

# 49 CFR Part 236 Subpart H

Comparison with AREMA MP 17.x.x

## Part 236 Subpart H

- Standards for Processor-Based Signal and Train Control Systems
- Purpose
  - To promote the safe operation of processor-based signal and train control systems, subsystems, and components that are safety-critical products as defined in Section 236.903 and to facilitate the development of those products.

## AREMA MP 17.3.1

- Recommended Safety Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications
- Top level safety goals
  - System shall operate safely under normal conditions
  - System shall operate safely under adverse conditions
  - System shall operate safely or maintain a safe state under all failure conditions
- Fundamental requirement that design requirements be validated and operation verified for safety prior to acceptance

## Part 236 Subpart H

- Abbreviated risk assessment
  - Meets the minimum performance requirements if
    - New MTTHE is greater than or equal to old MTTHE (OR)
    - Probability of hazard is equal to or less than the corresponding recommended rates as classified as more favorable than ‘undesirable’ by AREMA MP 17.3.5 or the Associate Administrator for Safety concurs with the acceptance of hazards classified as ‘undesirable’ (AND)
    - The product is developed in accordance with AREMA MPs (17.3.1, 17.3.3, &17.3.5) and appendix C (AND)
    - The analysis supporting the Product Safety Plan (PSP) suggests no credible reason for believing that the product will be less safe than the previous condition.

# AREMA

- MP 17.3.1
  - Recommended Safety Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications
    - Consistent with the requirements of Appendix C
    - Integrated approach including Quality Management, Safety Management, and Safety V&V
      - » 17.2.1 Recommended Quality Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications

# AREMA

- MP 17.3.1
  - Recommended Safety Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications
    - Safety Management
      - » Safety Organization
      - » Safety Program Plan
      - » Preliminary Hazard List (PHL)
      - » Preliminary Hazard Analysis (PHA)
      - » Product Safety Requirements
      - » Safety Requirement Allocation
      - » Detail Design Analysis
      - » Safety Validation & Verification (V&V)
      - » Safety Assurance during Life-cycle
      - » Safety and Design Reviews

# AREMA

- MP 17.3.1
  - Recommended Safety Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications
    - Safety V&V
      - » Safety V&V Plan
      - » Product Safety Requirements – Validation
      - » Hardware Safety V&V
      - » Software Safety V&V
      - » System Safety V&V
      - » Safety V&V during the life-cycle of modifications

# AREMA

- MP 17.3.3
  - Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Products Used in Signal and Train Control Applications
    - Hardware Design Requirements
      - » Class I Hardware–Vital hardware doing vital functions
      - » Class II Hardware–Non-vital hardware doing vital functions
      - » Class III Hardware–Non-vital hardware doing non-vital functions
    - Analysis of Class I Hardware
    - Analysis of Class II Hardware
    - Analysis of Class III Hardware

# AREMA

- MP 17.3.3
  - Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Products Used in Signal and Train Control Applications
    - Minimum Requirements for the Failure Modes and Effects Criticality Analysis (FMECA) of Vital Hardware
      - » Circuit operational modes not related to component failures (power supply variations, self oscillation, etc.)
      - » Sneak paths
      - » Includes a list of credible component failure modes that need to be considered
      - » Includes a list of special components with accepted ‘non-credible’ failure modes

# AREMA

- MP 17.3.5
  - Recommended Practice for Hazard Identification and Management for Vital Electronic/Software-Based Products Used in Signal and Train Control Applications
    - Product Safety Classes
      - » Safety-critical
      - » Safety-related
      - » Non-safety-related
    - Safety Class Determination
    - Preliminary Hazard Identification
      - » Fault Tree Analysis (FTA)
      - » Systematic failure prevention check list
      - » Brainstorming

# AREMA

- MP 17.3.5
  - Recommended Practice for Hazard Identification and Management for Vital Electronic/Software-Based Products Used in Signal and Train Control Applications
    - Hazard Log
    - Hazard Risk Assessment
      - » Severity
      - » Probability of Occurrence
      - » Risk Categories
    - Hazard Assignment and Completion

## Part 236 Subpart H

- Requirements of Appendix C
  - Address each of the following safety considerations when designing and demonstrating the safety of the products. If any of these principles are not followed, the reasons for departure and the alternatives utilized to mitigate hazards shall be stated.
    - Demonstrate safe operation under normal conditions with no hardware/software failures (AREMA 17.3.1)
    - Absence of specific operator actions or procedures will not prevent the system from operating safely (AREMA 17.3.1)
    - No hazards categorized as unacceptable or undesirable (AREMA 17.1.3)
    - Hazards categorized as unacceptable must be mitigated by design (AREMA 17.1.3)

## Part 236 Subpart H

- Requirements of Appendix C
  - Show how the product is designed to mitigate or eliminate unsafe systematic failures – those conditions which can be attributed to human error that could occur at various stages throughout the product development (AREMA 17.3.1 & 17.3.5).

## Part 236 Subpart H

- Requirements of Appendix C
  - Show product operates safely under conditions of random hardware failure
    - No single point failure resulting in hazards categorized as unacceptable or undesirable. Occurrence of credible single point failures that can result in hazards must be detected and the product must achieve a known safe state before falsely activating any physical appliance (AREMA 17.3.1)
    - Non-self-revealing failures combined with second failures can not cause a hazard categorized as unacceptable or undesirable (AREMA 17.3.1)
    - If a common mode failure exists, then any analysis cannot rely on the assumption that failures are independent. (AREMA 17.3.1)

## Part 236 Subpart H

- Requirements of Appendix C
  - The product must be shown to operate safely when subjected to external influences including electrical interference, mechanical interference (shock, vibration), and climatic conditions (temperature, humidity) (AREMA 17.3.1)
  - Safety must be ensured following modifications to the hardware, software, or both (AREMA 17.3.1)
  - Software faults must not cause hazards categorized as unacceptable or undesirable (AREMA 17.3.1)
  - Product must require positive action to be taken in a prescribed manner to either begin operation or to continue operation (Closed-Loop Principle) (AREMA 17.3.1)

## Part 236 Subpart H

- Requirements of Appendix C
  - Product design must sufficiently incorporate human factor engineering that is appropriate to the complexity of the product; the educational, mental, and physical capabilities of the intended operators and maintainers; the degree of required human interface with the component; and the environment in which the product will be used (Not explicitly cited in AREMA MP. Results of hazard analysis (O&SHA) and selected hazard mitigation techniques would identify HMI issues and requirements.)

## Part 236 Subpart H

- Requirements of Appendix C
  - Acceptable Verification and Validation Standards
    - MIL STD 882C \*
    - IEEE 1483-2000 \*
    - CENELEC – EN50126, EN50128, EN50129, EN50155 \*
    - ATCS Spec 140 and 130
    - AREMA C&S Manual of Recommended Practices, Part 17
    - Safety of High Speed Ground Transportation Systems
    - IEC61508
    - Unpublished standards to the extent that they are shown to achieve the requirements
    - \* - also cited by AREMA MP 17.3.1

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Complete description of the product (Not explicitly required by AREMA)
  - Description of the railroad operation or categories of operation on which the product is designed to be used, including (Not explicitly required by AREMA, however should be identified as part of hazard analyses if pertinent)
    - Train movement density
    - Gross Tonnage
    - Hazardous material volume
    - Railroad operating rules
    - Operating speeds

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - An operational concept document, including a complete description of the product functionality and informational flows (Not explicitly required by AREMA)
  - A safety requirements document including a list with complete description of all functions which the product performs to enhance or preserve safety (AREMA 17.1.3)
  - Description of the manner in which the product architecture satisfies the safety requirements (AREMA 17.1.3)
  - A hazard log (AREMA 17.3.1 & 17.3.5)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Risk assessment (AREMA 17.3.5)
  - Hazard risk mitigation analysis (AREMA 17.3.1 & 17.3.5)
  - Complete description of the safety assurance concepts (AREMA 17.3.5)
  - A human factors analysis including a complete description of all functions performed by humans in connection with the product to enhance or preserve safety and an analysis in accordance with appendix E (HMI Design) or other criteria (Not explicitly required by AREMA – Results of O&SHA identifies human factors issues and mitigations)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - A complete description of the specific training of railroad and contractor employees and supervisors necessary to ensure the safe and proper installation, operation, maintenance, repair, inspection, testing, and modification of the product (Not explicitly required by AREMA – Results of hazard analyses identify training requirements for hazard mitigation)
  - An analysis of the applicability of subparts A through G (Not required by AREMA)
  - Description of necessary security measures (Not explicitly required by AREMA)
  - Description of each warning to be placed in the Operations and Maintenance Manual and of all warning labels to be placed on equipment (AREMA 17.3.1 & 17.3.5)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are mitigated (AREMA 17.3.1)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Description of
    - Post-implementation testing (validation) and maintenance procedures including intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation process, and safety-critical tolerances are not compromised over time, through use, or after maintenance is performed (AREMA 17.3.1)
    - Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspection, tests, repairs, replacements, adjustments, and the system's resulting conditions including records of component failures resulting in safety-relevant hazards (Not explicitly required by AREMA)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Description of any safety-critical assumptions regarding availability of the product and a description of all backup methods of operation (Not explicitly required by AREMA)
  - Description of all incremental and predefined changes (Not explicitly required by AREMA)
  - Identification of configuration/revision control measures (AREMA 17.5.1 & 17.5.3)

## Part 236 Subpart H

- Product Safety Plan (PSP)
  - Specify all contractual arrangements with hardware and software suppliers for immediate notification of any and all safety-critical software upgrades, patches, or revisions. (Not required by AREMA)
  - Specify railroad procedures for action upon notification of a safety-critical upgrade, patch, or revision (Not required by AREMA)

## Conclusions

- AREMA 17.3.1 and the rule have similar safety goals
- AREMA Manual Parts 17.x.x are effective in meeting many of the requirements of the rule
- The PSP requires additional detailed documentation the AREMA does not explicitly require, however most of it would be necessary to complete the AREMA requirements or would be generated (probably in a different form) as the result of the various hazard analyses and the identification of hazard mitigation techniques

# QUESTIONS?