typical North American driving ODD, or an object that does in fact reasonably exist in the ODD that is a gap in the current item design
   4) Events, maneuvers, behaviors, and other actions by external objects and infrastructure
      EXAMPLE: Wrong-direction traffic encountered on a one-way street
c) Ego item faults and behaviors
   EXAMPLE: Coincident failure of two supposedly independent redundant components, unexpected vehicle motion such as a spin-out regardless of whether the vehicle motion results in an incident.
d) Arrival rate of “surprises” and other exceptions, including at least:
   1) Known unknowns
      EXAMPLES: Arrival of events for which the arrival rate is unknown
   2) Unknown unknowns
      EXAMPLES: Novel objects and novel events which are present in the ODD but which are absent from training data, requirements, and other aspects of item design
   3) Ego item behavioral anomalies
      EXAMPLE: Control system has learned incorrect control actions from defective or biased training data

16.2.3.2 REQUIRED:

a) Identification of interface incompatibilities and non-compliant (to the interface specification) interactions between different vehicles, due to at least:
   1) Different types of vehicles

2) Vehicles from different developers
3) Vehicles and non-automated road users

16.2.3.3 HIGHLY RECOMMENDED:

a) Violations of assumptions and operational constraints implicitly built into the item
EXAMPLE: Automated movement command sequences or control strategies can induce accelerated mechanical wear out, fatigue cracking, loosening of attachments, and so on for equipment originally intended for human controlled vehicles.
b) Monitoring for recovery-induced incidents
NOTE: Approaches to recover from risky situations or mitigate risk could themselves be introducing unsafe conditions
EXAMPLE: False alarm emergency braking can increase the risk of being hit by other vehicles

16.2.3.4 RECOMMENDED:

a) Model based anomaly detection, such as:
1) Item controllability
EXAMPLE: Item behaves in manner that does not match control intent, indicating a defect in the item itself
2) Maneuverability
EXAMPLE: Item turns or changes speed faster or slower than anticipated, indicating a defective item model
3) Violations of current model of situational awareness
EXAMPLE: Obstacle appears suddenly without plausible pre-detection occlusion; obstacle appears from occlusion when prediction indicated this was very unlikely to occur
4) Violation of object models
EXAMPLE: Detected pedestrian (perhaps on roller blades) travels faster than pedestrians are supposed to travel, indicating either a defective pedestrian model, a classification ontology gap, or incorrect classification
b) Making data as public as is practical; sharing data with and from other organizations
c) Incorporating publicly available data

16.2.3.5 CONFORMANCE:

Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.2.4 SPIs that relate to fault and failure recovery shall be defined.

16.2.4.1 MANDATORY:

a) Activations of failsafes and other active risk mitigation capabilities, including at least:
1) Successful activations of failsafes (risk mitigation of an activated hazard is successful)
2) False alarm activations of failsafes

3) Unsuccessful activations of failsafes (risk mitigation unsuccessful)
4) Non-activations of failsafes when activation criteria should reasonably have been met

NOTE: It is recognized that false negatives might not all be detectible in practice. However, this item is not a requirement to detect all false negatives, but rather to have a metric strategy that attempts to characterize how often this might be happening, even if it is known to be an under-estimate.

b) Occurrence of impairment of safety related functionality, whether or not this has resulted in a field reportable event, including at least:
   1) Faults or failures of a backup component
   2) Faults or failures in a failsafe capability or mechanism
   3) Faults or failures in a recovery capability or mechanism

16.2.4.2 REQUIRED – N/A

16.2.4.3 HIGHLY RECOMMENDED – N/A

16.2.4.4 RECOMMENDED – N/A

16.2.4.5 CONFORMANCE:

Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.2.5 SPIs that relate to safety culture shall be defined.

16.2.5.1 MANDATORY:

a) Conformance to requirements for safety related aspects of the item:
   1) Process adherence
   2) Training and skill validation
b) Fraction of field identified defects traced back to deviations from development and validation processes, including at least:
   1) Approved technical deviations
   2) Unapproved technical deviations
   3) Failure to perform activities documented as having been performed
   4) Unacceptable quality in activities and artifacts

16.2.5.2 REQUIRED – N/A

16.2.5.3 HIGHLY RECOMMENDED:

a) Conformance to applicable requirements for non-safety related aspects of the item:
   1) Process adherence
   2) Training and skill validation

16.2.5.4 RECOMMENDED:

a) Making data as public as is practical; sharing data with and from other organizations
b) Incorporating publicly available data
c) Other safety culture related metrics acceptable to the item, team, and domain

16.2.5.5 CONFORMANCE:
Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.3 Metric analysis and response

16.3.1 Data for each defined SPI shall be collected.

16.3.1.1 MANDATORY:

a) Identify data collection mechanism
EXAMPLES: Run-time monitoring, on-vehicle data collection, incident report analysis
b) Describe data collection triggering mechanism, transmission method, and storage method
EXAMPLES: Data collection for a particular SPI is triggered by an on-item monitor and stored on the vehicle for later transmission; vehicle sends collected data periodically to developer data center

16.3.1.2 REQUIRED:

a) Data integrity assurance and retention, for data associated with each SPI including at least:
    1) Data integrity assurance mechanism
    EXAMPLE: CRC error detection code computed at source item and maintained end-to-end including developer data storage
    2) Data delivery assurance mechanism
    EXAMPLE: Sequence numbers and periodic heartbeat data reports to ensure that all items are reporting data and that no data has been lost
    3) Data provenance assurance mechanism
    EXAMPLES: Data includes item serial number, public key signature
    4) Data retention policy
    EXAMPLE: Field data is retained for life of deployed cohort
    5) Data configuration management
    EXAMPLE: Field data is linked to configuration of item it was collected from
    NOTE: item configuration changes can invalidate data relevance

16.3.1.3 HIGHLY RECOMMENDED:

a) Data collection and transmission cybersecurity measures in keeping with security plan, including:
    1) Data privacy
    2) Anti-tamper
    3) Anti-spoofing
    4) Non-repudiation

16.3.1.4 RECOMMENDED – N/A

16.3.1.5 CONFORMANCE:
Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.
See also: Run-Time Monitoring, Section 12.5.

