Consensus Rule Text:

§229.23 Periodic inspection: General.

(d) Each periodic inspection shall be recorded on Form FRA F 6180–49A. The form shall be signed by the person conducting the inspection and certified by that person's supervisor that the work was done. The form shall be displayed under a transparent cover in a conspicuous place in the cab of each locomotive.

INSERT (d)(1) A carrier maintaining and transferring records as provided for in §229.20 shall print the name of the person who performed the inspections, repairs, or certified work on the Form FRA F 6180-49A that is displayed in the cab of each locomotive.

(g) The carrier shall maintain, and provide employees with, a list of the defects and repairs made on each locomotive over the last ninety-two days;

(h) The carrier shall provide employees performing inspections under this section with a document containing all tests and procedures needed to perform the inspection.

* * * * *

§229.27 Annual tests (load meters).

[Deleted:(b) The load meter shall be tested. Each device used by the engineer to aid in the control or braking of the train or locomotive that provides an indication of air pressure electronically shall be tested by comparison with a test gauge or self-test designed for this purpose. An error of greater than five percent or three pounds per square inch shall be corrected. The date and place of the test shall be recorded on Form FRA F 6180-49A, and the person conducting the test and that person's supervisor shall sign the form.]

Replaced by:
(b) Load meters that indicate current or amperage being applied to traction motors shall be tested. Each device used by the engineer to aid in the control or braking of the train or locomotive that provides an indication of air pressure electronically shall be tested by comparison with a test gauge or self-test designed for this purpose. An error of greater than five percent or three pounds per square inch shall be corrected. The date and place of the test shall be recorded on Form FRA F 6180-49A, and the person conducting the test and that person's supervisor shall sign the form.

* * * * *

§229.27 Annual tests (COT&S).

A locomotive, including a DMU or MU locomotive, shall be subjected to the tests and inspections prescribed in paragraphs (b) and (c) of this section. A locomotive, including a DMU or MU locomotive, equipped with a microprocessor based event recorder that includes a self-monitoring feature, shall be subjected to the tests and inspections prescribed in paragraph (d) of this section. All testing under this section shall be performed at intervals that do not exceed 368 days.

[Deleted: 229.27(a)] replaced by new 229.29

[Deleted: 229.29] replace with the following:

229.29 Air Brake System Maintenance and Testing

A locomotive shall be subjected to the maintenance and testing prescribed in paragraph (a) of this section. Intervals for maintenance and testing of locomotives with various types of air brake systems shall be as prescribed in paragraphs (b), (c), and (d) of this section. Records of the maintenance and testing required in this section shall be kept as prescribed in paragraph (e) of this section.

(a) Levels of air brake system maintenance and testing shall be:

(1) Level one: Locomotives shall have the filtering devices or dirt collectors located in the main reservoir supply line to the air brake system cleaned, repaired, or replaced.

(2) Level two: Locomotives shall have the following components cleaned, repaired, and tested: brake cylinder relay valve portions; main reservoir safety valves; brake pipe vent valve portions; and, feed and reducing valve portions in the air brake system (including related dirt collectors and filters)–

(3) Level three: The following components shall be removed from the locomotive and disassembled; cleaned and lubricated (if necessary); have all parts that can deteriorate within the inspection interval as defined in (c) or (d)(1),(2), or (3) replaced; and tested: All pneumatic components of the locomotive equipment's brake system that contain moving parts, and are sealed against air leaks; all valves, valve portions, MU locomotive brake cylinders, electric-pneumatic master controllers in the air brake system, and all air brake related filters and dirt collectors–

(b) Locomotives shall receive level one air brake maintenance and testing as described in this section at intervals that do not exceed 368 days, except for MU locomotives covered under 238.309(b).

(c) For locomotives equipped with an air brake system not specifically identified in paragraphs (d)(1) through (d)(3) of this section; Level two air brake maintenance and testing as described in this section, shall be performed at intervals that do not exceed 368 days and Level three air

brake maintenance and testing as described in this section, shall be performed at intervals that do not exceed 736 days.

(d) Level two and three air brake maintenance and testing shall be performed:

(1) At intervals that do not exceed 1,104 days for a locomotive equipped with a 26-L or equivalent brake system;

(2) At intervals that do not exceed 1,472 days for locomotives equipped with an air dryer and a 26-L or equivalent brake system and for locomotives not equipped with an air compressor and semi-permanently coupled and dedicated to locomotives with an air dryer; and

(3) At intervals that do not exceed 1,840 days for locomotives equipped with CCB-1, CCB-2, CCB-26, Epic 1, Epic 2, or Fastbrake brake system.

(e) The following records shall be generated and maintained as prescribed below:

(1) The date and place of the cleaning, repairing and testing required by this section shall be recorded on Form FRA F 6180-49A, and the person performing the work and that person's supervisor shall sign the form. A record of the parts of the air brake system that are cleaned, repaired, and tested shall be kept in the carrier's files or in the cab of the locomotive.

(2) At its option, a carrier may fragment the work required by this section. In that event, a separate air record shall be maintained under a transparent cover in the cab. The air record shall include the locomotive number, a list of the air brake components, and the date and place of the inspection and test of each component. The signature of the person performing the work and the signature of that person's supervisor shall be included for each component. A duplicate record shall be maintained in the carrier's files.

(f) MU locomotives. The brake equipment of each MU locomotive shall be cleaned, repaired and tested, and the filtering devices or dirt collectors located in the main reservoir supply line to the air brake system cleaned, repaired or replaced at intervals in accordance with 238.309(b)(1),(2), and (3).

* * * * *

§229.46 Brakes: General.

(a) Before each trip, the railroad shall know the following:

(1) The locomotive brakes and devices for regulating pressures, including but not limited to the automatic and independent brake control systems, operate as intended; and

(2) The water and oil have been drained from the air brake system of all locomotives in the consist.

(b) A locomotive with an inoperative or ineffective automatic or independent brake control system will be considered to be operating as intended for purposes of paragraph (a) of this section, if all of the following conditions are met:

(1) The locomotive is in a trailing position and is not the controlling locomotive in a distributed power consist;

(2) The railroad has previously determined, in conjunction with the locomotive and/or airbrake manufacturer, that placing such a locomotive in trail mode adequately isolates the non-functional valves so as to allow safe operation of the brake systems from the controlling locomotive;

(3) If deactivation of the circuit breaker for the air brake system is required, it shall be specified in the railroad's operating rules;

(4) A tag shall immediately be placed on the isolation switch of the locomotive giving the date and location and stating that the unit may only be used in a trailing position and may not be used as a lead or controlling locomotive;

(5) The tag required in paragraph (b)(4) of this section shall remain attached to the isolation switch of the locomotive until repairs are made; and

(6) The inoperative or ineffective brake control system shall be repaired prior to or at the next periodic inspection.

