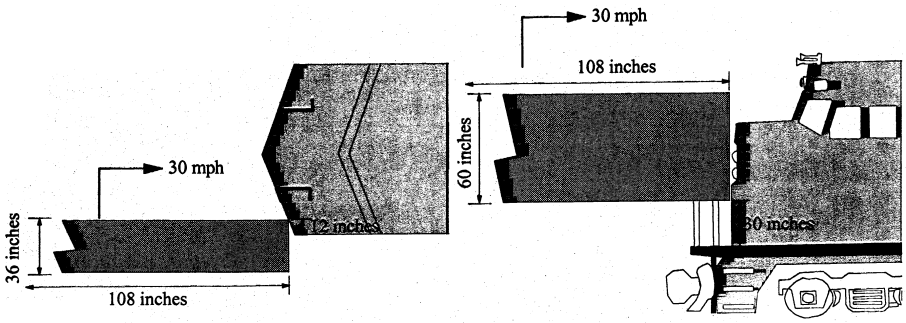

Figure 2. Schematic of Front End Structure (Short Hood) Offset Impact

[71 FR 36915, June 28, 2006]

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 is 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 contained in §229.305, 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 ASSESSMENTS—RECOMMENDED 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. FRA recommends that such assessments contain 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;

(b) A description of the railroad operation or categories of operations on which the product is designed to be used;

(c) An operational concepts document, including a complete description of the product functionality and information flows; as well as identifying which functions are intended to enhance or preserve safety and the manner in which the product architecture implements these functions;

(d) 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;

(e) 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);

(f) A risk assessment and analysis.

(1) 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 the intended product life. 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.

(2) 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.

(3) An MTTHE value should be calculated for each 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.

(4) The analysis should clearly document:

(i) 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. The analysis should document these assumptions in such a form as to permit later comparisons with in-service experience (e.g., a spreadsheet). The analysis should also document any assumptions regarding human performance. The documentation should be in a form that facilitates later comparisons with in-service experience.

(ii) Any assumptions regarding software defects. These assumptions should be in a form which permits the railroad to project the likelihood of detecting an in-service software defect and later comparisons with in-service experience.

(iii) All of the identified safety-critical fault paths leading to a mishap as predicted by the SA. The documentation should be in a form that facilitates later comparisons with in-service faults.

(4) 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.

(5) 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.

(g) 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;

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

(i) 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 should 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.

(1) *Normal operation.* The system (including all hardware and software) should 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 should be performed properly under these normal conditions. Absence of specific operator actions or procedures will not prevent the system from operating safely. Hazards categorized as unacceptable should be eliminated by design. Best effort should also be made by the designer to eliminate hazards that are undesirable. Those undesirable hazards that cannot be eliminated must be mitigated to an acceptable level.

(2) *Systematic failure.* It should 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 phase, or both; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

(3) *Random failure.* The product should 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 should 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 be detected and the product should achieve a known state that eliminates the possibility of false activation of 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 should be detected and the product must achieve a known safe state that eliminates the possibility of false activation.

(4) *Common Mode failure.* Another concern of multiple failures involves common mode failure 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 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.

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

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

(ii) Mechanical influences such as vibration and shock; and climatic conditions such as temperature and humidity.

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

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

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

(j) 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;

(k) 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;

(l) 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;

(m) A complete description of the necessary security measures for the product over its life-cycle;

(n) A complete description of each warning to be placed in the Operations and Maintenance Manual and of all warning labels required to be placed on equipment as necessary to ensure safety;

(o) 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;

(p) 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

(q) A complete description of 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;

(r) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and

(s) 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.

GUIDANCE REGARDING THE APPLICATION OF HUMAN FACTORS IN THE DESIGN OF PRODUCTS

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 minimize negative safety effects by causing designers to consider human factors in the development of HMIs. As used in this discussion, ''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.