16.3.2 Item improvement shall be conducted responsive to SPI data.

16.3.2.1 MANDATORY – N/A

16.3.2.2 REQUIRED:
a) Periodic analysis of data for each SPI
    1) Period based on amount of risk mitigation associated with the SPI
    EXAMPLE: An assumption that a life critical risk has been mitigated by a particular mechanism should require re-analysis of the accompanying SPI every time a related incident occurs
b) Comparison of each SPI against target value
    1) Violation of a SPI target treated as a field defect report and subject to corrective action

16.3.2.3 HIGHLY RECOMMENDED:
a) Statistical modeling and outlier detection
b) Use of metrics data for updating maintenance cycles
    EXAMPLE: Wear & tear data
c) SPI trend analysis to detect changes in item, operational environment, safety case assumptions, etc.
    1) Identification of normal and abnormal trends and values
    2) Identification of normal tolerance and expected trends

16.3.2.4 RECOMMENDED:
a) Analysis of correlations between SPIs
    1) Identification of violation of typical correlations
    2) Identification of correlated SPI values that are predictive of item issues

16.3.2.5 CONFORMANCE:
Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

16.3.3 Non-SPI data shall be analyzed for the purpose of validating and improving the predictive power of SPIs.

16.3.3.1 MANDATORY:
a) V&V of data analysis techniques used for SPI analysis
    EXAMPLES: V&V of tools, techniques, reporting, and summary capabilities used for

statistical analysis, trend analysis, tolerance violation as well as analysis of interrelated safety metrics etc.

16.3.3.2 REQUIRED:

a) Analysis of whether SPIs are correlated with or predicted a safety related field event in conjunction with each root cause analysis
b) Process created and followed to identify and implement new SPIs to cover novel hazards identified by root cause analysis
c) V&V of triggering conditions for SPI data collection

16.3.3.3 HIGHLY RECOMMENDED:

a) Periodic re-evaluation of and improvement of SPI strategy
    1) Retire SPIs that have poor predictive power
    2) Implement SPIs that promise good predictive power based on historical data
b) Identification of precursor metrics to permit intervention before a safety related event has occurred

16.3.3.4 RECOMMENDED – N/A

16.3.3.5 CONFORMANCE:

Conformance is checked via inspection of safety argument, evidence, metric definition, data collection, item change information and safety case change information.

17 Assessment

17.1 Conformance assessment

17.1.1 The safety case shall be assessed for conformance to this standard.

17.1.1.1 MANDATORY:

a) Creation and maintenance of conformance plan and assessment package (See Section 17.2)
b) Self-audit (See Section 17.2.2)
c) Independent assessment (See Section 17.3)
d) Conformance monitoring (See Section 17.4)
e) Prompt element feedback (See Section 17.5)
f) Safety case contents complete enough to enable reasonably effective and efficient independent assessment

17.1.1.2 REQUIRED – N/A

17.1.1.3 HIGHLY RECOMMENDED – N/A

17.1.1.4 RECOMMENDED – N/A

17.1.1.5 CONFORMANCE:
Conformance is checked via consideration of the safety case and subsection conformance checks, including traceable inclusion of each applicable prompt element in the safety case.

17.1.1.6.1 NOTE: The purpose of the conformance plan is to define and ensure activities are performed that will result in an initial satisfactory conformance assessment package, and also that as the item, process, environment, and other aspects of the item change the conformance assessment package will be maintained and suitable for independent reassessment as may be necessary. Further specifics are discussed regarding the properties of the conformance plan (see Section 17.2).

17.1.1.6.2 NOTE: The safety case includes activities performed by the developer staff and any subcontractors, collectively referred to as the “developer” for brevity. The conformance plan is created by the developer and the activities it describes are primarily performed by the developer, which can include gathering information and conformance plans of suppliers as appropriate. This includes a self-audit of conformance to ensure that the safety case is complete and well-formed before independent assessment. In contrast, the independent assessor confirms conformance, and may perform field engineering feedback (ongoing independent monitoring and reassessment).

17.1.1.6.3 NOTE: Any statement of conformance to this standard based on a subsetting of the standard not specifically permitted by the standard, without use of an independent qualified assessor, assessing less than the complete safety case, or claiming approximate conformance (e.g., “in the spirit of UL 4600” or “a version of UL 4600”) is presumptively invalid.

17.1.1.6.4 NOTE: Acceptable tailoring of this standard is accomplished by one of three methods. Method one is specifically stating exceptions, safety case deviations, and areas of inapplicability as part of the safety case while following the stated safety case deviation rules for each category of items. Method two is an explicitly stating tailoring approach in a publicly available end product standard, in which case the conformance claim is with regard to that end product standard and not UL 4600. Method three is defined in Section 17.3.4. Any other form of tailoring results in a determination of non-conformance.

17.1.2 Safety case conformance shall be determined with regard to the criteria in this standard rather than subjective assessor opinion.

17.1.2.1 MANDATORY:

a) Conformance determined by whether the safety case addresses prompt elements
See also: Section 4.1 for interpretation of MANDATORY, REQUIRED, HIGHLY RECOMMENDED, and RECOMMENDED prompt element categorizations.

17.1.2.2 REQUIRED:

a) Safety case material satisfying “identify” prompt elements cover at least:
    1) All sub-prompt elements provided in this standard (potentially with some designated not applicable)
    2) No traceability gaps to the rest of the safety case
    EXAMPLE: A requirement to identify the approach taken to mitigate each hazard has a gap if it does not actually include all hazards identified elsewhere in the safety case
b) Safety case material satisfying “describe” prompt elements provide a non-trivial description of the property or aspect of the system responsive to the prompt element
c) Safety case material relating to mitigation of a hazard includes non-trivial argument and non-trivial evidence of mitigation actually related to the hazard
d) **Pitfall:** Use of subjective assessor opinions of sufficiency of argument is prone to resulting in non-reproducible assessments.

17.1.2.3 HIGHLY RECOMMENDED – N/A

17.1.2.4 RECOMMENDED – N/A

17.1.2.5 CONFORMANCE:

Conformance is checked via consideration of the safety case and assessment report.