* * * * *

§229.85 Doors and cover plates marked "Danger".

[Deleted: §229.85 Doors and cover plates marked "Danger".
All doors and cover plates guarding high voltage equipment shall be marked "Danger-High Voltage" or with the word "Danger" and the normal voltage carried by the parts so protected.]

Replaced by:
§229.85 Doors and cover plates marked "Danger".
All doors or cover plates guarding or providing direct access to high voltage equipment shall be marked "Danger-High Voltage" or with the word "Danger" and the normal voltage carried by the parts so protected.

* * * * *

§229.114 Steam generator inspections and tests.

[Language taken from 229.23, 229.25, and 229.27 to consolidate steam generator requirements for clarity and convenience]

229.114(a)
(a) Periodic steam generator inspection. Each steam generator shall be inspected to determine whether it complies with this section at intervals not to exceed 92 days, except as provided in §229.33. All non-complying conditions shall be repaired, or the steam generator shall be isolated as prescribed in §229.114(b), before the locomotive is used.

229.114(b)
(b) The periodic inspection of the steam generator may be postponed indefinitely if the water suction pipe to the water pump and the leads to the main switch (steam generator switch) are disconnected, and the train line shut-off-valve is wired closed or a blind gasket applied. However, the steam generator shall be so inspected before it is returned to use.

229.114(c)
(c) Each periodic steam generator inspection shall be recorded on the Form FRA F 6180-49A required by paragraph 229.23(d). When the Form FRA F 6180-49A for the locomotive is replaced, data for the steam generator inspections shall be transferred to the new Form FRA F6180-49A.

229.114(d)
(d) Each steam generator that is not isolated as prescribed in § 229.114(b) shall be inspected and tested as follows:

229.114(d)(1) All electrical devices and visible insulation shall be inspected.

229.114(d)(2)All automatic controls, alarms and protective devices shall be inspected and tested.

229.114(d)(3)Steam pressure gauges shall be tested by comparison with a dead-weight tester or a test gauge designed for this purpose. The siphons to the steam gauges shall be removed and their connections examined to determine that they are open.

229.114(d)(4)Safety valves shall be set and tested under steam after the steam pressure gauge is tested.

229.114(e) Annual steam generator tests. Each steam generator that is not isolated as prescribed in §229.114(b), shall be subjected to a hydrostatic pressure at least 25 percent above the working pressure and the visual return water-flow indicator shall be removed and inspected. All testing under this paragraph shall be performed at intervals that do not exceed 368 calendar days.

* * * * *

§229.123 Pilots, snowplows, end plates.

[Deleted: After January 1, 1981, each lead locomotive shall be equipped with an end plate that extends across both rails, a pilot, or a snowplow. The minimum clearance above the rail of the pilot, snowplow or end plate shall be 3 inches and the maximum clearance 6 inches.]

Replaced by:
(a) Each lead locomotive shall be equipped with a pilot, snowplow, or end plate that extends across both rails. The minimum clearance above the rail of the pilot, snowplow or end plate shall be 3 inches. Except as noted in (b), the maximum clearance shall be 6 inches.

(b) To provide clearance for passing over retarders, locomotives utilized in hump yard or switching service at hump yard locations may have pilot, snowplow, or end plate maximum height of 9 inches.

(1) Each pilot, snowplow, or end plate with clearance above 6 inches shall be prominently stenciled at two locations with "9 inch Maximum End Plate Height, Yard or Trail Service Only."

(2) When operated in switching service in a leading position, locomotives with a pilot, snowplow, or end plate clearance above 6 inches shall be limited to 10 miles per hour over grade crossings.

(3) Train crews shall be notified in writing of the restrictions on the locomotive, by label or stencil in the cab, or by written operating instruction given to the crew and maintained in the cab of the locomotive.

(4) Pilot, snowplow, or end plate clearance above 6 inches shall be noted in the remarks section of Form FRA 6180-49a.

(5)Locomotives with a pilot, snowplow, or end plate clearance above 6 inches shall not be placed in the lead position when being moved under Part 229.9

* * * * *

§229.125 Headlights and auxiliary lights.

[language that is being added is in italics; and language being deleted appears in brackets].

(a) Each lead locomotive used in road service shall *illuminate its headlight while the locomotive is in use. When illuminated,* the headlight shall produce a peak intensity of at least 200,000 candela *and produce at least 3,000 candela at an angle of 7.5 degrees and at least 400 candela*

at an angle of 20 degrees from the centerline of the locomotive when the light is aimed parallel to the tracks. If a locomotive or locomotive consist in road service is regularly required to run backward for any portion of its trip other than to pick up a detached portion of its train or to make terminal movements, it shall also have on its rear a headlight that meets the intensity requirements above. Each headlight shall be arranged to illuminate a person at least 800 feet ahead and in front of the headlight. For purposes of this section, a headlight shall be comprised of either one or two lamps.

(1) If a locomotive is equipped with a single-lamp headlight, the single lamp shall produce a peak intensity of at least 200,000 candela *and shall produce at least 3,000 candela at an angle of 7.5 degrees and at least 400 candela at an angle of 20 degrees from the centerline of the locomotive when the light is aimed parallel to the tracks.* The following *operative* lamps meet the standard set forth in this paragraph (a)(1): a single [Deleted: "operative"] *incandescent* PAR-56, 200-watt, 30-volt lamp; *a single halogen PAR-56, 200-watt, 30-volt lamp; a single halogen PAR-56, 350-watt, 75-volt lamp, or a single lamp meeting the intensity requirements given above* [Deleted:"or an operative lamp of equivalent design and intensity"].

(2) If a locomotive is equipped with a dual-lamp headlight, a peak intensity of at least 200,000 candela *and at least 3,000 candela at an angle of 7.5 degrees and at least 400 candela at an angle of 20 degrees from the centerline of the locomotive when the light is aimed parallel to the tracks* shall be produced by the headlight based either on a single lamp capable of individually producing the required peak intensity or on the candela produced by the headlight with both lamps illuminated. If both lamps are needed to produce the required peak intensity, then both lamps in the headlight shall be operational. The following *operative* lamps meet the standard set forth in this paragraph (a)(2): a single *incandescent* PAR-56, 200-watt, 30-volt lamp; *a single halogen PAR-56, 200-watt, 30-volt lamp; a single halogen PAR-56, 350-watt, 75-volt lamp*; two [Deleted: "operative"] *incandescent* PAR-56, 350-watt, 75-volt lamps; [Deleted:"or an operative lamp of equivalent design and intensity"] *or lamp(s) meeting the intensity requirements given above.*

(i) A locomotive equipped with two incandescent PAR-56, 350-watt, 75-volt lamps which has an en route failure of one lamp in the headlight fixture, may continue in service as a lead locomotive until its next daily inspection under §229.21 provided:

(A) Auxiliary lights on the locomotive are set to burn steadily and shall remain activated continually until the headlight lamp is repaired or the unit is moved to a trailing position, except as provided in paragraphs (e) and (f) of this section.