I. FRA recommends that 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;

(c) Present information that accurately represents or predicts system states; and

(d) Ensure that electronics equipment radio frequency emissions are compliant with appropriate Federal Communications

Commission (FCC) regulations. The FCC rules and regulations are codified in Title 47 of the Code of Federal Regulations (CFR). The following documentation is applicable to obtaining FCC Equipment Authorization:

(1) *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.

(2) *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.

(3) *Title 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.

(4) *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.

II. Human factors issues designers should consider with regard to the general functioning of a system include:

(a) *Reduced situational awareness and overreliance.* 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:

(1) The system should 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;

(2) The system should 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;

(3) The system should warn operators in advance when they require an operator to take action;

(4) HMI design should equalize an operator's workload; and

(5) HMI design should not distract from the operator's safety related duties.

(b) *Expectation of predictability and consistency in product behavior and communications.* HMI design should accommodate an operator's expectation of logical and consistent relationships between actions and results. Similar objects should behave consistently when an operator performs the same action upon them. End users have a limited memory and ability to process information. Therefore, HMI design should also minimize an operator's information processing load.

(1) To minimize information processing load, the designer should:

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

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

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

(2) 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 should be recalled from unaided memory when making critical decisions, and promote active processing of the information.

(3) When creating displays and controls, the designer shall consider user ergonomics and should:

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

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

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

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

(v) Group similar controls together;

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

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

(viii) Design controls to allow easy recovery from error; and

(ix) Design display and controls to reflect specific gender and physical limitations of the intended operators.

(4) 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).

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

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

(ii) Comply with the ANSI/HFS 100–2007, or more recent standard;

(iii) 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);

(iv) Display only the information necessary to the user;

(v) 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;

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

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

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

(ix) Group items that belong together;

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

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

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

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

(6) With respect to problem management, the HMI designer should ensure that the HMI design:

(i) enhances an operator's situation awareness;

(ii) supports response selection and scheduling; and

(iii) supports contingency planning.

(7) Designers should 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 CFR 1.1307(b), 1.1310, 2.1091, 2.1093). The FCC has a number of bulletins and supplements that offer guidelines and suggestions for evaluating compliance. These documents are not intended to establish mandatory procedures; other methods and procedures may be acceptable if based on sound engineering practice.

(i) OET Bulletin No. 65 (Edition 97–01, August 1997), ''Evaluating Compliance With FCC Guidelines For Human Exposure To Radio frequency Electromagnetic Fields'';

(ii) OET Bulletin No 65 Supplement A, (Edition 97–01, August 1997), OET Bulletin No 65 Supplement B (Edition 97–01, August 1997); and

(iii) OET Bulletin No 65 Supplement C (Edition 01–01, June 2001). This bulletin provides assistance in determining whether proposed or existing transmitting facilities, operations, or devices comply with limits for human exposure to radio frequency RF fields adopted by the FCC.

GUIDANCE FOR VERIFICATION AND VALIDATION OF PRODUCTS

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.

(a) 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.

(1) U.S. Department of Defense Military Standard (MIL–STD) 882C, ''System Safety Program Requirements'' (January 19, 1993);

(2) The most recent CENLE/IEC Standards as follows:

(i) EN50126:/IEC 62278, Railway Applications: Communications, Signaling, and Processing Systems Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(ii) EN50128/IEC 62279, Railway Applications: Communications, Signaling, and Processing Systems Software for Railway Control and Protection Systems;

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

(iv) EN50155, Railway Applications: Electronic Equipment Used in Rolling Stock.

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

(4) ATCS Specification 130, Software Quality Assurance.

(5) 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.