17.1.2.6.1 NOTE: **This clause is intended to increase assessment repeatability** by basing a finding of conformance primarily upon whether the safety case is well formed, internally consistent, and inclusive of the prompt elements included in this standard. **It is critical to note that as part of this approach, final responsibility for safety of the item rests with the design team, and not the assessor(s).** Assessors might have significant wisdom and guidance to provide to the design team with informal feedback where potential gaps are seen, but ultimately a finding of conformance is delivered if the safety case is well formed despite such gaps. Assessors have the option of recommending closing any such gaps via inclusion of

additional prompt elements or modification of deviation rules for specific prompt elements as feedback to the UL 4600 Standard maintenance process.

17.2 Conformance assessment package

17.2.1 A conformance package shall be created and maintained for inspection.

17.2.1.1 MANDATORY:

a) Conformance assessment plan documenting activities to support conformance
b) Complete safety case addressing all normative aspects of this standard
c) Each normative element of the standard traceable to the safety case (backward and forward traceability)
d) Identification of human language used for safety case goals and argument. (See Section 5.2.3.1.)

17.2.1.2 REQUIRED:

a) Conformance assessment package is acceptable
b) Identification of additional human languages used in evidence if other than the human language used for the safety case.
   NOTE: This can inform assessor personnel selection based upon language skills.
c) Normative clause and prompt element traceability includes at least:
   1) Clause and prompt element number of standard mapped onto safety argument sub-tree
      NOTE: Failure to establish traceability to this standard is likely to result in significantly increased assessment and maintenance costs due to the need to re-create traceability on-the-fly during assessment and safety case maintenance.
      NOTE: A uniform representation of subsections for this prompt element is: 17.2.1.2(b)(1).
   2) Explanation of strategy for conformance
      i) If strategy is not to conform to some non-MANDATORY aspect of this standard, this is stated along with a specific, acceptable rationale.
   3) Evidence of conformance
      i) Evidence is presented that supports the validity of permissible deviations
   4) All enumerative lists include an entry for “unknown,” “other” or similar catch-all for items that might have been missed in analysis.
      i) If it is analytically justifiable that “other” items cannot exist, justification for this as the contents of the “other” portion of the argument.
      ii) The validity of any implicit assumption that the catch-all bin is not relevant to item safety is an assumption that must have a supporting lifecycle monitoring activity.
      NOTE: this is explicitly intended to be a mechanism for monitoring the occurrence of “unknowns”
b) Include assessment records and reports

c) Configuration management of conformance package, including ability to associate and retrieve all valid conformance packages (including relevant independent assessment results) for inspection that apply or have applied to each unit manufactured for the life of that unit.
d) **Pitfall:** Any statement or finding of conformance in the absence of a complete conformance package is prone to being incorrect, and therefore is presumptively invalid.
EXAMPLE: If the conformance package is destroyed, lost in part or in whole, or corrupted after assessment, any conformance finding resulting from the assessment that relied upon that conformance package is invalidated.
e) If conformance strategy or evidence is based on an assumption, a supporting lifecycle activity has been defined in the safety case to monitor the validity of that assumption.
EXAMPLE: assumption without acceptable supporting data that a particular failure mode is implausible
f) Conformance assessment results from previous successful conformance assessments, if any.
g) Safety Case deviations documented according to type of requirement element (MANDATORY, REQUIRED, HIGHLY RECOMMENDED, RECOMMENDED)
See also: Section 4.1 for a description of requirement element types.
h) Safety case analysis work products and other documentation related to self-audit
NOTE: Any work products created for use by the self-audit are made available to the independent assessor. The objective is to improve repeatability and assessment efficiency by having the self-audit team (presumably more familiar with the item and tools) retain and provide work products likely to be revisited by the independent assessor.
EXAMPLES: Safety case traceability reports, manually generated audit worksheets, libraries of reference materials, component catalogs.
i) Documentation for tooling used to support self-audit to the extent tools are used

17.2.1.3 HIGHLY RECOMMENDED:

a) Tooling support for safety case:
    1) Creation
    2) Browsing
    3) Search
    4) Maintenance
    5) Static analysis
    6) Versioning and configuration management
    7) Self-audit and independent assessment book keeping and review support

17.2.1.4 RECOMMENDED:

a) Conformance assessment results from previous unsuccessful conformance assessments. (Especially if relied upon in some way by the safety case.)
EXAMPLE: If an unsuccessful conformance assessment required only comparatively minor corrections to the safety case, a successful conformance assessment might be

based upon the documented unsuccessful conformance results plus documentation of correction of identified minor issues.

b) Records from gap analysis, and other preparation activities not relied upon in an assessment may be kept, but are optional so long as they are not relied upon by a final (successful) assessment.

17.2.1.5 CONFORMANCE:

Conformance is checked by inspection of the conformance argument and safety case.

17.2.1.6.1 NOTE: The conformance package has two primary purposes: (1) Make it more straightforward for assessors to understand and assess the safety case (2) Provide durable documentation of the safety case used for a particular assessment.

17.2.1.6.2 NOTE: Each manufactured product instance might be associated with multiple conformance packages over its lifetime if the item or its conformance package has been updated. However, at any instant in time each instance of an item should be associated with exactly one conformance package.

17.2.2 The safety case shall be continually self-audited for conformance to this standard.

17.2.2.1 MANDATORY:

a) Self-audit effective execution of conformance plan (see Section 17.4.1)
b) Self-audit validity and completeness of safety case, excluding Independent Assessment provisions in Section 17.3.
c) Document self-audit results for safety case completeness and validity
    1) Documentation of audit method and results
    2) Self-audit results updated to correspond to the version of the safety case being independently assessed
    3) Specific attention to identification and documentation of “unknowns,” accepted risks, and other potential safety case gaps and associated risk evaluation

    NOTE: A self-audit can be provided by a contractor or other organization with a close working relationship with the item development team. Independence is not required. Significant familiarity with the specifics of the item, its use of technology, and its envisioned deployment are expected of the self-audit team.

17.2.2.2 REQUIRED

a) To the degree practicable, self-auditor performs all tasks expect of independent assessor, minus the expectation of independence.

    NOTE: A determination of conformance can only be made by an Independent Assessor

17.2.2.3 HIGHLY RECOMMENDED – N/A

17.2.2.4 RECOMMENDED:

a) Maintain self-audit results history and conduct retrospectives for process improvement

17.2.2.5 CONFORMANCE

The self-audit process is expected to result in a complete, well-formed safety case that is presented to the independent assessor.

17.2.2.6.1 NOTE: Important goals for self-audit include: ensuring that the safety case is well formed during the design cycle to avoid surprises from independent assessment; use of domain experts who are familiar with the specific item to ensure correctness and completeness of the safety case; avoid an untenable safety culture based on expecting an independent assessor to bear the burden of finding safety issues rather than using an independent assessor as a quality check on the safety case and its self-audit.

17.3 Independent assessment

17.3.1 Conformance shall be established based upon independent assessment of the conformance package as well as interviews and demonstrations.

17.3.1.1 MANDATORY:

a) The entirety of the safety case, including all argument and evidence, provided to the independent assessor.

17.3.1.2 REQUIRED:

a) Conformance to all normative clauses in the standard in accordance with Section 4.1
b) Demonstrations performed as requested by assessor.
c) Access to the entirety of the safety case being used as a basis for conformance assessment.
    1) Credit not given for elements of the safety case not provided to assessor.
d) Assessor provided timely access to the tooling used to support self-audit, including at least:
    1) Browsing tools
    2) Search tools
    3) Static analysis tools
e) Assessor provided timely access to evidence upon request
    NOTE: Access to evidence might require use of proprietary tooling. It is acceptable and often desirable for the design team to facilitate assessor access to evidence to avoid the cost of a long proprietary tool learning curve for the assessor.

17.3.1.3 HIGHLY RECOMMENDED:

a) Assessor selects demonstrations of relevant aspects of the safety case selected based upon expert judgment
    NOTE: While subjective, this is an audit mechanism for sampling the validity of the safety case and does not affect the actual safety case content. Demonstrations are used to compare the attributes of the item in operation to claimed attributes according to the safety case. Any mismatch found could be the basis for a finding of non-conformance regarding the mismatch safety case elements.

b) Additional available supporting evidence provided to assessor upon request
c) Ability to export safety case materials to non-proprietary data or commonly accessible freely viewable formats
   EXAMPLES: Plain text files, Portable Document Format (PDF) files
d) **Pitfall:** Making safety case information available only as exported “flat file” format data without access to proprietary browsing and analysis tools is prone to making the safety case impractical to work with for independent assessment.
   NOTE: Ability to export to a flat file can be useful, but is unlikely to be an efficient format for all assessment operations. A reasonable approach is that the Independent Assessor gets access to the same tooling support as used by the self-audit team.

17.3.1.4 RECOMMENDED:

a) The assessor is permitted to provide non-authoritative feedback as a result of assessment activities, including but not limited to:
   1) Identification of areas which seem likely to need attention before the next assessment, but which are currently in conformance
   2) Identifications of specific aspects of the safety case which need to be corrected.
      EXAMPLES: Risks that should be assigned an increased criticality; missing elements of the safety case; areas of unacceptable evidence
b) The assessor may use additional work aids in determining the validity, completeness, or plausibility of the safety case.
   1) Independent Assessor work aids do not have to be made part of the conformance package
   2) Any finding of non-conformance due to reference to non-public material is supported via documentation and explained to developer.

17.3.1.5 CONFORMANCE:

Conformance is checked by inspection of conformance package, interviews, and demonstrations.

17.3.1.6.1 NOTE: It is recognized that demonstrations are not written down work products. However, demonstrations are available as an audit mechanism. The basis for demonstrations that are relied upon by the developer in arguing safety (e.g., manufacturer test plans and corresponding results, demonstrations also required for other purposes beyond conformance to this standard) are a documented part of the safety case, including at least demonstration test plan, demonstration success criteria, and documented results of demonstrations conducted before assessment. Assessors may require additional demonstrations (potentially including demonstrations not described in the safety case) to aid in assessing the validity of the safety case. See also Section 17.3.1.

17.3.2 The Independent Assessor shall be acceptably independent and qualified.

17.3.2.1 MANDATORY:

a) A final conformance determination is performed by an Independent Assessor
b) Argument that the Independent Assessor is acceptably independent

1) Clear and unambiguous statement of Independent Assessor relationship to developer organization(s), marketing, suppliers
2) Clear and unambiguous statement of any other potential conflicts of interest that could compromise the independence of the assessment being performed
EXAMPLES: Time-to-market pressure, individual promotions, influencing the public value of the company, substantive ownership in the company

c) Argument that the Independent Assessor is acceptably qualified
1) Technical qualifications sufficient for understanding safety case
2) Sufficient language proficiency in language of safety case
NOTE: Work products might be in languages other than the language of the safety case. Translation services might need to be used in some cases. The need for translation is a relevant factor to consider when arranging an independent assessment.

NOTE: The Independent Assessor can be a team that spans required skill sets

17.3.2.2 REQUIRED:

a) No substantive involvement of Independent Assessor in design, implementation, and/or test of the item being assessed
b) Substantive independence of management chain between the design team and the Independent Assessor
1) Disclosure of any shared corporate governance if Independent Assessor works for a different corporate entity than the team(s) creating the item and work products being assessed.

17.3.2.3 HIGHLY RECOMMENDED:

a) Independent certification/accreditation of Independent Assessor for performing assessments by a third-party accreditation organization
b) No substantive involvement in the creation and/or maintenance of content of the safety case being assessed
NOTE: A permanent change of job responsibilities from design and/or safety case creation to Independent Assessor might be acceptable after a suitable process to ensure objectivity. However, handling such a situation requires care.
c) **Pitfall:** Having an assessor check his/her own work is prone to resulting in a non-independent assessment
d) Assessor(s) are substantively independent of management team responsible for the item being assessed
e) **Pitfall:** Having an assessor's performance review under the control of a manager who is incentivized to ship an item on time is prone to compromising the ability of the assessor to provide an accurate assessment

17.3.2.4 RECOMMENDED:

a) Use of an accredited, qualified external organization with a completely independent management and reporting structure from the organization performing the self-audit.