(B) Auxiliary lights shall be focused horizontally parallel to the longitudinal centerline of the locomotive or aimed to cross no less than 400 feet in front of the locomotive.

(C) The second headlight lamp and both auxiliary lights shall remain operational. In case of the failure of a second lamp (either a headlight or

auxiliary light), the locomotive shall be handled in accordance with 49 CFR §229.9.

(b) Each locomotive or locomotive consist used in yard service shall have two headlights, one located on the front of the locomotive or locomotive consist and one on its rear. Each headlight shall produce at least 60,000 candela and shall be arranged to illuminate a person at least 300 feet ahead and in front of the headlight.

(c) Headlights shall be provided with a device to dim the light.

(d) Effective December 31, 1997, each lead locomotive operated at a speed greater than 20 miles per hour over one or more public highway-rail crossings shall be equipped with operative auxiliary lights, in addition to the headlight required by paragraph (a) or (b) of this section. A locomotive equipped on March 6, 1996 with auxiliary lights in conformance with § 229.133 shall be deemed to conform to this section until March 6, 2000. All locomotives in compliance with § 229.133(c) shall be deemed to conform to this section. Auxiliary lights shall be composed as follows:

(1) Two white auxiliary lights shall be placed at the front of the locomotive to form *an equilateral triangle* with the headlight.

(i) The auxiliary lights shall be at least 36 inches above the top of the rail, except on MU locomotives and control cab locomotives where such placement would compromise the integrity of the car body or be otherwise impractical. Auxiliary lights on such MU locomotives and control cab locomotives shall be at least 24 inches above the top of the rail.

(ii) The auxiliary lights shall be spaced at least 36 inches apart if the vertical distance from the headlight to the horizontal axis of the auxiliary lights is 60 inches or more.

(iii) The auxiliary lights shall be spaced at least 60 inches apart if the vertical distance from the headlight to the horizontal axis of the auxiliary lights is less than 60 inches.

(2) Each auxiliary light shall produce a peak intensity of at least 200,000 candela or shall produce at least 3,000 candela at an angle of 7.5 degrees and at least 400 candela at an angle of 20 degrees from the centerline of the locomotive when the light is aimed parallel to the tracks. Any of the following *operative* lamps meet the standard set forth in this paragraph (d)(2): an [Deleted: "operative"] *incandescent* PAR-56, 200-watt, 30-volt lamp; *a halogen PAR-56, 200-watt, 30-volt lamp; a halogen PAR-56, 350-watt,75-volt lamp;* an *incandescent* PAR-56, 350-watt,75-volt lamp; [Deleted: "or an operative lamp of equivalent design and intensity"] *or a single lamp having equivalent intensities at the specified angles.*

(3) The auxiliary lights shall be focused horizontally within 15 degrees of the longitudinal centerline of the locomotive.

(e) Auxiliary lights required by paragraph (d) of this section may be arranged

(1) to burn steadily, or

(2) flash on approach to a crossing.;

(i) If the auxiliary lights are arranged to flash they shall flash alternately at a rate of at least 40 flashes per minute and at most 180 flashes per minute,

(ii) the railroad's operating rules shall set a standard procedure for use of flashing lights at public highway-rail grade crossings, and

(iii) the flashing feature may be activated automatically, but shall be capable of manual activation and deactivation by the locomotive engineer.

(f) Auxiliary lights required by paragraph (d) of this section shall be continuously illuminated immediately prior to and during movement of the locomotive, except as provided by railroad operating rules, timetable or special instructions, unless such exception is disapproved by FRA. A railroad may except use of auxiliary lights at a specific public highway-rail grade crossing by designating that exception in the railroad's operating rules, timetable, or a special order. Any exception from use of auxiliary lights at a specific public grade crossing can be disapproved for a stated cause by FRA's Associate Administrator for Safety or any one of FRA's Regional Administrators, after investigation by FRA and opportunity for response from the railroad.

(g) Movement of locomotives with defective auxiliary lights.

(1) A lead locomotive with only one failed auxiliary light shall be repaired or switched to a trailing position before departure from the place where an initial terminal inspection is required for that train.

(2) A locomotive with only one auxiliary light that has failed after departure from an initial terminal, shall be repaired not later than the next calendar inspection required by § 229.21.

(3) A lead locomotive with two failed auxiliary lights may only proceed to the next place where repairs can be made. This movement shall be consistent with § 229.9.
229.125(h)

(h) Any locomotive subject to Part 229, that was built before December 31, 1948, and that is not used regularly in commuter or intercity passenger service, shall be considered historic equipment and excepted from the requirements of paragraphs (d) through (h) of this section.

§229.133 Interim locomotive conspicuity

Remove §229.133(b)(1):

(1) *Ditch lights.* (i) Ditch lights shall consist of two white lights, each producing a steady beam of at least 200,000 candela, placed at the front of the locomotive, at least 36 inches above the top of the rail.

(ii) Ditch lights shall be spaced at least 36 inches apart if the vertical distance from the headlight to the horizontal axis of the ditch lights is 60 inches or more.

(iii) Ditch lights shall be spaced at least 60 inches apart if the vertical distance from the headlight to the horizontal axis of the ditch lights is less than 60 inches.

(iv) Ditch lights shall be focused horizontally within 45 degrees of the longitudinal centerline of the locomotive.

Remove §229.133(b)(3):

(3) *Crossing lights.* (i) Crossing lights shall consist of two white lights, placed at the front of the locomotive, at least 36 inches above the top of the rail.

(ii) Crossing lights shall be spaced at least 36 inches apart if the vertical distance from the headlight to the horizontal axis of the ditch lights is 60 inches or more.

(iii) Crossing lights shall be spaced at least 60 inches apart if the vertical distance from the headlight to the horizontal axis of the ditch lights is less than 60 inches.

(iv) Each crossing light shall produce at least 200,000 candela, either steadily burning or alternately flashing.

(v) The flash rate of crossing lights shall be at least 40 flashes per minute and at most 180 flashes per minute.

(vi) Crossing lights shall be focused horizontally within 15 degrees of the longitudinal centerline of the locomotive.

* * * * *

§229.20 Electronic record keeping

(a) For purposes of compliance with the recordkeeping requirements of this part, except for the cab copy of Form FRA F 6180-49-A required under 229.23 and records required under 229.9, a railroad may create, maintain, and transfer any of the records required by this part through electronic transmission, storage, and retrieval provided that all of the requirements contained in this section are met.

