Recommended Safety Assurance Program for Electronic/Software Based Products Used in Safety-Critical (Vital) Applications

Revised 2025 (13 Pages)

A. Purpose

This Manual Part recommends a safety assurance program for electronic/software based products used in safety-critical (vital) applications that is designed to ensure their safety throughout their lifecycle.

B. General

1. The safety assurance program described in this Manual Part should be considered a guideline to manufacturers and railroads involved in the development, manufacturing and utilization of electronic/software based products in safety-critical (vital) applications.

   These guidelines exclude end-user developed application software (e.g. interlocking Boolean equations).

   The following Manual Parts provide additional detail related to a safety assurance program.

   a. a. Manual Part 17.3.3 Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications.

   b. Manual Part 17.3.5 Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications.

2. The safety assurance program described in this Manual Part should support the achievement of applicable requirements of subparts H and I of 49 CFR Part 236, Standards for Processor-Based Signal and Train Control Systems and Positive Train Control Systems, respectively.

3. Top level safety goals include:

   a. The product shall operate safely under normal operating conditions.

   b. The product shall operate safely under adverse operating conditions (environmental, operating stress).

   c. The product shall operate safely, or maintain a safe state, under all credible failure conditions.

4. A fundamental requirement for electronic/software-based products used in safety-critical (vital) applications and systems is that the design

requirements shall be verified and the operation shall be validated for safety prior to acceptance.

C. **Product Design Considerations**

1. 1. Product design should take into account expected use and reasonably foreseeable misuse of the equipment to mitigate hazards.

2. Product design should consider the safety of installer, maintainer and user.

3. Product design should consider the applicable portions of established industry practices or standards as promulgated through appropriate standard-making bodies. These standards include:

   a. IEEE Standard 1483-2000 Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

   b. IEEE Standard 1474.1-2004 Section 5.3.3 (IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements).

   c. MIL-STD-882E Department of Defense Standard Practice: System Safety.

   d. European Committee for Electrotechnical Standardization (CENELEC). EN50126: Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

   e. European Committee for Electrotechnical Standardization (CENELEC). EN 50129: Railway Applications, Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling.

   f. European Committee for Electrotechnical Standardization (CENELEC). EN 50128: Railway Applications, Communication, Signalling and Processing Systems: Software for Railway Control and Protection Systems.

4. Provisions should be made for periodic functional checks of safety devices and features incorporated into the product.

5. Warning and caution notes should be provided in installation, maintenance, and repair instructions.

6. Distinctive warning markings should be provided on any hazardous components that may affect personnel safety.

7. The product shall conform to the environmental limits of Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Signal Systems, and Manual Part 11.5.2 Recommended Electromagnetic Compatibility Immunity and Emissions Testing for Signaling Products. Consideration should be given to ensuring that the product does not fail in an unsafe manner when these limits are exceeded.

8. Adjustable components should be located so that exposure to hazards by installation, maintenance and operating personnel is minimized.

9. Ergonomic engineering (user-friendly) factors should be taken into account in the design of the product.

10. Fusing and grounding shall conform to Manual Part 11.1.1 Recommended Functional Operating Guidelines for Electrical Safety.

11. Design shall make reasonable provisions to mitigate unsafe failures arising from procedural error, neglect, and vandalism.

12. Product design shall be such that failures that cause unacceptable or undesirable hazards are eliminated by design. Failures that are non-self-revealing shall not cause unacceptable or undesirable hazards, even in combination with subsequent failures.

13. For signal and train control applications, the safe state is defined as causing a more restrictive aspect to be displayed, trains to stop, a speed limit known to be safe to be imposed, or a specific sequence of operations known to be safe to be followed.

14. Provisions shall be made to ensure that common-cause failures do not result in an unsafe condition.

15. Electronic/software based products purchased from a third party, which have an effect on safety, are subject to the safety considerations discussed in this Manual Part. The analysis can either be provided by the third party (in line with these recommended practices) or performed by the purchaser.