17.3.2.5 CONFORMANCE:
Conformance is checked by inspection of conformance package, interviews, and demonstrations.

17.3.3 The Independent Assessor shall create an assessment report.

17.3.3.1 MANDATORY:

a) Assessment report in same human language as safety case (argument and goals)
   NOTE: A later translation of the assessment report might be required if used as SEooC evidence in a safety case written in a different language.
b) Independent Assessor report retained in safety case
c) List, in full, any un-remediated discrepancies; if none, so state
d) Record of result of assessment
   1) Scope of assessment
   2) Versioning information of item and corresponding safety case
   3) Whether conformance has been shown
e) Arguments that Independent Assessor is acceptably independent
   1) Identification of Independent Assessor organization
   2) Identification of Independent Assessor personnel
   3) Arguments of sufficient independence to render a substantively unbiased determination of conformance (see also Section 17.3.2).
      NOTE: For external organizations the Independent Assessors will need to provide information to be included in this argument. Personal information and sensitive corporate information should be treated with care. However, claims of sensitive information should not be used to evade the spirit and intent of disclosure of substantive conflicts of interest.
      EXAMPLE: Consider an Independent Assessor with a non-substantive financial relationship with a supplier who is performing an Independent Assessment on that supplier (e.g., owns a few shares of publicly traded stock in that supplier). Personal financial information in a Conflict of Information statement disclosing this potential conflict is unlikely to be called for in the safety case. Rather, acceptable evidence might be that a credible conflict of interest process is in place, and that there is evidence that the relevant company has vetted potential conflicts of interest for the Independent Assessor personnel and organization, with acceptable records kept independent of the safety case.
f) Arguments that Independent Assessor has an acceptably current qualification to perform the assessment

17.3.3.2 REQUIRED:

a) Independent Assessor assessment capability credentials and currency of requalification date, if any
   NOTE: This item will apply if a credentialing program for assessors has been used by the independent assessor

b) Auditable record of which clauses of this standard that have been considered in the assessment
NOTE: This is intended to provide an audit trail for completeness of an assessment activity
c) Versioning information for SEooC safety cases considered in assessment, if any
d) Discrepancies identified, if any, by the assessment and documented resolution status of discrepancies that is one of:
    1) Post-assessment agreement between developer and Independent Assessor that specific discrepancies have been satisfactorily remedied
    2) Post-assessment agreement between developer and Independent Assessor for any specific discrepancies do not have to be remedied for a satisfactory assessment result, if any, with justification
    EXAMPLE: Non-substantive but pervasive typographical error correction has been deferred to next Independent assessment due to high impact on number of safety case elements that need to be modified.

    NOTE: This prompt element permits a finding of conformance despite minor issues so long as they are resolved post-assessment to the Independent Assessor's satisfaction. It also permits performing the majority of an independent assessment even if a few loose ends are known to remain open in the safety case.
    EXAMPLE: The safety case is missing evidence of a particular test that has not been completed at the time of independent assessment. The design team promises the test will be run, but this nonetheless results in a finding of non-conformance because it is a substantive omission from the safety case. However, that finding can be remedied by providing the test results at a later date, potentially resulting in a finding of conformance upon agreement of the independent assessor so long as no other portions of the safety case have changed. If other portions of the safety case have changed in the meantime, a new independent assessment is required, potentially reduced in scope in accordance with an impact analysis.
e) The existence of any discrepancy which the Independent Assessor does not either agree has been remedied or agree does not have to be remedied results in a finding of non-conformance.

17.3.3.3 HIGHLY RECOMMENDED:

a) For un-credentialed Independent Assessors, other evidence indicating completion of a suitable training and qualification process, including periodic requalification and/or refresher training
b) Record on a clause-by-clause basis:
    1) Clause assessment result: {Fully satisfied, Acceptable safety case deviation due to fundamental inapplicability to item, Other acceptable safety case deviation, Partially satisfied (describe), Not satisfied}
    2) Whether assessment result differed from self-audit result, and actions taken to reconcile any differences

3) Safety case version assessed and date of assessment of each clause
NOTE: A safety case version change can result in per-clause reassessments depending upon change impact analysis.

c) A post-resolution version of the assessment report may be prepared which omits discrepancies which the assessor has agreed in writing have been remediated, but does include all un-remediated discrepancies. Such a report provides reasons for a finding of non-conformance.

d) Identification of discrepancies remedied rather than documented as safety case deviations

17.3.3.4 RECOMMENDED:

a) Independent assessor involvement during construction of safety case rather only at end
NOTE: This can provide early detection of gaps or other issues in the safety case.

17.3.3.5 CONFORMANCE:

Conformance is checked by inspection of the conformance argument and safety case. Conformance statement includes an item conformity inspection which fully identifies the item in question. A conformance statement is signed by an officer of the organization producing the item.

17.3.3.6.1 NOTE: It is recognized that it is unreasonable to expect an assessor to catch every instance of non-conformance or unsafe condition. It is important to note that the primary responsibility for safety rests with the developer. Self-audits are a primary line of quality check. Independent Assessors are a check-and-balance on Self-audit quality.

17.3.4 A finding of partial conformance shall only be produced in specifically designated situations.

17.3.4.1 MANDATORY:

a) Finding of partial conformance prohibited except as enumerated in this clause.
NOTE: This is specifically intended to avoid abuse via a finding of “partial conformance” that does not substantively indicate actual conformance with the standard. Similarly, statements that some item “meets the spirit and intent” of this standard or the like are invalid.
NOTE: Full conformance permits safety case deviations for non-mandatory elements.
NOTE: A finding of full conformance can still contain discrepancies so long as they are enumerated in the conformance report. (See Section 17.3.3.)

17.3.4.2 REQUIRED:

a) Any permitted partial conformance subject to:
1) Uses specified required wording as indicated
2) Inclusion in the conformance statement of the list of prompt elements waived (i.e., safety case deviation due to partial conformance)
3) Waived prompt elements limited to prompt elements relevant to the nature of the partial conformance

b) A finding of partial conformance except for road testing evidence is permitted.
    1) Road testing evidence partially incomplete and/or entirely missing
    2) Arguments based upon road testing preliminary and lacking data due to lack of road testing evidence
    3) Road testing plans and related pre-testing materials are included in safety case to maximum degree practicable
    4) Permissible assessment statement is: “Provisionally conformant to UL 4600 pending road testing.”

    NOTE: This is specifically intended to permit a preliminary assessment of conformance to this standard prior to road testing. Such an assessment might be appropriate as a condition of starting road testing.
c) A finding of partial conformance except for cohort operational experience data is permitted.
    1) Cohort operational data evidence partially incomplete and/or entirely missing
    2) Arguments based upon cohort operational experience preliminary due to lack of cohort operational evidence.

       NOTE: This is primarily expected to apply to Sections 15 and 16.
    3) Cohort operational procedures, materials, and other argument and evidence are in safety case to maximum degree practicable
    4) Permissible assessment statement is: “Provisionally conformant to UL 4600 pending deployment.”

    NOTE: This is specifically intended to permit a preliminary assessment of conformance to this standard prior to cohort deployment. Such an assessment might be appropriate as a condition of initiating a cohort deployment. It would be expected that once cohort deployment has been completed (e.g., deployment of few first cohort vehicles) that data would be fed back into the safety case, with an independent assessment evaluating non-provisional conformance.

17.3.3.3 HIGHLY RECOMMENDED – N/A

17.3.3.4 RECOMMENDED – N/A

17.3.3.5 CONFORMANCE:

Conformance is checked by inspection of the conformance report.

17.4 Conformance monitoring

17.4.1 The safety case shall include a conformance monitoring plan.

17.4.1.1 MANDATORY:

a) Documentation for plan and procedures for continual conformance monitoring and accumulation of evidence of conformance monitoring

17.4.1.2 REQUIRED:

a) Effective execution of conformance monitoring plan.
b) Implementing and updating a repository for evidence of conformance monitoring, encompassing recording at least all of the following items:
    1) Potential, actual, and/or suspected violations of assumptions during all lifecycle phases
    2) Activations of hazards that correspond to “accepted” risks
    3) Evidence supporting quantification of and/or identification of “unknowns”
    4) Documentation supporting determinations that some event or condition placed into the evidence repository was not safety related
        i) Items placed into the repository are not deleted due to a determination of non-safety relevance
    5) Scope includes third party components and legacy components
    6) Periodic re-evaluation of assumptions, accepted risks, and unknown unacceptable risk mitigation, including evaluation of potential accumulation of evidence contradicting historical findings that events or conditions were not safety related and/or were not indicative of a safety related item, process, or safety case issue. (Outcomes of all such re-evaluations to be documented and retained.)
c) Records of item and process improvements
    1) Root cause analysis with traceability of each root cause to potentially affected elements of the safety case including tracking to resolution
    2) Updates, corrections, and other changes to the safety case since the previous conformance assessment.

17.4.1.3 HIGHLY RECOMMENDED – N/A

17.4.1.4 RECOMMENDED – N/A

17.4.1.5 CONFORMANCE:

Conformance is checked by inspection of the safety case and conformance plan.

17.4.1.6.1 NOTE: It is expected that conformance monitoring will be subject to version control and configuration management as part of the safety case.

17.4.2 Conformance shall be re-evaluated on an ongoing basis.

17.4.2.1 MANDATORY:

a) Definition of types and sizes of changes that trigger a need for a revision to the safety case, including at least factors based on:
    1) Change or accumulation of evidence including design evidence, testing evidence, and/or field failure reports
    2) Occurrence of events that potentially invalidate the safety case
    EXAMPLE: Assumption violations
    3) Change to item requirements, design, or implementation

4) Change of definition, expansion, or contraction of ODD
5) Change of conditions, including previously unobserved conditions, within existing ODD

b) Definition of types and sizes of changes that trigger the need for an independent assessment, including at least factors based on:
   1) Changes to safety case
   2) Requirements imposed by assessors, including time limits for conformance validity
      EXAMPLE: Reassessment required after a predetermined number of calendar months if no other event has triggered a reassessment
   3) **Pitfall:** An accumulation of “small” changes is prone over time to significantly affecting item safety.
      NOTE: This is a motivation for periodic independent assessments even if there has been no major change that would otherwise trigger an independent assessment.
   4) Reassessment timeliness criteria, including support for potential urgent “hot fix” updates pending reassessment.

c) Conformance re-evaluation to address goal and argument sufficiency (see Section 5.3).

17.4.2.2 REQUIRED:

a) All changes to the safety case trigger an update to the conformance package
   1) Validity of the conformance package (including coverage and correctness) reevaluated after each change (self-audit, potentially of limited scope)

b) Items that have been marked as “accepted risk” or undergoing only partial risk mitigation based on assumptions or other limited evidence revisited after each occurrence of a violation of the assumption or risk accepted.
   1) No incident, mishap, or potential occurrence of an unmitigated risk dismissed solely based upon a statement that it is the first such occurrence, nor upon a subjective statement that the report is not “credible” or otherwise discounted

c) An assessor-set policy for periodic, event-based, and situational triggers for reassessment.
   1) Those policies are included or added to in the conformance plan at the time of assessment, and apply to the conformance package going forward unless explicitly waived or altered by the assessor.

d) **Pitfall:** Arguing that changes are “too small” to require a safety case change and/or “too small” to require a safety case reassessment is prone to missing superficially “small” changes that nonetheless substantively affect safety.

e) Items that are argued to be “Not applicable” and items that are “accepted” risks based on an argument of limited scale deployment revisited when deployment size is substantively increased, even if no change whatsoever has been made to the item design and implementation.
   NOTE: A substantive increase accomplished gradually over an extended period of time

is nonetheless a substantive increase if the change in scale materially affects the acceptability of assumptions or any other factors involved in the safety case.

f) Any change to a SEooC safety case that affects its component interface reported to all users of that SEooC component interface.
NOTE: This is intended to impose a burden of communicating changes of SEooC safety cases to all active users of that SEooC. Each version of a SEooC that is in use maintains an up to date safety case that is shared with users of that SEooC.