(b) Design Requirements. Any electronic record system used to create, maintain, or transfer a record required to be maintained by this part shall meet the following design parameters:

(1) The electronic record system shall be designed such that the integrity of each record maintained through appropriate levels of security such as recognition of an electronic signature, or other means, which uniquely identify the initiating person as the author of that record. No two persons shall have the same electronic identity;

(2) The electronic system shall ensure that each record cannot be modified, or replaced, once the record is transmitted;

(3) Any amendment to a record shall be electronically stored apart from the record which it amends. Each amendment to a record shall uniquely identify the person making the amendment;

(4) The electronic system shall provide for the maintenance of inspection records as originally submitted without corruption or loss of data; and

(5) Policies and procedures shall be in place to prevent persons from altering electronic records, or otherwise interfering with the electronic system.

(c) Operational Requirements. Any electronic record system used to create, maintain, or transfer a record required to be maintained by this part shall meet the following operating parameters:

(1) The electronic storage of any record required by this part shall be initiated by the person performing the activity (inspection or repair) to which the record pertains within 24 hours following the completion of the activity [unless Hours of Service would be violated, then computer shall be designed to prompt the person to input the data as soon as he comes back on duty];

(2) For each locomotive for which records of inspection or maintenance required by this part are maintained electronically, the electronic record system shall automatically notify the railroad each time the locomotive is due for an inspection, other than the daily inspection, or maintenance that the electronic system is tracking and that is required by this part.

(d) Accessibility and Availability. Any electronic record system used to create, maintain, or transfer a record required to be maintained by this part shall meet the following access and availability parameters:

(1) The carrier shall provide FRA and state inspectors with all electronic records maintained for compliance with this part for any specific locomotives at any mechanical department terminal upon request by FRA;

(2) Paper copies of electronic records and amendments to those records, that may be

necessary to document compliance with this part, shall be provided to the FRA for inspection and copying upon request. Paper copies shall be provided to the FRA no later than 15 days from the day the request is made;

(3) Inspection records required by this part shall be available to persons who performed the inspection and to persons performing subsequent inspections on the same locomotive.

* * * * *

Subpart E Locomotive Electronics

§ 229.X1 Purpose and scope.

(a) The purpose of this subpart is to promote the safe design, operation, and maintenance of safety-critical (as defined in § 229.X05.) electronic locomotive systems, subsystems, and components)

(b) Locomotive control systems or their functions that commingle or interface with safety critical processor based signal and train control systems are regulated under 49 CFR 236 Subpart H.

§ 229.X3 Exclusions.

(a) The requirements of this subpart do not apply to electronic locomotive control system products:

1) That are in service as of MONTH_1 DAY_1, YEAR_1. Railroads may continue to implement and use these products. under development, but which are not in service as of MONTH_1 DAY_1,YEAR_1 may be excluded from this subpart if placed in service by MONTH_1, DAY_1, YEAR_2. (YEAR_2 = YEAR_1 + 3) Products under development but not placed in service by MONTH_1 DAY_1, YEAR_2 shall comply with the provisions of this subpart. Railroads and vendors shall identify products under development to FRA within 6 months from the publication of this rule. This exclusion does not apply to products or product changes that result in degradation of safety, or a material increase in safety-critical functionality.

2) During on-track testing within a test facility**.** To obtain FRA approval of on-track testing outside of a test facility, the railroad shall submit a justification that provides:

(a) Adequate information regarding the function and history of the electronic system that it intends to use;
(b) The proposed tests;
(c) The date, time and location of the tests; and,
(d) The safety consequences that will result from operating the system operating for purposes of testing.

§ 22X.X5 Definitions.

As used in this part—

Associate Administrator for Safety means the Associate Administrator for Safety, FRA, or that person's delegate as designated in writing.
Component means an electronic element, device, or appliance (including hardware or software) that is part of a system or subsystem.
Configuration management control plan means a plan designed to ensure that the proper and intended product configuration, including the electronic hardware components and software version, is documented and maintained through the life-cycle of the products in use.
Employer means a railroad, or contractor to a railroad, that directly engages or compensates individuals to perform the duties specified in § 229.X23 (a).
Executive software means software common to all installations of a given electronic product. It generally is used to schedule the execution of the site-specific application programs, run timers, read inputs, drive outputs, perform self-diagnostics, access and check memory, and monitor the execution of the application software to detect unsolicited changes in outputs.
FRA means the Federal Railroad Administration.
Initialization refers to the startup process when it is determined that a product has all required data input and the product is prepared to function as intended.
Materials handling refers to explicit instructions for handling safety-critical components established to comply with procedures specified by the railroad.
New or next-generation locomotive control system means a locomotive control system using technologies or combinations of technologies not in use in revenue service at the date of this regulation or without established histories of safe practice.
Product means any safety critical electronic locomotive control system processor-based system, subsystem, or component.
Safety Analysis refers to a formal set of documentation which describes in detail all of the safety aspects of the product, including but not limited to procedures for its development, installation, implementation, operation, maintenance, repair, inspection, testing and modification, as well as analyses supporting its safety claims.
Railroad means any form of non-highway ground transportation that runs on rails or electromagnetic guide ways and any entity providing such transportation, including:

(a) Commuter or other short-haul railroad passenger service in a metropolitan or suburban area and commuter railroad service that was operated by the Consolidated Rail Corporation on January 1, 1979; and

(b) High speed ground transportation systems that connect metropolitan areas, without regard to whether those systems use new technologies not associated with traditional railroads; but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation.

Revision control means a chain of custody regimen designed to positively identify safety-critical components and spare equipment availability, including repair/replacement tracking.
Safety-critical, as applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel or equipment, or both; or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist.
Subsystem means a defined portion of a system.
System refers to any electronic locomotive control system and includes all subsystems and components thereof, as the context requires.

Test facility means a track that is not part of the general railroad system of transportation and is being used exclusively for the purpose of testing equipment and has all of its public grade crossings protected.

§ 229.X7 Safety Analysis (SA)

(a) The SA shall:

1) establish and document the minimum requirements that will govern the development and implementation of all products subject to this subpart, and be based on good engineering practice and should address items discussed in Appendix F of this subpart establish that a product's safety-critical functions will operate with a high degree of confidence in a fail-safe manner prior to initial use;
2) include procedures for immediate repair of safety-critical functions; and,
3) be made available to FRA upon request.

(b) Each railroad shall:

1) ensure there is a complete an SA for each new or next generation safety-critical electronic locomotive product or product change in use on their property; and,
2) comply with the SA requirements and procedures for the development, implementation, and repair.

§ 229.X8 Waivers

(a) A person subject to a requirement of this part may petition the Administrator for a waiver of compliance with such requirement. The filing of such a petition does not affect the person's responsibility for compliance with that requirement while the petition is being considered.

(b) Each petition for waiver under this section shall be filed in the manner and contain the information required by part 211 of this chapter.

(c) If the Administrator finds that a waiver of compliance is in the public interest and is consistent with railroad safety, the Administrator may grant the waiver subject to any conditions the Administrator deems necessary.

§ 229.X9 Safety Critical Hardware and Software Changes (Reporting requirements)

(a) The railroad shall:

1) immediately notify FRA of any and all electronic system safety critical changes;
2) conduct all safety critical changes in a manner that allows the change to be audited;
3) specify all contractual arrangements with suppliers and private equipment owners for immediate notification of any and all electronic system safety critical changes to their system, subsystem, or components, and the reasons for such changes from the suppliers or equipment owners, whether or not the railroad has experienced a failure of that safety critical system, sub-system, or component;

4) specify the railroad's procedures for action upon notification of a safety-critical change to the electronic system, sub-system, or component, and until the upgrade, patch, or revision has been installed; and,
5) identify all configuration/revision control measures designed to ensure that safety- functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change, and that any such change can be audited.
    (i.) Product suppliers and private equipment owners shall immediately report any previously unidentified hazards to each railroad using the product.
    (ii.) Private equipment owners shall establish configuration/revision control measures.

§ 229.X11 FRA Preliminary Review and Performance Audit of SAs

(a) Prior to the initial planned use of a new or next generation product, the railroad shall inform the Associate Administrator for Safety, FRA**,** 1200 New Jersey Avenue SE,. Mail Stop 25, Washington, DC 20590 of the intent to place this product in service. The notification shall provide a description of the product, and identify the location where the complete SA documentation as described in § 229.X07 and the training program of § 229.X25 is maintained.
(b) FRA may choose to review and/or audit the SA within 60 days of receipt of the notification or anytime after the product is placed in use.

§ 229.X13 Retention of records.

(a) The railroad shall:
    (1) make available adequate documentation to demonstrate that the product meets the safety requirements of the SA for the life-cycle of the product;
    (2) maintain an Operations and Maintenance Manual pursuant to § 229.X17 at a designated location on the railroad ; and,
    (3) maintain training records pursuant to § 229.X19 at a designated location on the railroad.
(b) Contractors shall maintain training records pursuant to § 229.X21 at a designated office.
(c) Results of required inspections and tests shall be recorded and maintained as prescribed in § 229.X15.
(d) After the product is placed in service, the railroad shall maintain a database of all safety relevant hazards encountered with the product. The database shall include all hazards identified in the SA and those that had not been previously identified in the SA. If the frequency of the safety-relevant hazards exceeds the threshold set forth in the SA then the railroad shall:

(1) Report the inconsistency in writing (by mail, facsimile, e-mail, or hand delivery to the Director, Office of Safety Assurance and Compliance, FRA, 1200 New Jersey Ave SE Mail Stop 25, Washington, DC 20590, within 15 days of discovery.
(2) Take immediate countermeasures to reduce the frequency of the safety relevant hazard(s) below the threshold set forth in the SA, and
(3) Provide a final report to the FRA Director, Office of Safety Assurance and Compliance, on the results of the analysis and countermeasures taken to reduce the frequency of the safety relevant hazard(s) below the calculated probability of failure threshold set forth in the SA when the problem is resolved. For hazards not identified in the SA the threshold shall be exceeded at one occurrence.

§ 229.X15 Results of tests and training.

(a) Results of equipment testing and employee training conducted in compliance with this subpart shall be recorded on preprinted forms provided by the railroad, or stored electronically. Electronic record keeping is subject to the FRA Associate Administrator for Safety's approval.
(b) These records shall contain the:
(1) name of the railroad;
(2) location and date that the test or training was conducted;
(3) equipment tested;
(4) results of tests;
(5) repairs or replacement of equipment;
(6) preventative adjustments made; and,
(7) condition in which the equipment is left.
(c) Each record shall be:
(a) signed by the employee conducting the test, or electronically coded, or identified by the automated test equipment number;
(b) unless otherwise noted, filed in the office of a supervisory official having jurisdiction; and
(c) available for inspection and replication by FRA and FRA-certified State inspectors.
(d) Results of tests and training made in compliance with this subpart shall be retained as follows:
(a) results of tests that pertain to installation or modification shall be retained for the life-cycle of the equipment tested and may be kept in any office designated by the railroad
(b) results of periodic tests required for maintenance or repair of the equipment tested shall be retained until the next record is filed and in no case less than one year.
(c) results of all other tests and training shall be retained until the next record is filed and in no case less than one yea
(d) Electronic or automated tracking systems used to meet the requirements contained in paragraph (a) of this section shall **be** capable of being reviewed and monitored by FRA at any time to ensure the integrity of the system. FRA's Associate Administrator for Safety may prohibit or revoke a railroad's authority to utilize an electronic or automated tracking system in lieu of preprinted forms if FRA finds that the electronic or automated tracking system is not properly secured, is inaccessible to

FRA, FRA-certified State inspectors, or railroad employees requiring access to discharge their assigned duties, or fails to adequately track and monitor the equipment. The Associate Administrator for Safety will provide the affected railroad with a written statement of the basis for the decision prohibiting or revoking the railroad from utilizing an electronic or automated tracking system.

§ 229.X17 Operations and Maintenance Manual.

(a) The railroad shall maintain all documents pertaining to the installation, maintenance, repair, modification, inspection, and testing of the product in one Operations and Maintenance Manual (OMM).
   (1) The OMM shall be readily available to persons who conduct the installation, maintenance, repair, modification, inspection, and testing, and for inspection by FRA and FRA-certified State inspectors
   (2) At a minimum, the OMM shall reflect all product vendor operation and maintenance guidance

(b) Plans required for proper maintenance, repair, inspection, and testing of safety-critical products shall contain adequate detail and be made available for inspection by FRA and FRA-certified State inspectors when such products are placed in use or maintained.
   The plans shall identify all software versions, revisions, and revision dates.
   The plans shall be legible and correct.
   (1) Hardware, software, and firmware revisions shall be documented in the OMM according to the railroad's configuration management control plan.
   (2) Safety-critical components, including spare equipment, shall be positively identified, handled, replaced, and repaired in accordance with the procedures specified in the railroad's configuration management control plan.

(c) The railroad shall determine, prior to placing the product in use on their property that the requirements of this section have been met and shall make available the necessary analyses and documentation as required in this subpart for review and audit by the FRA upon the request of the FRA.

§ 229.X19 Training and qualification program.

(a) Employers shall establish and implement training and qualification programs for products subject to this subpart. These programs shall meet the minimum requirements set forth in §§ 229.X17 through 229.X23 for:
   (1) persons whose duties include installing, maintaining, repairing, modifying, inspecting, and testing safety-critical elements of the product, systems, and/or subsystems;
   (2) persons who operate trains or serve as a train or engine crew member subject to instruction and testing under part 217 of this chapter;
   (3) roadway and maintenance of way workers whose duties require them to know and understand how the locomotive control system affects their safety and how to avoid interfering with its proper functioning; and

(4) the direct supervisors of persons listed in paragraphs (a)(1) through (a)(3) of this section.

(b) The employer's program shall provide training for persons who perform the functions described in paragraph (a) of this section to ensure that they have the necessary knowledge and skills to effectively complete their duties related to locomotive control systems.

§ 229.X21 Task analysis and basic requirements.

(a) For program required by § 229.X21, employers shall:

(1) identify the specific goals of the training program for each target population (craft, experience level, scope of work, etc.), task(s), and desired success rate;

(2) based on a formal task analysis, identify the installation, maintenance, repair, modification, inspection, testing, and operating tasks that shall be performed on a railroad's products, including but not limited to the development of failure scenarios and the actions expected under such scenarios;

(3) develop written procedures for the performance of the tasks identified;

(4) identify the additional knowledge, skills, and abilities above those required for basic job performance necessary to perform each task;

(5) develop a training curriculum that includes formally structured training designed to impart the knowledge, skills, and abilities identified as necessary to perform each task;

(6) prior to assignment of related tasks, require all persons identified in § 29.X21(a) to successfully complete a training curriculum and pass an examination that covers the product and appropriate rules and tasks for which they are responsible (however, such persons may perform such tasks under the direct onsite supervision of a qualified person prior to completing such training and passing the examination);

(7) Except with respect to basic skills for which proficiency is known to remain high as a result of frequent repetition of the task, require periodic refresher training at intervals to be formally specified**;** and

(8) conduct regular and periodic evaluations of the effectiveness of the training program specified in § 229.X**19**(a) verifying the adequacy of the training material and its validity with respect to current railroads products and operations.

(b) employers shall retain records which designate persons who are qualified under this section until new designations are recorded or for at least one year after such persons leave applicable service. These records shall be kept in a designated location and be available for inspection and replication by FRA and FRA-certified State inspectors.

§ 229.X23-Training specific to locomotive engineers and other operating personnel.

(a) Training provided under this subpart for any locomotive engineer or other person who participates in the operation of a train using an onboard electronic locomotive control system shall be formally specified in writing, and shall address the following**:**

(1) familiarization with the electronic control system equipment onboard the locomotive and the functioning of that equipment as part of the system and in relation to other onboard systems under that person's control;

(2) any actions required of the operating personnel to enable or enter data into the system and the role of that function in the safe operation of the train;

(3) sequencing of interventions by the system, including notification, enforcement, penalty initiation and post penalty application procedures as applicable;

(4) railroad operating rules applicable to control systems, including provisions for movement and protection of any unequipped trains, or trains with failed or cut-out controls;

(5) means to detect deviations from proper functioning of onboard electronic control system equipment and instructions explaining the proper response to be taken regarding control of the train and notification of designated railroad personnel; and,

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

(b) training required under this subpart for a locomotive engineer, together with required records, shall be integrated into the program of training required by 49 CFR part 240.

* * * * *

Appendix F to Part 229—Recommended Practices for Design and Safety Analysis

The purpose of this appendix is to provide recommended criteria for design and safety analysis that will maximize the safety of electronic locomotive control systems and mitigate potential negative safety effects. It seeks to promote full disclosure of potential safety risks to facilitate minimizing or eliminating elements of risk where practicable. It discuses critical elements of good engineering practice that the designer should consider when developing safety critical electronic locomotive control systems to accomplish this objective. The criteria and processes specified this appendix are intended to minimize the probability of failure to an acceptable level within the limitations of the available engineering science, cost, and other constraints. Railroads procuring safety critical electronic locomotive controls are encouraged to ensure that their vendor addresses each of the elements of this appendix in the design of the product being procured. FRA uses the criteria and processes set forth in this appendix (or other technically equivalent criteria and processes that may be recommended by industry) when evaluating analyses, assumptions, and conclusions provided in the SA documents.

Definitions

In addition to the definitions of §229.X03, the following definitions are applicable to this Appendix:

Hazard means an existing or potential condition that can result in an accident.

High degree of confidence, as applied to the highest level of aggregation, means there exists credible safety analysis supporting the conclusion that the risks associated with the product have been adequately mitigated.

Human factors refers to a body of knowledge about human limitations, human abilities, and other human characteristics, such as behavior and motivation, that shall be considered in product design.
Human-machine interface (HMI) means the interrelated set of controls and displays that allows humans to interact with the machine.
Risk means the expected probability of occurrence for an individual accident event (probability) multiplied by the severity of the expected consequences associated with the accident (severity).
Risk assessment means the process of determining, either quantitatively or qualitatively, the measure of risk associated with use of the product under all intended operating conditions.
System Safety Precedence means the order of precedence in which methods used to eliminate or control identified hazards within a system are implemented.
Validation means the process of determining whether a product's design requirements fulfill its intended design objectives during its development and life-cycle. The goal of the validation process is to determine ''whether the correct product was built.''
Verification means the process of determining whether the results of a given phase of the development cycle fulfill the validated requirements established at the start of that phase. The goal of the verification process is to determine ''whether the product was built correctly.''

Safety Assessment Contents

The safety-critical assessment of each product should include all of its interconnected subsystems and components and, where applicable, the interaction between such subsystems. It should contain, at a minimum, the following:

(a) A complete description of the product, including a list of all product components and their physical relationship in the subsystem or system;
(a) A description of the railroad operation or categories of operations on which the product is designed to be used;
(b) An operational concepts document, including a complete description of the product functionality and information flows;
(c) A safety requirements document, including a list with complete descriptions of all functions, which the product performs to enhance or preserve safety, and that describes the manner in which product architecture satisfies safety requirements;
(d) A hazard log consisting of a comprehensive description of all safety relevant hazards addressed during the life cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence);

The analysis should document any assumptions regarding the reliability or availability of mechanical, electric, or electronic components. Such assumptions 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 analysis shall document these assumptions in such a form as to permit later automated comparisons with in-service experience (e.g., a spreadsheet).

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

The analysis should 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 should be documented in such a form as to permit later automated comparisons with in-service experience.

The analysis should 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.

(e) A risk assessment;

The risk metric for the proposed product should describe with a high degree of confidence the accumulated risk of a locomotive control system that operates over a life-cycle of 25 years or greater. Each risk metric for the proposed product should be expressed with an upper bound, as estimated with a sensitivity analysis, and the risk value selected is demonstrated to have a high degree of confidence.

Each risk calculation should consider the totality of the locomotive control system and its method of operation. The failure modes of each subsystem or component, or both, should be determined for the integrated hardware/ software (where applicable) as a function of the Mean Time to Hazardous Events (MTTHE), 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, should also be considered.

An MTTHE value should 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 should be included in the assessment, whenever applicable, to provide an integrated MTTHE value. The MTTHE calculation should 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.

MTTHE compliance verification and validation should 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 shall be demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to have a high degree of confidence.

The safety-critical behavior of all non-processor based components, which are part of a processor-based system or subsystem, should be quantified with an MTTHE metric. The MTTHE assessment methodology should 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. The MTTHE compliance verification and validation should 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 should also be demonstrated to have a high degree of confidence.

(f) A hazard mitigation analysis, including a complete and comprehensive description of all hazards to be addressed in the system design and development, mitigation techniques used, and system safety precedence followed;

(g) A complete description of the safety assessment and verification and validation processes applied to the product and the results of these processes;

(h) A complete description of the safety assurance concepts used in the product design, including an explanation of the design principles and assumptions;The designer should address each of the following safety considerations when designing and demonstrating the safety of products covered by this part. In the event that any of these principles are not followed, the analysis shall describe both the reason(s) for departure and the alternative(s) utilized to mitigate or eliminate the hazards associated with the design principle not followed.

Normal operation. The system (including all hardware and software) shall 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 shall be performed properly under these normal conditions. Absence of specific operator actions or procedures will not prevent the system from operating safely. There shall be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable shall be eliminated by design.

Systematic failure. It shall 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.

Random failure. The product shall 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 shall be considered in the hazard analysis There should 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 shall be detected and the product shall achieve a known safe state before falsely activating any physical appliance. 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 shall be detected and the product shall achieve a known safe state before falsely activating any physical appliance.

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 shall be ensured in these instances. When dealing with the effects of hardware failure, the designer should 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.

External influences. The product should operate safely when subjected to different external influences, including:

-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;
-Mechanical influences such as vibration and shock; and Climatic conditions such as temperature and humidity.

Modifications. Safety shall be ensured following modifications to the hardware or software, or both. All or some of the concerns previously identified may be applicable depending upon the nature and extent of the modifications.

Software. Software faults shall not cause hazards categorized as unacceptable or undesirable.

Closed Loop Principle. The product design shall require positive action to be taken in a prescribed manner to either begin product operation or continue product operation.

(i) A human factors analysis, including a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the product to enhance or preserve safety, and an analysis of the physical ergonomics of the product on the operators and the safe operation of the system;
(j) A complete description of the specific training of railroad and contractor employees and supervisors necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product;
(k) A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, test, and modification of the product. These procedures, including calibration requirements, should be consistent with or explain deviations from the equipment manufacturer's recommendations;
(l) A complete description of the necessary security measures for the product over its life-cycle;
(m) A complete description of each warning to be placed in the Operations and Maintenance Manual identified in § 229.X23, and of all warning labels required to be placed on equipment as necessary to ensure safety;
(n) A complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated;

(o) A complete description of:

All post-implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety-critical tolerances are not compromised over time, through use, or after maintenance (repair, replacement, adjustment) is performed; and

Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety relevant hazards;

(p) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and
(q) The configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any change. Changes classified as maintenance require validation.

Human Factors in Design

The product design should sufficiently incorporate human factors engineering that is appropriate to the complexity of the product; the gender, 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. HMI design criteria will minimize negative safety effects by causing designers to consider human factors in the development of HMIs. 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 this part, and ‘‘operator’’ means any human who is intended to receive information from, provide information to, or perform repairs or maintenance on a safety critical locomotive control product subject to this part.

System designers should:

(a) Design systems that anticipate possible user errors and include capabilities to catch errors before they propagate through the system;
(b) Conduct cognitive task analyses prior to designing the system to better understand the information processing requirements of operators when making critical decisions; and
(c) Present information that accurately represents or predicts system states.
(d) Ensure that electronics equipment radio frequency emissions are compliant with appropriate Federal Communications Commission regulations. The FCC rules and regulations are codified in Title 47 of the Code of Federal Regulations (CFR) as follows:

Electronics equipment shall be have appropriate FCC Equipment Authorizations. The following documentation is applicable to obtaining FCC Equipment Authorization:

(a) *OET Bulletin Number 61 (October, 1992 Supersedes May, 1987 issue) FCC Equipment Authorization Program for Radio Frequency Devices* This document provides an overview of the equipment authorization program to control radio interference from radio transmitters and certain other electronic products. And how to obtain an equipment authorization.
(b) *OET Bulletin 63: (October 1993)Understanding The FCC Part 15 Regulations for Low Power, Non-Licensed Transmitters.* This document provides a basic understanding of the FCC regulations for low power, unlicensed transmitters, and includes answers to some commonly-asked questions. This edition of the bulletin does not contain information concerning personal communication services (PCS) transmitters operating under Part 15, Subpart D of the rules.
(c) *47 Code of Federal Regulations Parts 0 to 19.* The FCC rules and regulations governing PCS transmitters may be found in 47 CFR, Parts 0 to 19.
(d) *OET Bulletin 62 (December 1993) Understanding The FCC Regulations for Computers and other Digital Devices* This document has been prepared to provide a basic understanding of the FCC regulations for digital (computing) devices, and includes answers to some commonly-asked questions

Human factors issues the designers should consider with regard to the general function of a system include

Reduced situational awareness and over-reliance. HMI design shall 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 shall be ''in-the loop.'' Designers should consider at minimum the following methods of maintaining an active role for human operators:

(a) The system shall 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;
(b) The system shall 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;
(c) The system shall warn operators in advance when they require an operator to take action; and
(d) HMI design shall equalize an operator's workload.
(e) HMI design shall not distract from the operator's safety related duties.

Expectation of predictability and consistency in product behavior and communications. HMI design shall accommodate an operator's expectation of logical and consistent relationships between actions and results. Similar objects shall behave consistently when an operator performs the same action upon them. End Users have a Limited memory and ability to process information. HMI design shall therefore 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.

To minimize short-term memory load, the designer should 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.

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

When creating displays and controls, the designer shall consider user ergonomics and should

(a) Locate displays as close as possible to the controls that affect them;
(b) Locate displays and controls based on an operator's position;
(c) Arrange controls to minimize the need for the operator to change position;
(d) Arrange controls according to their expected order of use;
(e) Group similar controls together;
(f) Design for high stimulus-response compatibility (geometric and conceptual);
(g) 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
(h) Design controls to allow easy recovery from error.
(i) Design display and controls to reflect specific gender and physical limitations of the intended operators.