16. The following characteristics of processor-based systems are widely accepted as necessary to achieve systems that provide a level of safety at least as great as previous generation systems. Deviation from these characteristics needs to be specifically addressed in a safety analysis. Further information on these attributes can be found in:

    Leveson, N.G. (1995). *Safeware: System Safety and Computers.* Reading, Massachusetts: Addison-Wesley Publishing Company.

    Storey, N. (1996). *SAFETY-CRITICAL Computer Systems*. Reading, Massachusetts: Addison-Wesley Publishing Company.

a. Simplicity is a critical aspect for any safety-critical design. Simplicity allows a more complete understanding of the system operation minimizing the chances for error. Simplicity also minimizes the number of interfaces with other systems, making the designs easier to test and reducing another common source of error. Drastically reducing the number of functions performed by the safety-critical system (and enforcing this reduction) also keeps function creep under control and allows future changes to be made and verified.

Complex software systems are easier to build than simple ones. For example, use of an operating system makes the design simpler but adds complexity, thereby making it more difficult to be analyzed. If an operating system is used, the safety analysis must identify how safety is not affected.

b. Deterministic software is a major advantage in processor-based systems used for safety-critical applications. Since communication among all the components is known at design time, the system can be designed without the need for complex inter-process communications that would normally be provided by an operating system or dynamic memory management. Leveson identifies four underlying requirements for deterministic systems:

(1) First, there is a need for strict time controls. Many of the required functions need to be repeated on a periodic basis.

(2) Secondly, there is a need for analyzing algorithm behavior with the ability to consistently predict how it will behave in the future.

(3) Thirdly, an ability to test software and obtain consistently repeatable results (e.g., not dependent on random timing) is needed.

(4) Finally, deterministic behavior is necessary to provide the human interface in such a way that the displayed information is consistent in a variety of situations. This need for deterministic operation highlights that a simple, deterministic system can be more difficult to design and develop than a complex system.

c. Separation of safety-critical functions from the non-safety-critical functions is an essential characteristic of safety-critical systems. This reduces the complexity and coupling of the safety-critical system allowing it to be implemented with a much higher degree of confidence. In addition, the separation allows the safety analysis to be performed on a manageable portion of the system. The complexity of a system grows exponentially as the number of its functions increase. In such cases, separation of safety-critical from non-safety-critical functions becomes more critical in order to achieve practical systems.

d. Decoupling is another attribute desirable in developing a safety-critical design. This ensures that one component will not affect the operation of another component. Tightly coupled systems substantially increase the risk of faults due to unintended interrelationships between components. Once again, tightly coupled systems are typically more efficient and require less design effort than loosely coupled systems. However, the interdependence of these tightly coupled components adds new hazards to the safety-critical system.

17. The product design shall require positive actions to be taken in a prescribed manner to either begin its operation or continue its operation (closed loop principle).

D. <u>Safety Assurance Program</u>

1. The objective of a Safety Assurance Program is to provide proof-of-safety of electronic/software-based products being developed for safety-critical (vital) applications. An integrated approach should be followed to meet this objective.

2. The integrated approach should consist of three programs:

a. Quality Management

b. Safety Management

c. Safety Verification & Validation (V&V)

3. Quality Management

A Quality System conforming to Manual Part 17.2.1 Recommended Quality Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications should be followed.

4. Safety Management

A safety management program should be in place throughout the lifecycle of electronic/software-based products used in safety-critical (vital) applications. This program should consist of the following steps, in the order listed:

a. Safety Organization

(1) A safety organization should be in place or set up prior to the start of the development of the product or system.

(2) The objective of the safety organization is to manage the overall safety assurance program.

(3) The safety organization should preferably be independent of the design function and should have the ability to determine the completeness and correctness of the safety activities.

(4) The final release of a new vital system should require the approval of the safety organization.