17.4.2.3 HIGHLY RECOMMENDED:

a) **Pitfall:** Deferring update and self-audit of the safety case until the next independent assessment is prone to missing novel risks and safety case defects.

17.4.2.4 RECOMMENDED:

a) Limited scope of re-assessment of conformance package for “small” changes using impact analysis and defined threshold criteria for complete reassessment.
    1) Can be applied to self-audits
    2) Can be applied to independent assessment according to criteria accepted at the most recent assessment (i.e., “small change” criteria must be approved in a previous assessment and cannot be altered without concurrence of assessor)

17.4.2.5 CONFORMANCE:

Conformance is checked by inspection of the safety case and conformance plan.

17.4.2.6.1 NOTE: Self-audit of the conformance package and independent reassessment of multiple changes can be batched within reason, recognizing that the latency after the change represents a potential unmitigated hazard window. Batching policies for reassessments are at the discretion of the assessor, but latency does not exceed any mandated periodic reassessment.

17.4.2.6.2 NOTE: It is understood that at the time of an assessment there might be a comparatively small number of outstanding changes that are still in the process of propagating to safety case updates. That number should be small and a description of the in-progress changes disclosed. Such action items are closed out before a final finding of conformance can be made.

17.4.2.6.3 NOTE: Accepted risks can correspond to events that will occur in operation, but that are low enough in severity and/or frequency that leaving those risks unmitigated is acceptable. A primary goal of this clause is to ensure that evidence is accumulated over time that either supports or rejects the acceptance of a particular risk without biasing that data collection to discount or disregard reports of events that should serve to call into question the acceptance of a particular risk.

17.4.2.6.4 NOTE: This clause explicitly applies to SEooC safety cases as well as item safety cases.

17.5 Prompt element feedback

17.5.1 The safety case shall record customizations and elaborations to prompt element lists relevant to the item and its ODD.

17.5.1.1 MANDATORY – N/A

17.5.1.2 REQUIRED:

a) Deletion and/or modification of prompt elements included in this standard is prohibited other than via the official standard update process.
NOTE: Safety case deviations can be made according to the safety case deviation policy associated with a prompt element.

b) Identification of prompt elements in use in a safety case that do not trace to prompt elements identified in this standard.
NOTE: These are prompt elements that do not trace to a prompt element in this standard. If none, then identification as “none” required. Traceability can be satisfied by tracing these added prompt elements to a category linked to this prompt element.

c) Addition of prompt elements to locally maintained prompt element lists if necessary to complete the safety case.

17.5.1.3 HIGHLY RECOMMENDED:

a) Creation of prompt element-subtype lists used in the safety case
NOTE: This can include enumeration of items that are given as examples for specific prompt elements. Enumerating such example lists can help avoid omissive errors in analysis of safety case changes or item changes.

17.5.1.4 RECOMMENDED:

a) Notification of stakeholders of prompt element added in response to an incident or other field feedback.
EXAMPLE: A contributing factor to an incident was a novel hat style causing perception classification failure, and inclusion of hat style is (hypothetically) not readily apparent in the current version standard prompt lists. This discovery of an omission in the standard that has been empirically shown to be relevant to safety should be shared with stakeholders on an urgent basis to avoid other operators suffering a similar loss event.
NOTE: It is hoped that a mechanism to support urgent sharing of lessons learned from incidents will be created, but it is outside of the scope of this standard to specify such a mechanism.

17.5.1.5 CONFORMANCE:

Conformance is checked via inspection of design and V&V evidence.

17.5.2 Independent assessors shall propose candidate prompt elements for revising this standard.

17.5.2.1 MANDATORY – N/A

17.5.2.2 REQUIRED:

a) Based on independent assessment experience, propose prompt elements as feedback to the UL 4600 Standards development and maintenance process as defined by Underwriters Laboratories.

b) Propose for discussion with the Standards Technical Panel (STP) for UL 4600 any prompt element omissions and/or other prompt element opportunities for improvement that were a potentially contributing cause to life critical and/or severe injury incidents and/or loss events identified in historical data when performing independent assessment.
NOTE: There are potential confidentiality issues, but this nonetheless remains a requirement to ensure that the standard captures critical lessons learned over time. Independent assessors will need to ensure non-disclosure agreements (if applicable) permit this flow of information back into the standard. It is the intent that feedback at the level of prompt elements will minimize flow of competitor-sensitive information as the result of an independent assessment.

c) Proposal of prompt element suggestions to be performed in a timely manner.
NOTE: At a minimum, each independent assessor reports prompt element suggestions/proposals when polled as part of the process of performing a standard revision cycle.

d) Document prompt element suggestions from independent assessment:
    1) Prompt element suggestion contents
    2) Approval status for release to standards organization
    3) Dates of suggestion, approval, release to standards organization

17.5.2.3 HIGHLY RECOMMENDED:

a) Anonymization of sources of prompt element feedback consistent with reasonable timeliness and actual improvement of this standard in response to lessons learned.

17.5.2.4 RECOMMENDED – N/A

17.5.2.5 CONFORMANCE:

Conformance is checked via inspection of safety case and prompt element release records.

Annex A (Informative) – Use with ISO 26262 and ISO/PAS 21448

A.1 Compatibility

A.1.1 It is the intent of UL 4600 to be compatible with existing relevant safety standards to the maximum extent practicable. In particular in this version of UL 4600, compatibility with ISO 26262:2018 and ISO/PAS 21448:2019 has been considered. This appendix provides non-normative guidance for combining use of those two standards with UL 4600. This guidance is non-exhaustive, but is intended to point out significant areas in which the standards potentially interact with each other.

A.2 Safety Case

A.2.1 A safety case is required by ISO 26262-2:2018 clause 6.4.8. Evaluation of the safety case is discussed by ISO 26262-2:2018 clause C.10.

A.2.2 UL 4600 goes into significantly more detail than ISO 26262-2:2018 about the safety case contents and evaluation method. All things being equal, a comprehensive safety case that meets UL 4600 requirements should also meet ISO 26262-2:2018 requirements. However, there are some Pitfalls presented when attempting to take an existing ISO 26262:2018 compliant safety case and attempting to claim credit for UL 4600 conformance.