Detailed locomotive ergonomics human machine interface guidance may be found in "Human Factors Guidelines for Locomotive Cabs" (FRA/ORD-98/03 or DOT-VNTSC-FRA-98-8)

The designer should also address information management. To that end, HMI design should:

(a) Display information in a manner which emphasizes its relative importance;
(b) Comply with the ANSI/HFS 100–1988 standard;
(c) Utilize a display luminance that has a difference of at least 35cd/m2 between the foreground and background (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);
(d) Display only the information necessary to the user;
(e) Where text is needed, use short, simple sentences or phrases with wording that an operator will understand and appropriate to the educational and cognitive capabilities of the intended operator;
(f) 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;
(g) Adopt a consistent format for all display screens by placing each design element in a consistent and specified location;
(h) 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;
(i) Group items that belong together;
(j) 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;
(k) Limit the number of colors over a group of displays to no more than seven;
(l) Design warnings to match the level of risk or danger with the alerting nature of the signal; and

(m) With respect to information entry, avoid full QWERTY keyboards for data entry.

With respect to problem management, the HMI designer should ensure that the:

(a) HMI design shall enhance an operator's situation awareness.
(b) HMI design shall support response selection and scheduling.
(c) HMI design shall support contingency planning.

Designers shall comply with FCC requirements for Maximum Permissible Exposure limits for field strength and power density for the transmitters operating at frequencies of 300 kHz to 100 GHz and specific absorption rate (SAR) limits for devices operating within close proximity to the body. The Commission's requirements are detailed in Parts 1 and 2 of the FCC's Rules and Regulations [47 C.F.R. 1.1307(b), 1.1310, 2.1091, 2.1093

The FCC has prepared

(a) OET Bulletin No. 65 (Edition 97-01,August 1997), "Evaluating Compliance With FCC Guidelines For Human Exposure To Radiofrequency Electromagnetic Fields",
(b) OET Bulletin No 65 Supplement A, (Edition 97-01, August 1997), OET Bulletin No 65 Supplement B (Edition 97-01, August 1997) And
(c) OET Bulletin No 65 Supplement C (Edition 01-01, June 2001)

To provide assistance in determining whether proposed or existing transmitting facilities, operations or devices comply with limits for human exposure to radiofrequency RF fields adopted by the FCC

The bulletin and supplements offers guidelines and suggestions for evaluating compliance. However, it is not intended to establish mandatory procedures, other methods and procedures may be acceptable if based on sound engineering practice.

Verification and Validation

The goal of this assessment is to provide an 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 requirements, the requirements of this part, and any other previously agreed-upon controlling documents or standards. The standards employed for verification or validation, or both, of products shall be sufficient to support achievement of the applicable requirements of this part.

The latest version of the following standards have been recognized by FRA as providing appropriate risk analysis processes for incorporation into verification and validation standards.

(a) U.S. Department of Defense Military Standard (MIL-STD) 882C, ‘‘System Safety Program Requirements’’ (January 19, 1993),

(b) CENELEC Standards as follows:
   (1) EN50126: 1999, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);
   (2) EN50128 (May 2001), Railway Applications: Software for Railway Control and Protection Systems;
   (3) EN50129: 2003, Railway Applications: Communications, Signaling, and Processing Systems-Safety Related Electronic Systems for Signaling; and
   (4) EN50155:2001/A1:2002, Railway Applications: Electronic Equipment Used in Rolling Stock.

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

(d) ATCS Specification 130, Software Quality Assurance.

(e) 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.

(f) IEC 61508 (International Electro-technical Commission), Functional Safety of Electrical/Electronic/ Programmable/Electronic Safety (E/E/P/ES) Related Systems, Parts 1–7 as follows:
   (1) IEC 61508–1 (1998–12) Part 1: General requirements and IEC 61508–1 Corr. (1999–05) Corrigendum 1-Part 1:General Requirements.
   (2) IEC 61508–2 (2000–05) Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems.
   (3) IEC 61508–3 (1998–12) Part 3: Software requirements and IEC 61508–3 Corr.1(1999–04) Corrigendum 1-Part3: Software requirements.
   (4) 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.
   (5) 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.
   (6) IEC 61508–6 (2000–04) Part 6: Guidelines on the applications of IEC 61508–2 and –3.
   (7) IEC 61508–7 (2000–03) Part 7: Overview of techniques and measures.

When using unpublished standards, including proprietary standards, the standards should be available for inspection and replication by the railroad and FRA and for public examination in any public proceeding before the FRA to which they are relevant

The railroad, the supplier, or FRA may conclude it is necessary for a third party assessment of the system. A third party assessor should be “independent”. An

"independent third party" means a technically competent entity responsible to and compensated by the railroad (or an association on behalf of one or more railroads) that is independent of the supplier of the product. An entity that is owned or controlled by the supplier, that is under common ownership or control with the supplier, or that is otherwise involved in the development of the product would not be considered "independent".

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. The supplier should provide the reviewer access to any, and all, documentation that the reviewer requests and attendance at any design review or walk through that the reviewer determines as necessary to complete and accomplish the third party assessment. Representatives from FRA or the railroad might accompany the reviewer.

Third party reviews can occur at a preliminary level a functional level, or implementation level. At the preliminary level, the reviewer should 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 should compare the supplier processes with industry best practices to determine if the vendor methodology is acceptable and employ any other such tests or comparisons if they have been agreed to previously with the railroad or FRA. Based on these analyses, the reviewer shall identify and document any significant safety vulnerabilities that are not adequately mitigated by the supplier's (or user's) processes. At the functional level, the reviewer evaluates the adequacy, and comprehensiveness, of the safety analysis, and any other documents pertinent to the product being assessed for completeness, correctness, and compliance with applicable standards. This includes, but is not limited to the Preliminary Hazard Analysis (PHA), all Fault Tree Analyses (FTA), all Failure Mode and Effects Criticality Analysis (FMECA), and other hazard analyses At the implementation level the reviewer randomly selects various safety-critical software modules for audit to verify whether the system process and design requirements were followed. The number of modules audited shall be determined as a representative number sufficient to provide confidence that all un-audited modules were developed in similar manner as the audited module. During this phase the reviewer would also evaluate and comment on the adequacy of the plan for installation and test of the product for revenue service.

Upon completion of an assessment, the reviewer prepares a final report of the assessment. The report contain at least the following information:

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

(b) 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 or vendor assure that all potentially hazardous failure modes are identified?) and the method by which the railroad or vendor addresses comprehensiveness of the

product design for the requirements of the operations it will govern (i.e., how does the railroad and/or vendor 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?);

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

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

(e) A listing of each design procedure or process which was not properly followed;

(f) 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;

(g) 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

(h) Method by which the supplier or railroad addresses comprehensiveness of the product design which considers the safety elements.