

§ 238.105

railroad's operating environment and the material's size, or location, or both; or

(B) The railroad takes alternative action which reduces the risk of personal injuries to an acceptable level.

(4) Where possible prior to transferring existing equipment to a new category of service, but in no case more than 90 days following such a transfer, the passenger railroad shall complete a new fire safety analysis taking into consideration the change in railroad operations and shall effect prompt action to reduce any identified risk to an acceptable level.

(5) As used in this paragraph, "category of rail equipment and current rail service" shall be determined by the railroad based on relevant fire safety risks, including available ignition sources, presence or absence of heat/smoke detection systems, known variations from the required material test performance criteria or alternative standards approved by FRA, and availability of rapid and safe egress to the exterior of the vehicle under conditions secure from fire, smoke, and other hazards.

(e) *Inspection, testing, and maintenance.* Each railroad shall develop and adopt written procedures for the inspection, testing, and maintenance of all fire safety systems and fire safety equipment on the passenger equipment it operates. The railroad shall comply with those procedures that it designates as mandatory for the safety of the equipment and its occupants.

§ 238.105 Train hardware and software safety.

These requirements of this section apply to hardware and software used to control or monitor safety functions in passenger equipment ordered on or after September 8, 2000, and such components implemented or materially modified in new or existing passenger equipment on or after September 9, 2002.

(a) The railroad shall develop and maintain a written hardware and software safety program to guide the design, development, testing, integration, and verification of computer software and hardware that controls or monitors equipment safety functions.

(b) The hardware and software safety program shall be based on a formal safety methodology that includes a Failure Modes, Effects, Criticality Analysis (FMECA); verification and validation testing for all hardware and software components and their interfaces; and comprehensive hardware and software integration testing to ensure that the software functions as intended.

(c) Under the hardware and software safety program, software that controls or monitors safety functions shall be considered safety-critical unless a completely redundant, failsafe, non-software means ensuring the same function is provided. The hardware and software safety program shall include a description of how the following will be accomplished, achieved, carried out, or implemented to ensure software safety and reliability:

- (1) The software design process;
- (2) The software design documentation;
- (3) The software hazard analysis;
- (4) Software safety reviews;
- (5) Software hazard monitoring and tracking;
- (6) Hardware and software integration safety tests; and
- (7) Demonstration of overall software safety as part of the pre-revenue service tests of equipment.

(d) Hardware and software that controls or monitors passenger equipment safety functions shall include design feature(s) that result in a safe condition in the event of a computer hardware or software failure.

(e) The railroad shall comply with the elements of its hardware and software safety program that affect the safety of the passenger equipment.

§ 238.107 Inspection, testing, and maintenance plan.

(a) *General.* Beginning on January 1, 2002, the following provisions of this section apply to railroads operating Tier I passenger equipment covered by this part. A railroad may request earlier application of these requirements upon written notification to FRA's Associate Administrator for Safety as provided in § 238.1(c).