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 **RECOMMENDED – 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 elements, 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

See also Section 13.4.

4) Remote software functionality, if used

EXAMPLES: Infrastructure data sources, other-item data sources, teleoperation systems

5) On-line services, if used

EXAMPLES: Cloud-based map data, weather report feeds

e) Quality of safety related elements 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.

See also 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-element 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 validated) 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 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) Degrading 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.

NOTE: The concept of a "Minimal Risk Condition" corresponds to defining one or more operational modes according to this clause.

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

EXAMPLES: Vehicle delivery, being towed, ferry ride

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

NOTE: The redundancy approach might be that no redundancy is required.

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 element 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: