

§ 236.929

49 CFR Ch. II (10–1–07 Edition)

(6) Information needed to prevent unintentional interference with the proper functioning of onboard train control equipment.

(b) *How must locomotive engineer training be conducted?* Training required under this subpart for a locomotive engineer, together with required records, must be integrated into the program of training required by part 240 of this chapter.

(c) *What requirements apply to full automatic operation?* The following special requirements apply in the event a train control system is used to effect full automatic operation of the train:

(1) The PSP must identify all safety hazards to be mitigated by the locomotive engineer.

(2) The PSP must address and describe the training required with provisions for the maintenance of skills proficiency. As a minimum, the training program must:

(i) As described in § 236.923(a)(2), develop failure scenarios which incorporate the safety hazards identified in the PSP, including the return of train operations to a fully manual mode;

(ii) Provide training, consistent with § 236.923(a), for safe train operations under all failure scenarios and identified safety hazards that affect train operations;

(iii) Provide training, consistent with § 236.923(a), for safe train operations under manual control; and

(iv) Consistent with § 236.923(a), ensure maintenance of manual train operating skills by requiring manual starting and stopping of the train for an appropriate number of trips and by one or more of the following methods:

(A) Manual operation of a train for a 4-hour work period;

(B) Simulated manual operation of a train for a minimum of 4 hours in a Type I simulator as required; or

(C) Other means as determined following consultation between the rail-

road and designated representatives of the affected employees and approved by the FRA. The PSP must designate the appropriate frequency when manual operation, starting, and stopping must be conducted, and the appropriate frequency of simulated manual operation.

§ 236.929 Training specific to roadway workers.

(a) *How is training for roadway workers to be coordinated with part 214?* Training required under this subpart for a roadway worker must be integrated into the program of instruction required under part 214, subpart C of this chapter (“Roadway Worker Protection”), consistent with task analysis requirements of § 236.923. This training must provide instruction for roadway workers who provide protection for themselves or roadway work groups.

(b) *What subject areas must roadway worker training include?* (1) Instruction for roadway workers must ensure an understanding of the role of processor-based signal and train control equipment in establishing protection for roadway workers and their equipment.

(2) Instruction for roadway workers must ensure recognition of processor-based signal and train control equipment on the wayside and an understanding of how to avoid interference with its proper functioning.

(3) Instructions concerning the recognition of system failures and the provision of alternative methods of on-track safety in case the train control system fails, including periodic practical exercises or simulations and operational testing under part 217 of this chapter to ensure the continued capability of roadway workers to be free from the danger of being struck by a moving train or other on-track equipment.

APPENDIX A TO PART 236—CIVIL PENALTIES¹

Section	Violation	Willful violation
Subpart A—Rules and Instructions—All Systems		
<i>General:</i>		
236.0 Applicability, minimum requirements	\$2,500	\$5,000

Section	Violation	Willful violation
236.1 Plans, where kept	1,000	2,000
236.2 Grounds	1,000	2,000
236.3 Locking of signal apparatus housings:		
(a) Power interlocking machine cabinet not secured against unauthorized entry	2,500	5,000
(b) other violations	1,000	2,000
236.4 Interference with normal functioning of device	5,000	7,500
236.5 Design of control circuits on closed circuit principle	1,000	2,000
236.6 Hand-operated switch equipped with switch circuit controller	1,000	2,000
236.7 Circuit controller operated by switch-and-lock movement	1,000	2,000
236.8 Operating characteristics of electro-magnetic, electronic, or electrical apparatus	1,000	2,000
236.9 Selection of circuits through indicating or annunciating instruments	1,000	2,000
236.10 Electric locks, force drop type; where required	1,000	2,000
236.11 Adjustment, repair, or replacement of component	2,500	5,000
236.12 Spring switch signal protection; where required	1,000	2,000
236.13 Spring switch; selection of signal control circuits through circuit controller	1,000	2,000
236.14 Spring switch signal protection; requirements	1,000	2,000
236.15 Timetable instructions	1,000	2,000
236.16 Electric lock, main track releasing circuit:		
(a) Electric lock releasing circuit on main track extends into fouling circuit where turnout not equipped with derail at clearance point either pipe-connected to switch or independently locked, electrically	2,500	5,000
(b) other violations	1,000	2,000
236.17 Pipe for operating connections, requirements	1,000	2,000
236.18 Software management control plan:		
Failure to develop and adopt a plan	\$5,000	\$10,000
Failure to fully implement plan	5,000	10,000
Inadequate plan	2,500	10,000
<i>Roadway Signals and Cab Signals—</i>		
236.21 Location of roadway signals	1,000	2,000
236.22 Semaphore signal arm; clearance to other objects	1,000	2,000
236.23 Aspects and indications	1,000	2,000
236.24 Spacing of roadway signals	2,500	5,000
236.26 Buffing device, maintenance	1,000	2,000
<i>Track Circuits—</i>		
236.51 Track circuit requirements:		
(a) Shunt fouling circuit used where permissible speed through turnout greater than 45 m.p.h.	2,500	5,000
(b) Track relay not in de-energized position or device that functions as track relay not in its most restrictive state when train, locomotive, or car occupies any part of track circuit, except fouling section of turnout of hand-operated main-track crossover	2,500	5,000
(c) other violations	1,000	2,000
236.52 Relayed cut-section	1,000	2,000
236.53 Track circuit feed at grade crossing	1,000	2,000
236.54 Minimum length of track circuit	1,000	2,000
236.55 Dead section; maximum length	1,000	2,000
236.56 Shunting sensitivity	2,500	5,000
236.57 Shunt and fouling wires:		
(a) Shunt or fouling wires do not consist of at least two discrete conductors	2,500	5,000
(b) other violations	1,000	2,000
236.58 Turnout, fouling section:		
(a) Rail joint in shunt fouling section not bonded	2,500	5,000
(b) other violations	1,000	2,000
236.59 Insulated rail joints	1,000	2,000
236.60 Switch shunting circuit; use restricted	2,500	5,000
<i>Wires and Cables—</i>		
236.71 Signal wires on pole line and aerial cable	1,000	2,000
236.73 Open-wire transmission line; clearance to other circuits	1,000	2,000
236.74 Protection of insulated wire; splice in underground wire	1,000	2,000
236.76 Tagging of wires and interference of wires or tags with signal apparatus	1,000	2,000
<i>Inspections and Tests; All Systems—</i>		
236.101 Purpose of inspection and tests; removal from service or relay or device failing to meet test requirements	2,500	5,000
236.102 Semaphore or search-light signal mechanism	1,000	2,000
236.103 Switch circuit controller or point detector	1,000	2,000
236.104 Shunt fouling circuit	1,000	2,000
236.105 Electric lock	1,000	2,000
236.106 Relays	1,000	2,000
236.107 Ground tests	1,000	2,000
236.108 Insulation resistance tests, wires in trunking and cables:		
(a) Circuit permitted to function on a conductor having insulation resistance value less than 200,000 ohms	2,500	5,000

Section	Violation	Willful violation
(b) other violations	1,000	2,000
236.109 Time releases, timing relays and timing devices	1,000	2,000
236.110 Results of tests	1,000	2,000
Subpart B—Automatic Block Signal Systems		
236.201 Track circuit control of signals	1,000	2,000
236.202 Signal governing movements over hand-operated switch	1,000	2,000
236.203 Hand-operated crossover between main tracks; protection	1,000	2,000
236.204 Track signaled for movements in both directions, requirements	1,000	2,000
236.205 Signal control circuits; requirements	1,000	2,000
236.206 Battery or power supply with respect to relay; location	1,000	2,000
Subpart C—Interlocking		
236.207 Electric lock on hand-operated switch; control:		
(a) Approach or time locking of electric lock on hand-operated switch can be defeated by unauthorized use of emergency device which is not kept sealed in the non-release position	2,500	5,000
(b) other violations	1,000	2,000
236.301 Where signals shall be provided	1,000	2,000
236.302 Track circuits and route locking	1,000	2,000
236.303 Control circuits for signals, selection through circuit controller operated by switch points or by switch locking mechanism	1,000	2,000
236.304 Mechanical locking or same protection effected by circuits	1,000	2,000
236.305 Approach or time locking	1,000	2,000
236.306 Facing point lock or switch-and-lock movement	1,000	2,000
236.307 Indication locking:		
236.308 Mechanical or electric locking or electric circuits; requisites	1,000	2,000
236.309 Loss of shunt protection; where required:		
(a) Loss of shunt of five seconds or less permits release of route locking of power-operated switch, movable point frog, or derail	2,500	5,000
(b) Other violations	1,000	2,000
236.310 Signal governing approach to home signal	1,000	2,000
236.311 Signal control circuits, selection through track relays or devices functioning as track relays and through signal mechanism contacts and time releases at automatic interlocking	1,000	2,000
236.312 Movable bridge, interlocking of signal appliances with bridge devices:		
(a) Emergency bypass switch or device not locked or sealed	2,500	5,000
(b) other violations	1,000	2,000
236.314 Electric lock for hand-operated switch or derail:		
(a) Approach or time locking of electric lock at hand-operated switch or derail can be defeated by unauthorized use of emergency device which is not kept sealed in non-release position	2,500	5,000
(b) other violations	1,000	2,000
<i>Rules and Instructions—</i>		
236.326 Mechanical locking removed or disarranged; requirement for permitting train movements through interlocking	1,000	2,000
236.327 Switch, movable-point frog or split-point derail	1,000	2,000
236.328 Plunger of facing-point	1,000	2,000
236.329 Bolt lock	1,000	2,000
236.330 Locking dog of switch and lock movement	1,000	2,000
236.334 Point detector	1,000	2,000
236.335 Dogs, stops and trunnions of mechanical locking	1,000	2,000
236.336 Locking bed	1,000	2,000
236.337 Locking faces of mechanical locking; fit	1,000	2,000
236.338 Mechanical locking required in accordance with locking sheet and dog chart	1,000	2,000
236.339 Mechanical locking; maintenance requirements	1,000	2,000
236.340 Electromechanical interlocking machine; locking between electrical and mechanical levers	1,000	2,000
236.341 Latch shoes, rocker links, and quadrants	1,000	2,000
236.342 Switch circuit controller	1,000	2,000
<i>Inspection and Tests—</i>		
236.376 Mechanical locking	1,000	2,000
236.377 Approach locking	1,000	2,000
236.378 Time locking	1,000	2,000
236.379 Route locking	1,000	2,000
236.380 Indication locking	1,000	2,000
236.381 Traffic locking	1,000	2,000
236.382 Switch obstruction test	1,000	2,000
236.383 Valve locks, valves, and valve magnets	1,000	2,000

Federal Railroad Administration, DOT

Pt. 236, App. A

Section	Violation	Willful violation
236.384 Cross protection		
236.386 Restoring feature on power switches		
236.387 Movable bridge locking	1,000	2,000

Subpart D—Traffic Control Systems Standards

236.401 Automatic block signal system and interlocking standards applicable to traffic control systems:		
236.402 Signals controlled by track circuits and control operator	1,000	2,000
236.403 Signals at controlled point	1,000	2,000
236.404 Signals at adjacent control points	1,000	2,000
236.405 Track signaled for movements in both directions, change of direction of traffic	1,000	2,000
236.407 Approach or time locking; where required	1,000	2,000
236.408 Route locking	1,000	2,000
236.410 Locking, hand-operated switch; requirements:		
(a) Hand-operated switch on main track not electrically or mechanically locked in normal position where signal not provided to govern movement to main track, movements made at speeds in excess of 20 m.p.h., and train or engine movements may clear main track	2,500	5,000
(b) Hand-operated switch on signaled siding not electrically or mechanically locked in normal position where signal not provided to govern movements to signaled siding, train movements made at speeds in excess of 30 m.p.h., and train or engine movements may clear signaled siding	2,500	5,000
(c) Approach or time locking of electric lock at hand-operated switch can be defeated by use of emergency release device of electric lock which is not kept sealed in non-release position	2,500	5,000
(d) other violations	1,000	2,000
<i>Rules and Instructions—</i>		
236.426 Interlocking rules and instructions applicable to traffic control systems	1,000	2,000
236.476 Interlocking inspections and tests applicable to traffic control systems	1,000	2,000

Subpart E—Automatic Train Stop, Train Control and Cab Signal Systems Standards

236.501 Forestalling device and speed control	1,000	2,000
236.502 Automatic brake application, initiation by restrictive block conditions stopping distance in advance	1,000	2,000
236.503 Automatic brake application; initiation when predetermined rate of speed exceeded	1,000	2,000
236.504 Operations interconnected with automatic block-signal system	1,000	2,000
236.505 Proper operative relation between parts along roadway and parts on locomotive	1,000	2,000
236.506 Release of brakes after automatic application	1,000	2,000
236.507 Brake application; full service	1,000	2,000
236.508 Interference with application of brakes by means of brake valve	1,000	2,000
236.509 Two or more locomotives coupled	1,000	2,000
236.511 Cab signals controlled in accordance with block conditions stopping distance in advance	1,000	2,000
236.512 Cab signal indication when locomotive enters blocks	1,000	2,000
236.513 Audible indicator	1,000	2,000
236.514 Interconnection of cab signal system with roadway signal system	1,000	2,000
236.515 Visibility of cab signals	1,000	2,000
236.516 Power supply	1,000	2,000
<i>Rules and Instructions; Roadway—</i>		
236.526 Roadway element not functioning properly	2,500	5,000
236.527 Roadway element insulation resistance	1,000	2,000
236.528 Restrictive condition resulting from open hand-operated switch; requirement	1,000	2,000
236.529 Roadway element inductor; height and distance from rail	1,000	2,000
236.531 Trip arm; height and distance from rail	1,000	2,000
236.532 Strap iron inductor; use restricted	1,000	2,000
236.534 Rate of pressure reduction; equalizing reservoir or brake pipe	1,000	2,000
236.551 Power supply voltage	1,000	2,000
236.552 Insulation resistance	1,000	2,000
236.553 Seal, where required	2,500	5,000
236.554 Rate of pressure reduction; equalizing reservoir or brake pipe	1,000	2,000
236.555 Repaired or rewound receiver coil	1,000	2,000
236.556 Adjustment of relay	1,000	2,000
236.557 Receiver; location with respect to rail	1,000	2,000
236.560 Contact element, mechanical trip type; location with respect to rail	1,000	2,000
236.562 Minimum rail current required	1,000	2,000
236.563 Delay time	1,000	2,000
236.564 Acknowledging time	1,000	2,000
236.565 Provision made for preventing operation of pneumatic brake-applying apparatus by double-heading clock; requirement	1,000	2,000
236.566 Locomotive of each train operating in train stop, train control or cab signal territory; equipped	5,000	7,500

Section	Violation	Willful violation
236.567 Restrictions imposed when device fails and/or is cut out en route:		
(a) Report not made to designated officer at next available point of communication after automatic train stop, train control, or cab signal device fails and/or is cut en route	5,000	7,500
(b) Train permitted to proceed at speed exceeding 79 m.p.h. where automatic train stop, train control, or cab signal device fails and/or is cut out en route when absolute block established in advance of train on which device is inoperative	5,000	7,500
(c) other violations	1,000	2,000
236.568 Difference between speeds authorized by roadway signal and cab signal; action	1,000	2,000
<i>Inspection and Tests; Roadway—</i>		
236.576 Roadway element	1,000	2,000
236.577 Test, acknowledgement, and cut-in circuits	1,000	2,000
<i>Inspection and Tests; Locomotive—</i>		
236.586 Daily or after trip test	2,500	5,000
236.587 Departure test:		
(a) Test of automatic train stop, train control, or cab signal apparatus on locomotive not made on departure of locomotive from initial terminal if equipment on locomotive not cut out between initial terminal and equipped territory	5,000	7,500
(b) Test of automatic train stop, train control, or cab signal apparatus on locomotive not made immediately on entering equipped territory, if equipment on locomotive cut out between initial terminal and equipped territory	5,000	7,500
(c) Automatic train stop, train control, or cab signal apparatus on locomotive making more than one trip within 24-hour period not given departure test within corresponding 24-hour period	5,000	7,500
(d) other violations	2,500	5,000
236.588 Periodic test	2,500	5,000
236.589 Relays	2,500	5,000
236.590 Pneumatic apparatus:		
(a) Automatic train stop, train control, or cab signal apparatus not inspected and cleaned at least once every 736 days	2,500	5,000
(b) other violations	1,000	2,000
Subpart F—Dragging Equipment and Slide Detectors and Other Similar Protective Devices; Standards		
236.601 Signals controlled by devices; location	1,000	2,000
Subpart H—Standards for Processor-Based Signal and Train Control Systems		
236.905 Railroad Safety Program Plan (RSPP):		
Failure to develop and submit RSPP when required	5,000	7,500
Failure to obtain FRA approval for a modification to RSPP	5,000	7,500
236.907 Product Safety Plan (PSP):		
Failure to develop a PSP	5,000	7,500
Failure to submit a PSP when required	5,000	7,500
236.909 Minimum Performance Standard:		
Failure to make analyses or documentation available	2,500	5,000
Failure to determine that the standard has been met	5,000	7,500
236.913 Notification to FRA of PSPs:		
Failure to prepare a PSP or PSP amendment as required	2,500	5,000
Failure to submit a PSP or PSP amendment as required	5,000	7,500
Field testing without authorization or approval	10,000	20,000
236.915 Implementation and operation:		
(a) Operation of product without authorization or approval	10,000	20,000
(b) Failure to comply with PSP	2,500	5,000
(c) Interference with normal functioning safety-critical product	7,500	15,000
(d) Failure to determine cause and adjust, repair or replace without undue delay or take appropriate action pending repair	5,000	7,500
236.917 Retention of records:		
Failure to maintain records as required	7,500	15,000
Failure to report inconsistency	10,000	20,000
Failure to take prompt countermeasures	10,000	20,000
Failure to provide final report	2,500	5,000
236.919 Operations and Maintenance Manual	3,000	6,000
236.921 Training and qualification program, general	3,000	6,000
236.923 Task analysis and basic requirements:		
Failure to develop an acceptable training program	2,500	5,000
Failure to train persons as required	2,500	5,000
Failure to conduct evaluation of training program as required	2,500	5,000
Failure to maintain records as required	1,500	3,000
236.925 Training specific to control office personnel	2,500	5,000
236.927 Training specific to locomotive engineers and other operating personnel	2,500	5,000
236.929 Training specific to roadway workers	2,500	5,000

¹ The Administrator reserves the right to assess a civil penalty of up to \$27,000 per day for any violation where circumstances warrant. See 49 CFR part 209, appendix A.

¹ A penalty may be assessed against an individual only for a willful violation. The Administrator reserves the right to assess a penalty of up to \$27,000 for any violation where circumstances warrant. See 49 CFR part 209, appendix A.

[53 FR 52936, Dec. 29, 1988, as amended at 63 FR 11624, Mar. 10, 1998; 69 FR 30595, May 28, 2004; 70 FR 11104, Mar. 7, 2005]

APPENDIX B TO PART 236—RISK ASSESSMENT CRITERIA

The safety-critical performance of each product for which risk assessment is required under this part must be assessed in accordance with the following criteria or other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable:

(a) *How are risk metrics to be expressed?* The risk metric for the proposed product must describe with a high degree of confidence the accumulated risk of a train system that operates over a life-cycle of 25 years or greater. Each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis, and the risk value selected must be demonstrated to have a high degree of confidence.

(b) *How does the risk assessment handle interaction risks for interconnected subsystems/components?* The safety-critical assessment of each product must include all of its interconnected subsystems and components and, where applicable, the interaction between such subsystems.

(c) *How is the previous condition computed?* Each subsystem or component of the previous condition must be analyzed with a Mean Time to Hazardous Event (MTTHE) as specified subject to a high degree of confidence.

(d) *What major risk characteristics must be included when relevant to assessment?* Each risk calculation must consider the total signaling and train control system and method of operation, as subjected to a list of hazards to be mitigated by the signaling and train control system. The methodology requirements must include the following major characteristics, when they are relevant to the product being considered:

- (1) Track plan infrastructure;
- (2) Total number of trains and movement density;
- (3) Train movement operational rules, as enforced by the dispatcher and train crew behaviors;
- (4) Wayside subsystems and components; and
- (5) Onboard subsystems and components.

(e) *What other relevant parameters must be determined for the subsystems and components?* The failure modes of each subsystem or component, or both, must be determined for the integrated hardware/software (where applicable) as a function of the Mean Time to Failure (MTTF) failure restoration rates, and the

integrated hardware/software coverage of all processor-based subsystems or components, or both. Train operating and movement rules, along with components that are layered in order to enhance safety-critical behavior, must also be considered.

(f) *How are processor-based subsystems/components assessed?* (1) An MTTHE value must be calculated for each processor-based subsystem or component, or both, indicating the safety-critical behavior of the integrated hardware/software subsystem or component, or both. The human factor impact must be included in the assessment, whenever applicable, to provide an integrated MTTHE value. The MTTHE calculation must consider the rates of failures caused by permanent, transient, and intermittent faults accounting for the fault coverage of the integrated hardware/software subsystem or component, phased-interval maintenance, and restoration of the detected failures.

(2) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The compliance process must be demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to have a high degree of confidence.

(g) *How are non-processor-based subsystems/components assessed?* (1) The safety-critical behavior of all non-processor-based components, which are part of a processor-based system or subsystem, must be quantified with an MTTHE metric. The MTTHE assessment methodology must consider failures caused by permanent, transient, and intermittent faults, phase-interval maintenance and restoration of failures and the effect of fault coverage of each non-processor-based subsystem or component.

(2) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The non-processor-based quantification compliance must be demonstrated to have a high degree of confidence.

(h) *What assumptions must be documented?* (1) The railroad shall document any assumptions regarding the reliability or availability of mechanical, electric, or electronic components. Such assumptions must include MTTF

projections, as well as Mean Time to Repair (MTTR) projections, unless the risk assessment specifically explains why these assumptions are not relevant to the risk assessment. The railroad shall document these assumptions in such a form as to permit later automated comparisons with in-service experience (e.g., a spreadsheet).

(2) The railroad shall document any assumptions regarding human performance. The documentation shall be in such a form as to facilitate later comparisons with in-service experience.

(3) The railroad shall document any assumptions regarding software defects. These assumptions shall be in a form which permits the railroad to project the likelihood of detecting an in-service software defect. These assumptions shall be documented in such a form as to permit later automated comparisons with in-service experience.

(4) The railroad shall document all of the identified safety-critical fault paths. The documentation shall be in such a form as to facilitate later comparisons with in-service faults.

[70 FR 11105, Mar. 7, 2005]

APPENDIX C TO PART 236—SAFETY ASSURANCE CRITERIA AND PROCESSES

(a) *What is the purpose of this appendix?* This appendix seeks to promote full disclosure of safety risk to facilitate minimizing or eliminating elements of risk where practicable by providing minimum criteria and processes for safety analyses conducted in support of PSPs. The analysis required by this appendix is intended to minimize the probability of failure to an acceptable level, helping to optimize the safety of the product within the limitations of the available engineering science, cost, and other constraints. FRA uses the criteria and processes set forth in this appendix to evaluate analyses, assumptions, and conclusions provided in RSP and PSP documents. An analysis performed under this appendix must:

(1) Address each area of paragraph (b) of this appendix, explaining how such objectives are addressed or why they are not relevant, and

(2) Employ a validation and verification process pursuant to paragraph (c) of this appendix.

(b) *What categories of safety elements must be addressed?* The designer shall address each of the following safety considerations when designing and demonstrating the safety of products covered by subpart H of this part. In the event that any of these principles are not followed, the PSP shall state both the reason(s) for departure and the alternative(s) utilized to mitigate or eliminate the hazards associated with the design principle not followed.

(1) *Normal operation.* The system (including all hardware and software) must demonstrate safe operation with no hardware failures under normal anticipated operating conditions with proper inputs and within the expected range of environmental conditions. All safety-critical functions must be performed properly under these normal conditions. Absence of specific operator actions or procedures will not prevent the system from operating safely. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

(2) *Systematic failure.* It must be shown 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 product development. This includes unsafe errors in the software due to human error in the software specification, design or coding phases, or both; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

(3) *Random failure.* (i) The product must be shown to operate safely under conditions of random hardware failure. This includes single as well as multiple hardware failures, particularly in instances where one or more failures could occur, remain undetected (latent) and react in combination with a subsequent failure at a later time to cause an unsafe operating situation. In instances involving a latent failure, a subsequent failure is similar to there being a single failure. In the event of a transient failure, and if so designed, the system should restart itself if it is safe to do so. Frequency of attempted restarts must be considered in the hazard analysis required by §236.907(a)(8).

(ii) There shall be no single point failures in the product that can result 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.

(iii) If one non-self-revealing failure combined with a second failure can cause a hazard that is categorized as unacceptable or undesirable, then the second failure must be detected and the product must achieve a known safe state before falsely activating any physical appliance.

(4) *Common Mode failure.* Another concern of multiple failure involves common mode failures in which two or more subsystems or components intended to compensate one another to perform the same function all fail

by the same mode and result in unsafe conditions. This is of particular concern in instances in which two or more elements (hardware or software, or both) are used in combination to ensure safety. If a common mode failure exists, then any analysis performed under this appendix cannot rely on the assumption that failures are independent. Examples include: the use of redundancy in which two or more elements perform a given function in parallel and when one (hardware or software) element checks/monitors another element (of hardware or software) to help ensure its safe operation. Common mode failure relates to independence, which must be ensured in these instances. When dealing with the effects of hardware failure, the designer shall address the effects of the failure not only on other hardware, but also on the execution of the software, since hardware failures can greatly affect how the software operates.

(5) *External influences.* The product must be shown to operate safely when subjected to different external influences, including:

(i) Electrical influences such as power supply anomalies/transients, abnormal/improper input conditions (*e.g.*, outside of normal range inputs relative to amplitude and frequency, unusual combinations of inputs) including those related to a human operator, and others such as electromagnetic interference or electrostatic discharges, or both;

(ii) Mechanical influences such as vibration and shock; and

(iii) Climatic conditions such as temperature and humidity.

(6) *Modifications.* Safety must be ensured following modifications to the hardware or software, or both. All or some of the concerns identified in this paragraph may be applicable depending upon the nature and extent of the modifications.

(7) *Software.* Software faults must not cause hazards categorized as unacceptable or undesirable.

(8) *Closed Loop Principle.* The product design must require positive action to be taken in a prescribed manner to either begin product operation or continue product operation.

(9) *Human Factors Engineering.* The product design must sufficiently incorporate human factors 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 interaction with the component; and the environment in which the product will be used.

(c) *What standards are acceptable for verification and validation?* (1) The standards employed for verification or validation, or both, of products subject to this subpart must be sufficient to support achievement of the applicable requirements of subpart H of this part.

(2) U.S. Department of Defense Military Standard (MIL-STD) 882C, "System Safety Program Requirements" (January 19, 1993), is recognized as providing appropriate risk analysis processes for incorporation into verification and validation standards.

(3) The following standards designed for application to processor-based signal and train control systems are recognized as acceptable with respect to applicable elements of safety analysis required by subpart H of this part. The latest versions of the standards listed below should be used unless otherwise provided.

(i) IEEE 1483-2000, Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

(ii) CENELEC Standards as follows:

(A) EN50126: 1999, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(B) EN50128 (May 2001), Railway Applications: Software for Railway Control and Protection Systems;

(C) EN50129: 2003, Railway Applications: Communications, Signaling, and Processing Systems-Safety Related Electronic Systems for Signaling; and

(D) EN50155:2001/A1:2002, Railway Applications: Electronic Equipment Used in Rolling Stock.

(iii) ATCS Specification 140, Recommended Practices for Safety and Systems Assurance.

(iv) ATCS Specification 130, Software Quality Assurance.

(v) AAR-AREMA 2005 Communications and Signal Manual of Recommended Practices, Part 17.

(vi) Safety of High Speed Ground Transportation Systems. Analytical Methodology for Safety Validation of Computer Controlled Subsystems. Volume II: Development of a Safety Validation Methodology. Final Report September 1995. Author: Jonathan F. Luedeke, Battelle. DOT/FRA/ORD-95/10.2.

(vii) IEC 61508 (International Electrotechnical Commission), Functional Safety of Electrical/Electronic/Programmable/Electronic Safety (E/E/P/ES) Related Systems, Parts 1-7 as follows:

(A) IEC 61508-1 (1998-12) Part 1: General requirements and IEC 61508-1 Corr. (1999-05) Corrigendum 1-Part 1: General Requirements.

(B) IEC 61508-2 (2000-05) Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

(C) IEC 61508-3 (1998-12) Part 3: Software requirements and IEC 61508-3 Corr.1(1999-04) Corrigendum 1-Part3: Software requirements.

(D) IEC 61508-4 (1998-12) Part 4: Definitions and abbreviations and IEC 61508-4 Corr.1(1999-04) Corrigendum 1-Part 4: Definitions and abbreviations.

(E) IEC 61508-5 (1998–12) Part 5: Examples of methods for the determination of safety integrity levels and IEC 61508-5 Corr.1 (1999-04) Corrigendum 1 Part 5: Examples of methods for determination of safety integrity levels.

(F) IEC 61508-6 (2000-04) Part 6: Guidelines on the applications of IEC 61508-2 and -3.

(G) IEC 61508-7 (2000-03) Part 7: Overview of techniques and measures.

(4) Use of unpublished standards, including proprietary standards, is authorized to the extent that such standards are shown to achieve the requirements of this part. However, any such standards shall be available for inspection and replication by FRA and for public examination in any public proceeding before the FRA to which they are relevant.

[70 FR 11106, Mar. 7, 2005]

APPENDIX D TO PART 236—INDEPENDENT REVIEW OF VERIFICATION AND VALIDATION

(a) *What is the purpose of this appendix?* This appendix provides minimum requirements for independent third-party assessment of product safety verification and validation pursuant to subpart H of this part. The goal of this assessment is to provide an independent evaluation of the product manufacturer's utilization of safety design practices during the product's development and testing phases, as required by the applicable railroad's RSPP, the product PSP, the requirements of subpart H of this part, and any other previously agreed-upon controlling documents or standards.

(b) *What general requirements apply to the conduct of third party assessments?* (1) The supplier may request advice and assistance of the reviewer concerning the actions identified in paragraphs (c) through (g) of this appendix. However, the reviewer should not engage in design efforts, in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the product.

(2) The supplier shall provide the reviewer access to any and all documentation that the reviewer requests and attendance at any design review or walkthrough that the reviewer determines as necessary to complete and accomplish the third party assessment. The reviewer may be accompanied by representatives of FRA as necessary, in FRA's judgment, for FRA to monitor the assessment.

(c) *What must be done at the preliminary level?* The reviewer shall evaluate with respect to safety and comment on the adequacy of the processes which the supplier applies to the design and development of the product. At a minimum, the reviewer shall compare the supplier processes with acceptable methodology and employ any other such

tests or comparisons if they have been agreed to previously with FRA. Based on these analyses, the reviewer shall identify and document any significant safety vulnerabilities which are not adequately mitigated by the supplier's (or user's) processes. Finally, the reviewer shall evaluate the adequacy of the railroad's RSPP, the PSP, and any other documents pertinent to the product being assessed.

(d) *What must be done at the functional level?*

(1) The reviewer shall analyze the Preliminary Hazard Analysis (PHA) for comprehensiveness and compliance with the railroad's RSPP.

(2) The reviewer shall analyze all Fault Tree Analyses (FTA), Failure Mode and Effects Criticality Analysis (FMECA), and other hazard analyses for completeness, correctness, and compliance with the railroad's RSPP.

(e) *What must be done at the implementation level?* The reviewer shall randomly select various safety-critical software modules for audit to verify whether the requirements of the RSPP were followed. The number of modules audited must be determined as a representative number sufficient to provide confidence that all unaudited modules were developed in compliance with the RSPP.

(f) *What must be done at closure?* (1) The reviewer shall evaluate and comment on the plan for installation and test procedures of the product for revenue service.

(2) The reviewer shall prepare a final report of the assessment. The report shall be submitted to the railroad prior to the commencement of installation testing and contain at least the following information:

(i) Reviewer's evaluation of the adequacy of the PSP, including the supplier's MTTHE and risk estimates for the product, and the supplier's confidence interval in these estimates;

(ii) Product vulnerabilities which the reviewer felt were not adequately mitigated, including the method by which the railroad would assure product safety in the event of a hardware or software failure (*i.e.*, how does the railroad assure that all potentially hazardous failure modes are identified?) and the method by which the railroad addresses comprehensiveness of the product design for the requirements of the operations it will govern (*i.e.*, how does the railroad assure that all potentially hazardous operating circumstances are identified? Who records any deficiencies identified in the design process? Who tracks the correction of these deficiencies and confirms that they are corrected?);

(iii) A clear statement of position for all parties involved for each product vulnerability cited by the reviewer;

(iv) Identification of any documentation or information sought by the reviewer that was denied, incomplete, or inadequate;

(v) A listing of each RSPP procedure or process which was not properly followed;

(vi) Identification of the software verification and validation procedures for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(vii) Methods employed by the product manufacturer to develop safety-critical software, such as use of structured language, code checks, modularity, or other similar generally acceptable techniques; and

(viii) Method by which the supplier or railroad addresses comprehensiveness of the product design which considers the safety elements listed in paragraph (b) of appendix C to this part.

[70 FR 11107, Mar. 7, 2005]

APPENDIX E TO PART 236—HUMAN-MACHINE INTERFACE (HMI) DESIGN

(a) *What is the purpose of this appendix?* The purpose of this appendix is to provide HMI design criteria which will minimize negative safety effects by causing designers to consider human factors in the development of HMIs.

(b) *What is meant by "designer" and "operator"?* As used in this section, "designer" means anyone who specifies requirements for—or designs a system or subsystem, or both, for—a product subject to subpart H of this part, and "operator" means any human who is intended to receive information from, provide information to, or perform repairs or maintenance on a signal or train control product subject to subpart H of this part.

(c) *What kinds of human factors issues must designers consider with regard to the general function of a system?—(1) Reduced situational awareness and over-reliance.* HMI design must give an operator active functions to perform, feedback on the results of the operator's actions, and information on the automatic functions of the system as well as its performance. The operator must be "in-the-loop." Designers shall consider at minimum the following methods of maintaining an active role for human operators:

(i) The system must require an operator to initiate action to operate the train and require an operator to remain "in-the-loop" for at least 30 minutes at a time;

(ii) The system must provide timely feedback to an operator regarding the system's automated actions, the reasons for such actions, and the effects of the operator's manual actions on the system;

(iii) The system must warn operators in advance when they require an operator to take action; and

(iv) HMI design must equalize an operator's workload.

(2) *Expectation of predictability and consistency in product behavior and communications.*

HMI design must accommodate an operator's expectation of logical and consistent relationships between actions and results. Similar objects must behave consistently when an operator performs the same action upon them.

(3) *Limited memory and ability to process information.* (i) HMI design must minimize an operator's information processing load. To minimize information processing load, the designer shall:

(A) Present integrated information that directly supports the variety and types of decisions that an operator makes;

(B) Provide information in a format or representation that minimizes the time required to understand and act; and

(C) Conduct utility tests of decision aids to establish clear benefits such as processing time saved or improved quality of decisions.

(ii) HMI design must minimize the load on an operator's memory.

(A) To minimize short-term memory load, the designer shall integrate data or information from multiple sources into a single format or representation ("chunking") and design so that three or fewer "chunks" of information need to be remembered at any one time.

(B) To minimize long-term memory load, the designer shall design to support recognition memory, design memory aids to minimize the amount of information that must be recalled from unaided memory when making critical decisions, and promote active processing of the information.

(4) *Miscellaneous Human Factors Concerns.* System designers shall:

(i) Design systems that anticipate possible user errors and include capabilities to catch errors before they propagate through the system;

(ii) Conduct cognitive task analyses prior to designing the system to better understand the information processing requirements of operators when making critical decisions; and

(iii) Present information that accurately represents or predicts system states.

(d) *What kinds of HMI design elements must a designer incorporate in the development of on-board train displays and controls?—(1) Location of displays and controls.* Designers shall:

(i) Locate displays as close as possible to the controls that affect them;

(ii) Locate displays and controls based on an operator's position;

(iii) Arrange controls to minimize the need for the operator to change position;

(iv) Arrange controls according to their expected order of use;

(v) Group similar controls together;

(vi) Design for high stimulus-response compatibility (geometric and conceptual);

(vii) Design safety-critical controls to require more than one positive action to activate (*e.g.*, auto stick shift requires two movements to go into reverse); and

(viii) Design controls to allow easy recovery from error.

(2) *Information management.* HMI design must:

(i) Display information in a manner which emphasizes its relative importance;

(ii) Comply with the ANSI/HFS 100–1988 standard;

(iii) Design for display luminance of the foreground or background of at least 35 cd/m² (the displays should be capable of a minimum contrast 3:1 with 7:1 preferred, and controls should be provided to adjust the brightness level and contrast level);

(iv) Design the interface to display only the information necessary to the user;

(v) Where text is needed, using short, simple sentences or phrases with wording that an operator will understand;

(vi) Use complete words where possible; where abbreviations are necessary, choose a commonly accepted abbreviation or consistent method and select commonly used terms and words that the operator will understand;

(vii) Adopt a consistent format for all display screens by placing each design element in a consistent and specified location;

(viii) Display critical information in the center of the operator's field of view by placing items that need to be found quickly in the upper left hand corner and items which are not time-critical in the lower right hand corner of the field of view;

(ix) Group items that belong together;

(x) Design all visual displays to meet human performance criteria under monochrome conditions and add color only if it will help the user in performing a task, and use color coding as a redundant coding technique;

(xi) Limit the number of colors over a group of displays to no more than seven;

(xii) Design warnings to match the level of risk or danger with the alerting nature of the signal;

(xiii) With respect to information entry, avoid full QWERTY keyboards for data entry; and

(xiv) Use digital communications for safety-critical messages between the locomotive engineer and the dispatcher.

(e) *What kinds of HMI design elements must a designer consider with respect to problem management?* (1) HMI design must enhance an operator's situation awareness. An operator must have access to:

(i) Knowledge of the operator's train location relative to relevant entities;

(ii) Knowledge of the type and importance of relevant entities;

(iii) Understanding of the evolution of the situation over time;

(iv) Knowledge of the roles and responsibilities of relevant entities; and

(v) Knowledge of expected actions of relevant entities.

(2) HMI design must support response selection and scheduling.

(3) HMI design must support contingency planning.

[70 FR 11107, Mar. 7, 2005]

PART 238—PASSENGER EQUIPMENT SAFETY STANDARDS

Subpart A—General

Sec.

238.1 Purpose and scope.

238.3 Applicability.

238.5 Definitions.

238.7 Waivers.

238.9 Responsibility for compliance.

238.11 Penalties.

238.13 Preemptive effect.

238.15 Movement of passenger equipment with power brake defects.

238.17 Movement of passenger equipment with other than power brake defects.

238.19 Reporting and tracking of repairs to defective passenger equipment.

238.21 Special approval procedure.

238.23 Information collection.

Subpart B—Safety Planning and General Requirements

238.101 Scope.

238.103 Fire safety.

238.105 Train electronic hardware and software safety.

238.107 Inspection, testing, and maintenance plan.

238.109 Training, qualification, and designation program.

238.111 Pre-revenue service acceptance testing plan.

238.113 Emergency window exits.

238.115 Emergency lighting.

238.117 Protection against personal injury.

238.119 Rim-stamped straight-plate wheels.

Subpart C—Specific Requirements for Tier I Passenger Equipment

238.201 Scope/alternative compliance.

238.203 Static end strength.

238.205 Anti-climbing mechanism.

238.207 Link between coupling mechanism and car body.

238.209 Forward-facing end structure of locomotives.

238.211 Collision posts.

238.213 Corner posts.

238.215 Rollover strength.

238.217 Side structure.

238.219 Truck-to-car-body attachment.

238.221 Glazing.