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

(H) IEC 62278: 2002, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(I) IEC 62279: 2002 Railway Applications: Software for Railway Control and Protection Systems;

(4) Use of unpublished standards, including proprietary standards, is authorized to the extent that such standards are shown to achieve the requirements of this part.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.

(5) The various standards provided in this paragraph are for illustrative purposes only. Copies of these standards can be obtained in accordance with the following:

(i) U.S. government standards and technical publications may be obtained by contacting the federal National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312.

(ii) U.S. National Standards may be obtained by contacting the American National Standards Institute, 25 West 43rd Street, 4 Floor, New York, NY 10036.

(iii) IEC Standards may be obtained by contacting the International Electrotechnical Commission, 3, rue de Varembé, P.O. Box 131 CH—1211, GENEVA, 20, Switzerland.

(iv) CENLEC Standards may be obtained by contacting any of one the national standards bodies that make up the European Committee for Electrotechnical Standardization.

(v) IEEE standards may be obtained by contacting the IEEE Publications Office, 10662 Los Vaqueros Circle, P.O. Box 3014, Los Alamitos, CA 90720–1264.

(vi) AREMA standards may be obtained from the American Railway Engineering and Maintenance-of-Way Association, 10003 Derekwood Lane, Suite 210, Lanham, MD 20706.

[75 FR 2718, Jan. 15, 2010]

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

(a) This appendix provides minimum requirements for independent third-party assessment of product safety verification and validation pursuant to subpart H or subpart I 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 any mutually agreed upon controlling documents and standards and the applicable railroad's:

(1) Railroad Safety Program Plan (RSPP) and Product Safety Plan (PSP) for processor based systems developed under subpart H or,

(2) PTC Product Development Plan (PTCDP) and PTC Safety Plan (PTCSP) for PTC systems developed under subpart I.

(b) 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 shall not engage in any design efforts associated with the product, the products subsystems, or the products components, in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the product.

(c) 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.

(d) The reviewer shall evaluate the product 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 validation and verification 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 and document the adequacy of the railroad's

(1) RSPP, the PSP, and any other documents pertinent to a product being developed under subpart H of this part; or

(2) PTCDP and PTCSP for systems being developed under subpart I of this part.

(e) The reviewer shall analyze the Hazard Log and/or any other hazard analysis documents for comprehensiveness and compliance with applicable railroad, vendor, supplier, industry, national, and international standards.

(f) 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 applicable railroad, vendor, supplier, industry, national and international standards.

(g) The reviewer shall randomly select various safety-critical software, and hardware modules, if directed by FRA, for audit to verify whether the requirements of the applicable railroad, vendor, supplier, industry, national, and international standards 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 applicable railroad, vendor, supplier, industry, national, and international standards.

(h) The reviewer shall evaluate and comment on the plan for installation and test procedures of the product for revenue service.

(i) 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:

(1) Reviewer's evaluation of the adequacy of the PSP in the case of products developed under subpart H, or PTCSP for products developed under subpart I of this part, including the supplier's MTTHE and risk estimates for the product, and the supplier's confidence interval in these estimates;

(2) Product vulnerabilities, potentially hazardous failure modes, or potentially hazardous operating circumstances which the reviewer felt were not adequately identified, tracked, mitigated, and corrected by either the vendor or supplier or the railroad;

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

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

(5) A listing of each applicable vendor, supplier, industry, national, or international standard, procedure or process which was not properly followed;

(6) Identification of the software verification and validation procedures, as well as the hardware verification validation procedures if deemed appropriate by FRA, for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(7) Methods employed by the product manufacturer to develop safety-critical software;

(8) If deemed applicable by FRA, the methods employed by the product manufacturer to develop safety-critical hardware by generally acceptable techniques;

(9) 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.

[75 FR 2720, Jan. 15, 2010]

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

(a) This appendix provides human factors design criteria applicable to both subpart H and subpart I of this part. HMI design criteria will minimize negative safety effects by causing designers to consider human factors in the development of HMIs. 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.

(b) 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 or subpart I 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 safety-critical product subject to subpart H or I of this part.

(c) Human factors issues the designers must consider with regard to the general function of a system include:

(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 must consider at a 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 it requires an operator to take action;

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