(5) An effective safety organization should clearly identify its management structure, and specific responsibilities and roles of the safety assurance personnel within the organization.

b. Safety Program Plan

(1) The objective of the Safety Program Plan is to provide a structured approach to planning and implementing the safety assurance program. It should identify the safety organization, safety assurance activities, and safety-related documentation needs of the system under consideration.

(2) A V&V Plan should be an integral part of the Safety Program Plan.

c. Preliminary Hazard List

(1) A Preliminary Hazard List (PHL) should be compiled very early in the product/system acquisition lifecycle to identify potentially hazardous areas on which to put management emphasis.

(2) Safety experience on similar product/systems, including mishap/incident hazard tracking logs if available, safety lessons learned, etc., should be used in preparing the PHL.

(3) See Manual Part 17.3.5 Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications for additional supporting information.

d. Preliminary Hazard Analysis

(1) The Preliminary Hazard Analysis (PHA) should be conducted during the early stages of the development.

(2) The objective of the PHA is to analyze the potential hazards from the PHL and other sources, and the associated risks so that safety concerns can be addressed early and the design can be appropriately directed.

(3) A Hazard Log should be used as a reference to track the resolution of the identified hazards as the system development progresses.

(4) See Manual Part 17.3.5 Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications for additional supporting information.

e. Product Safety Requirements

(1) The objective of this step is to identify the overall safety requirements for the product, based on the overall functional requirements, user requirements, and safety concerns of electronic/software-based products in general.

(2) The PHA should be used as a guide in preparing the Product Safety Requirements (PSR). The PSR should be revised as new hazards are identified and the detailed hazard analyses are performed.

f. Safety Requirements Allocation

The objective of this step is to allocate the safety requirements to hardware and software based upon the PSR and architectural design decisions, including the overall safety design philosophy that is being followed for the product.

g. Detailed Hazard Analyses

(1) Detailed hazard analyses such as Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), Operating & Support Hazard Analysis (O&SHA), Fault Tree Analyses (FTA), Functional Fault Trees (FFT) and Failure Modes and Effects Analysis (FMEA) should be conducted on the product as the design progresses.

(2) The objective of these analyses is to help identify various hazards and their associated risks, and the possible means of eliminating the hazards or reducing their risks to acceptable levels. The analyses also help identify the V&V requirements and provide a measure of the completeness of the V&V activities.

h. Safety Verification & Validation

The objective of this key element of the Safety Management program is to demonstrate compliance with all safety requirements and to provide a final proof-of-safety of the product. Refer to Section E below.

i. Safety Assurance During the Lifecycle

During the lifecycle of the product, the Safety Management process shall ensure that safety is not affected by hardware, software and other product-related modifications subsequent to release of the product.

j. Safety and Design Reviews

(1) In addition to the preceding steps, safety reviews should be an integral part of design reviews and of the Safety Management process. Results of qualitative and quantitative assessment of the design should be reviewed and recorded to determine if the established safety allocation goals have been achieved. Safety reviews should be conducted throughout the product lifecycle.

(2) The objective is to ensure that critical safety activities are carried out at their appropriate times, and that safety issues are resolved in a timely manner.

(3) The Hazard Log should be used to record and track the resolution of the hazards identified in the PHA, the detailed hazard analyses, and during the product lifecycle.

E. <u>Safety Verification & Validation</u>

1. The Safety Verification and Validation process is a key part of the Safety Management process and therefore has been addressed separately.

2. The objective of the Safety V&V activity is to verify and validate the safety requirements.

3. The Safety V&V process should consist of the following activities:

Safety V&V Planning

Product Safety Requirements Verification

Hardware Safety Verification and Validation

Software Safety Verification and Validation

Product Safety Validation (following Hardware/Software Integration)

Safety V&V of Modifications

The above Safety V&V activities and their relationship to a typical product development cycle are shown in Figure 1731-1 and are elaborated on below.

a. Safety V&V Planning

(1) In the early stages of the product development and as an integral part of the Safety Program Plan, the Safety V&V activities should be planned. A sub-plan should be prepared for each of the Safety V&V activities identified in Figure 1731-1.