(6) 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:

(i) IEC 61508–1 (1998–12) Part 1: General requirements and IEC 61508–1 Corr. (1999–05) Corrigendum 1–Part 1: General Requirements;

(ii) IEC 61508–2 (2000–05) Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems;

(iii) IEC 61508–3 (1998–12) Part 3: Software requirements and IEC 61508–3 Corr.1(1999–04) Corrigendum 1–Part3: Software requirements;

(iv) 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;

(v) 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;

(vi) 1IEC 61508–6 (2000–04) Part 6: Guidelines on the applications of IEC 61508–2 and –3; and,

(vii) IEC 61508–7 (2000–03) Part 7: Overview of techniques and measures.

(7) ANSI/GEIA–STD–0010: Standard Best Practices for System Safety Program Development and Execution

(b) When using unpublished standards, including proprietary standards, the standards should be available for inspection and replication by the railroad and FRA and should be available for public examination.

(c) *Third party assessments.* 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''.

(1) 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.

(2) 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), the Hazard Log (HL), 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.

(d) *Reviewer Report.* Upon completion of an assessment, the reviewer prepares a final report of the assessment. The report should contain the following information:

(1) The 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;

(2) 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?);

(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 design procedure or process which was not properly followed;

(6) 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;

(7) 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

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

[77 FR 21352, Apr. 9, 2012]

APPENDIX G TO PART 229 [RESERVED]

APPENDIX H TO PART 229—STATIC NOISE TEST PROTOCOLS—IN-CAB STATIC

This appendix prescribes the procedures for the in-cab static measurements of locomotives.

I. MEASUREMENT INSTRUMENTATION

The instrumentation used should conform to the following: An integrating-averaging sound level meter shall meet all the requirements of ANSI S1.43–1997 (Reaffirmed 2002), ''Specifications for Integrating-Averaging Sound Level Meters,'' for a Type 1 Instrument. In the event that a Type 1 instrument is not available, the measurements may be conducted with a Type 2 instrument. The acoustic calibrator shall meet the requirement of the ANSI S1.40–1984 (Reaffirmed 2001), ''Specification for Acoustical Calibrators.'' The Director of the Federal Register approves the incorporation by reference of ANSI S1.43–1997 (Reaffirmed 2002) and ANSI S1.40–1984 (Reaffirmed 2001) in this section in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of the incorporated standards from the American National Standards Institute at 1819 L Street, NW., Washington, DC 20036 or *http://www.ansi.org*. You may inspect a copy of the incorporated standards at the Federal Railroad Administration, Docket Room, 1200 New Jersey Avenue, SE., Washington, DC 20950, or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030, or go to *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*

II. TEST SITE REQUIREMENTS

The test site shall meet the following requirements:

(1) The locomotive to be tested should not be positioned where large reflective surfaces are directly adjacent to or within 25 feet of the locomotive cab.

(2) The locomotive to be tested should not be positioned where other locomotives or rail cars are present on directly adjacent tracks next to or within 25 feet of the locomotive cab.

(3) All windows, doors, cabinets seals, etc., must be installed in the locomotive cab and be closed.

(4) The locomotive must be running for sufficient time before the test to be at normal operating temperature.

(5) The heating, ventilation and air conditioning (HVAC) system or a dedicated heating or air conditioner system must be operating on high, and the vents must be open and unobstructed.

(6) The locomotive shall not be tested in any site specifically designed to artificially lower in-cab noise levels.

III. PROCEDURES FOR MEASUREMENT

(1) $L_{Aeq,\ T}$ is defined as the A-weighted, equivalent sound level for a duration of T seconds, and the sound level meter shall be set for A-weighting with slow response.

(2) The sound level meter shall be calibrated with the acoustic calibrator immediately before and after the in-cab static tests. The calibration levels shall be recorded.

(3) Any change in the before and after calibration level(s) shall be less than 0.5 dB.

(4) The sound level meter shall be measured at each of the following locations:

(A) 30 inches above the center of the left seat;

(B) Centered in the middle of the cab between the right and left seats, and 56 inches above the floor;

(C) 30 inches above the center of the right seat; and

(D) One foot (0.3 meters) from the center of the back interior wall of the cab and 56 inches above the floor. See Figure 1.