A.2.3 **Pitfall:** Tailoring of the safety plan according to ISO 26262-2:2018 clause 6.4.5 could potentially result in a shortfall of evidence mandated or required for conformance to UL 4600.

A.2.4 **Pitfall:** Safety case coverage that is non-normative in ISO 26262:2018 or ISO/PAS 21448:2019 but mandatory or required by UL 4600 might be missed if not explicitly identified as having been considered in conformance assessment.

A.2.5 **Known Incompatibilities:** No clauses in UL 4600 force non-conformance to ISO 26262:2018 nor ISO/PAS 21448:2019.

A.2.6 **NOTE:** Conformance to ISO 26262:2018 does not relieve the need to conform to all relevant elements of UL 4600. However, it would be reasonable for a safety case contain a mapping onto ISO 26262:2018 for appropriate elements and adopt an argument strategy that specific elements are in fact covered by ISO 26262:2018 conformance. A similar strategy could be appropriate for mapping onto other safety standards as well, including ISO/PAS 21448:2019.

A.3 Clause Mapping to ISO 26262:2018

A.3.1 Table A.1 shows a mapping of UL 4600 clauses onto ISO 26262:2018. Credit can be taken for established ISO 26262:2018 conformance with respect to this mapping so long as the scope of the UL 4600 safety argument matches the scope considered in ISO 26262:2018 conformance assessment.

A.3.2 **EXAMPLE:** ISO 26262:2018 conformance is assessed with respect to a safety plan, which defines work products. Those work products “and those needed to reproduce the items and elements” are also placed under configuration management (ISO 26262-8:2018 clause 7.4.3). Consider an item in which a trained neural network is used for perception, with the results of that training (e.g., fixed neural network weights) stored in a database as calibration and configuration data. Depending upon interpretation, the neural network can be reproduced in the sense of creating a new item image just based on the database information, and thus only that database might be placed under configuration management for purposes of ISO 26262:2018 conformance, but not the training data and training toolchain. However, after training it might be discovered that UL 4600 arguments must rely in part upon the quality and provenance of the training data, necessitating that training material be placed under configuration management because it is safety related (i.e., depended upon by the safety argument) even though strictly speaking it is not required to recreate the production software build image. Thus, it is important for the scope of the safety plan assessed under ISO 26262:2018 to match the scope of the UL 4600 argument. (In practice, this hypothetical situation might necessitate re-assessment of ISO 26262:2018 conformance to a larger configuration management scope if the initial ISO 26262:2018 component assessment had previously not included this additional scope.)

A.3.3 Table A.1 is a non-exhaustive list of some clauses in UL 4600 that are suitable for mapping onto ISO 26262:2018. The last column notes that the ISO 26262:2108 safety plan must include the stated work products or otherwise include scope described in that column to provide sufficient evidence for UL 4600 assessment. (Note that some elements included in that column are non-mandatory, so the normal safety case deviation rules for UL 4600 still apply.)

Table A.1
UL 4600 Clauses Mapped to ISO 26262:2018

UL 4600 Clause	Topic	ISO 26262:2018 Clause	Defined ISO 26262:2018 safety plan work product and other notes
5.1.1.3	Configuration management	ISO 26262-8:2018 Clause 7	Safety case

8.5.2.2(c)(3)	Configuration management	ISO 26262-8:2018 Clause 7	All work tools and data identified in UL 4600 8.5.2.2(c)(3), including machine learning training data, testing data, data collection tools, training tools, data management and storage tools. If safety related: ODD coverage tools, performance metric tools, statistical analysis tools, test plans, test results, other work products.
9.1.4.1(c)	Configuration management	ISO 26262-8:2018 Clause 7	UL 4600 additionally requires evaluation of configuration management effectiveness.
14.3.2.1(a)	Configuration management	ISO 26262-8:2018 Clause 7	Nothing additional
14.3.4.3(b)	Configuration management	ISO 26262-8:2018 Clause 7	Training and validation data
14.3.4.3(c)	Configuration management	ISO 26262-8:2018 Clause 7	Per-unit calibration data
14.3.4.3(d)	Configuration management	ISO 26262-8:2018 Clause 7	On-line data sources used for validation
14.3.4.3(e)	Configuration management	ISO 26262-8:2018 Clause 7	Manufacturing process software and/or firmware
14.3.4.4	Configuration management	ISO 26262-8:2018 Clause 7	Component supplier builds and configuration information
16.3.1.2(a)(5)	Configuration management	ISO 26262-8:2018 Clause 7	Traceability from SPI to configuration identifier
17.2.1.2	Configuration management	ISO 26262-8:2018 Clause 7	Conformance package, including retention of all conformance packages applicable to the life of each deployed item instance
8.3.7	Sensor Faults	ISO 26262-5:2018	Coverage of sensor faults listed in Section 6.2.4
13.1	Tools General	ISO 26262-8:2018 Clause 11	Tools that support activities and tasks required by UL 4600, even if not required by ISO 26262 (see ISO

			26262-8:2018 clause 11.1(b), which otherwise limits applicability of tool qualification). Arguments justifying Tool Confidence Levels selected.
13.2	Tool identification	ISO 26262-8:2018 Clause 11	Same as in 13.1 above
13.3	Tool risk mitigation	ISO 26262-8:2018 Clause 11	Same as in 13.1 above
13.4	COTS	ISO 26262-8:2018 Clauses 12 and 13	Same as in 13.1 above

A.3.4 NOTE: ISO 26262-8:2018 clause 7.1 incorporates version management into the term configuration management. Thus “configuration management” in ISO 26262:2018 generally corresponds to the term “configuration management and version control” in UL 4600.

A.4 Clause Mapping to ISO/PAS 21448:2019

A.4.1 Currently no mapping has been identified between UL 4600 and ISO/PAS 21448:2019. The below table is a placeholder.

Table A.2
UL 4600 Clauses Mapped to ISO 21448:2019

UL 4600 Clause	**Topic**	**ISO 21448:2019 Clause**	**Defined ISO 21448:2019 safety plan work product**