(2) A Safety V&V Plan should be created as part of the Safety Program Plan described in Section D.4.b or as a separate document. This plan should address the verification that each phase of the lifecycle satisfies the specific safety requirements identified in the previous phase, and the validation of the completed product or system/subsystem against its original safety requirements.

(3) These activities should be fully documented, including appropriate testing and safety analyses. They should be repeated as appropriate in the event of any subsequent modification or addition to the product or system/subsystem.

(4) In some cases, it might be beneficial to have independence between the personnel performing the verification and validation, particularly when higher levels of safety are required.

b. Product Safety Requirements - Verification

This activity verifies that the PSR accurately reflects all of the product safety requirements as dictated by the user and/or the intended application of the product. The PSR should be reviewed for correctness, completeness, unambiguity, and consistency, and should be done per a Product Safety Requirements Verification Plan.

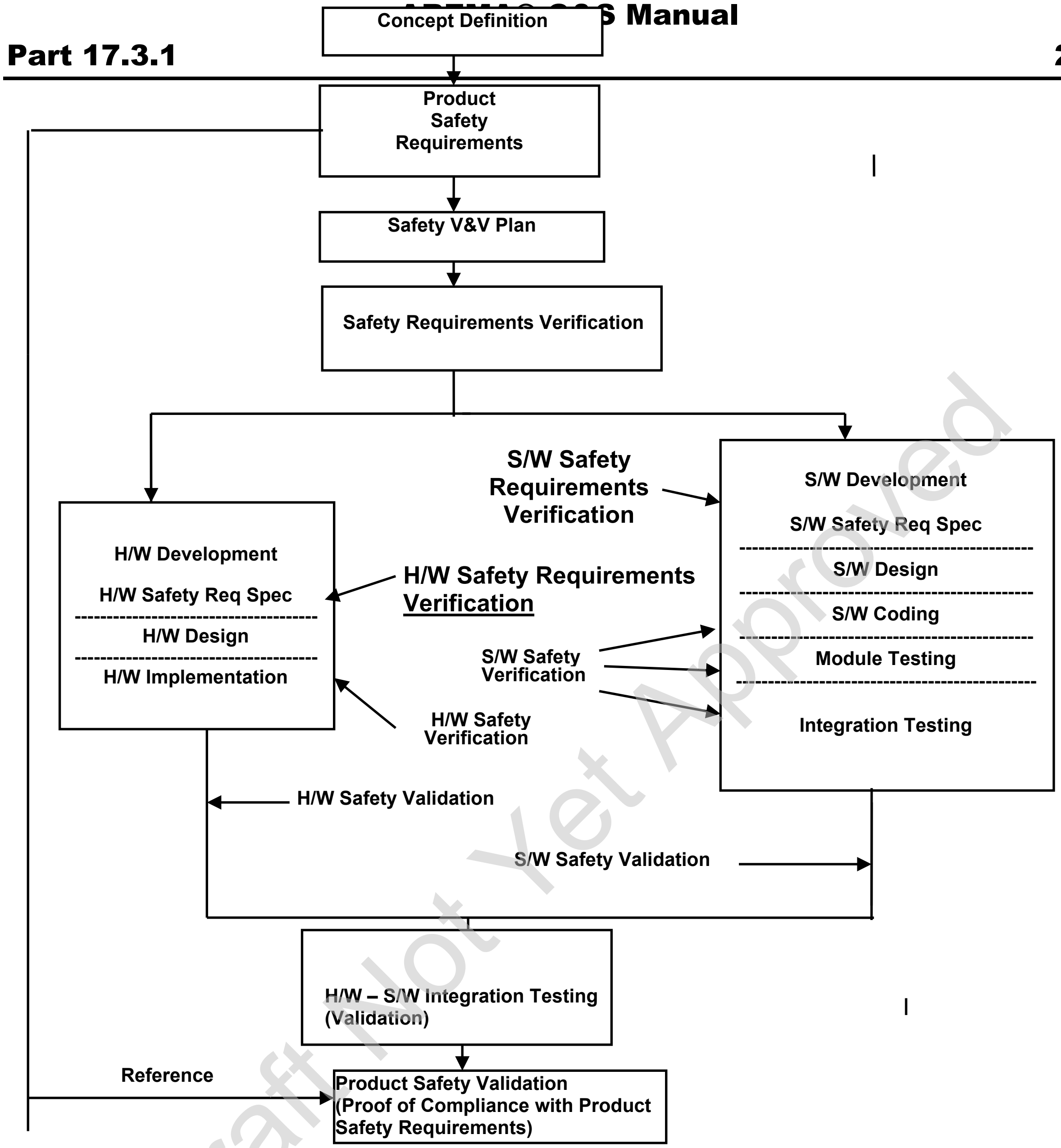

Figure 1731-1: Safety V&V Activities During Product Development Cycle

c. Hardware Safety Verification and Validation

These activities should include:

(1) Hardware safety requirements allocation verification to ensure that the allocations accurately reflect the safety-critical and safety-related hardware requirements, that human error has not occurred, that there are no omissions or commissions, and that the allocations are complete, correct, unambiguous and properly mapped to the Product Safety Requirements specification. (Verification that hardware safety allocations are complete and correct.)

(2) Hardware design verification to demonstrate safe operation of the hardware under normal operating conditions as well as under single point and non-self-revealing fault conditions in hardware that does not rely on software for safety. Verify that the design meets its safety requirements.

(3) Hardware implementation verification to demonstrate that hardware implementation correctly and accurately reflects the hardware design. Verify that the hardware is built as designed.

(4) See Manual Part 17.3.3 Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications for additional supporting information.

d. Software Safety Verification and Validation

This activity should include:

(1) Software safety requirements allocation verification to ensure that the allocations accurately reflect the safety-critical and safety-related software requirements, that human error has not occurred, that there are no omissions or commissions, and that the allocations are complete, correct, unambiguous and properly map to the Product Safety Requirements specification. (Verification that software safety allocations are complete and correct.)

(2) Software design verification to demonstrate that the design (and design specifications) correctly reflects the safety requirements, and that human error has not occurred during the design process (design of incorrect safety function, failing to design a safety function, and/or designing a safety function

incorrectly). Verify that the design meets its safety requirements.

(3) Software code verification to demonstrate that the code correctly reflects the safety requirements and that human error has not occurred during the coding process (coding of incorrect safety function, failing to code a safety function, and/or coding a safety function incorrectly).

(4) Software module testing to demonstrate that each software module performs its intended safety function correctly and does not operate in an unsafe manner. (Verify that the software module is safe as designed.)

(5) Software integration testing to demonstrate that the software modules integrate correctly, by progressively combining the modules into a composite whole and verifying safe interaction between the modules.

e. Product Safety Verification and Validation

This activity should include:

(1) An overall product safety verification and validation that shall be conducted following the integration of all hardware and software, and after all separate hardware and software V&V activities have been completed. The purpose is to verify compliance with the PSR and validate that the product is "fit for purpose" from a safety viewpoint.

(2) A final product safety description, an overall V&V review, and a final hardware/software integration verification. It should involve demonstrating the safety of hardware portions that were not addressed by the earlier hardware V&V activities. This should include the hardware that relies, at least in part, on software to ensure safe operation.

(3) Testing which demonstrates safe operation of the software and the overall product under normal input conditions (operational profiles), external influences (electrical, mechanical and climatic), and under various hardware fault conditions.

f. Safety V&V During the Lifecycle of Modifications

A safety V&V program shall be provided to include review and V&V of each modification to the product during its lifecycle to ensure that the modifications to the original requirements, design, or implementation do not compromise safety.

F. Risk Assessment

Refer to Manual Part 17.3.5. Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Products Used in Safety-Critical (Vital) Applications.