



August 13, 2009

U.S. Department of Transportation  
1200 New Jersey Avenue, SE  
W12-140  
Washington, DC  
20590

Re: Docket No. FRA-2008-0132, Notice No. 1

Attention: Docket Management Facility

HCRQ, Inc. hereby submits the following comments, regarding the proposed rule for Positive Train Control Systems, as a representative of Cattron Group International (CGI), 58 West Shenango St., Sharpsville, Pennsylvania, 16150.

These comments represent a collaborative effort between CGI and HCRQ.

CGI, a provider of locomotive remote controls, has over 60 years of radio frequency (RF) and wireless remote control experience. CGI companies have a total installed base of over 125,000 remote control systems throughout the world. Its products are suitable for all industries including railroads, construction, shipyards, mining, aerospace, steel, military, agriculture, shipping, material handling, utility vehicles and many more. CGI's development, system safety, and software safety processes meet the demands of safety-critical systems and benefit from continual improvement.

HCRQ services the safety-critical sectors of heavy rail, light rail, defense, aviation, and nuclear power generation. HCRQ has significant expertise in system safety, software safety, risk assessment, and both prior (i.e., IDOT PTC) and current experience with 49CFR236 Subpart H.



We sincerely hope that our comments are viewed as constructive and, should it be desirable, we are willing to discuss these comments further with FRA representatives and/or the RSAC PTC Working Group.

Respectfully,

Hunter Levan  
Director, Consulting



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
1	§234.275 (c)	“requiremnts”	Typo	“requirements”
2	§236.909 (e) (1)	“The analysis must confirm that the risk metrics of the system are not negatively affected by sensitivity analysis input parameters including, for example, component failure rates, human factor error rates, and variations in train traffic affecting exposure.”	It is not clear what “negatively affected” means. Does it mean the total residual risk exceeds that of the base case for any of the sensitivity analyses performed?	Unable to recommend replacement text since the intention is not known.
3	§236.909 (e) (1)	“The sensitivity analysis must document the sensitivity to worst case failure scenarios.”	It is not known what “worst case failure scenario” would imply with respect to human factor error rates. For instance, a typical Error Of Omission (EOO) rate is 1/100. What would be the worst case EOO rate? If a railroad expert panel was used to derive the human factor error rates, what would constitute worst case?  With respect to human factor error	Remove sentence.  Instead, require a reasoned justification for all failure rates.



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
			<p>rates, instead of “worst case failure scenarios” and in lieu of a costly Human Reliability Analysis (HRA) we believe there should be a reasoned justification for the failure rates that have been used. Indeed, there should be a reasoned justification for all failure rates that have been used.</p> <p>It is not known what “worst case failure scenario” would imply with respect to component failure rates. These rates are typically derived either from field data or from handbooks (e.g., Bellcore, EPRD, MIL-HDBK-217F). In the case of MIL-HDBK-217F the failure rates tend to be pessimistic by an order of magnitude.</p>	
4	§236.1003 (b) (2)	“Safe State means a system configuration that cannot cause harm when the	Definition is incorrect.	“Safe State means a system configuration that cannot cause harm.” (i.e., a failure



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
		system fails.”		should not result in the system transitioning from a safe state to an unsafe state)
5	§236.1049 (Appendix B) (e)	“In order to derive the frequency of hazardous events (or MTTHE) ... Such failure frequency is to be derived ...”	Assume “frequency of hazardous events” and “failure frequency” are equivalent.	“In order to derive the frequency of hazardous events (or MTTHE) ... The MTTHE is to be derived ...”
6	§236.1049 (Appendix B) (f) (1)	“The MTTHE calculation must consider the rates of failures caused by permanent, transient, and intermittent faults accounting for the fault coverage of the integrated hardware/software subsystem or component, phased-interval maintenance, and restoration of the detected failures.”	This is not clearly stated.  “Permanent” faults would result in an MTTHE of zero.  “Transient” by definition is something that comes and then goes away. It may never be detected. How could one determine its rate of occurrence?	“The MTTHE calculation must consider the rates of failures caused by contributory faults accounting for the fault coverage of the integrated hardware/software subsystem or component, phased-interval maintenance, and restoration of the detected failures.”
7	§236.1049 (Appendix B) (f) (2)	“Software fault/failure analysis must be based on the proper assessment of the design and implementation of the application code, its operating/executive program, and associated device drivers...”	“Proper” assessment is open to interpretation.  Real Time Operating System (RTOS) “evaluation” is possible.  Assessment of device driver	“Software fault/failure analysis must be based on the assessment of the design and implementation of the application code, an evaluation of the operating/executive program and other COTS software components...”



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
			software would require the source code which is usually proprietary.  Assessment should include Commercial Off-The-Shelf (COTS) software, if incorporated, other than the operating system.	
8	§236.1049 (Appendix B) (f) (2)	“The software assessment process must demonstrate through repeatable predictive results that all software defects have been identified and corrected by process with a high degree of confidence.”	It is not possible to demonstrate that all software defects have been identified with a high degree of confidence. A famous statement made years ago (author unknown) is “It is common in industry to find a piece of software, which has been subjected to a thorough and disciplined testing regime, has serious flaws.”  It is not clear what “high degree of confidence implies”.	“The software assessment process must demonstrate, through repeatable predictive results, that the software operates as specified without error.”
9	§236.1049 (Appendix B) (g) (1)	“(1) The safety-critical behavior ...”	This should be a new paragraph.	Self-explanatory.
10	§236.1049	“The MTTHE	“Permanent” faults	“The MTTHE



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
	(Appendix B) (g) (1)	assessment methodology must consider failures caused by permanent, transient, and intermittent faults ...”	would result in an MTTHE of zero.  “Transient” by definition is something that comes and then goes away. It may never be detected. There is no rate of occurrence associated with it.	assessment methodology must consider failures caused by contributory faults ...”
11	§236.1049 (Appendix B) (h) (1)	“(1) The railroad shall document ...”	This should be a new paragraph.	Self-explanatory.
12	§236.1049 (Appendix B) (h) (1)	“The railroad shall document these assumptions in such a form as to permit later automated comparisons with in-service experience.”	It is unclear how this could be accomplished. In addition, there is no need to specify an “automated” process for comparing risk assessment assumptions with actual experience.	“The railroad shall document these assumptions in such a form as to permit later comparisons with in-service experience.
13	§236.1049 (Appendix B) (h) (3)	The railroad shall document any assumptions regarding software defects. These assumptions shall be in a form which permits the railroad to project the likelihood of detecting an in-service software defect. These	In order to determine the likelihood of detecting an in-service software defect, one would have to apply software reliability growth modeling. This would be costly.	The railroad shall document any assumptions regarding software defects. These assumptions shall be documented in such a form as to permit later comparisons with in-service experience.



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
		assumptions shall be documented in such a form as to permit later automated comparisons with in-service experience.		
14	§236.1049 (Appendix B) (h) (4)	“The railroad shall document all of the identified safety-critical fault paths to a mishap as predicted by the safety analysis methodology.”	This text seems to imply that a detailed document, separate from the fault trees themselves, is required. This would be very costly.	“The railroad shall document all of the identified safety-critical fault paths to a mishap.”
15	§236.1049 (Appendix C) (b) (1)	“Absence of specific operator actions or procedures will not prevent the system from operating safely.”	This implies that the system will operate safely in the presence of human error. Is this possible?	Delete wording.
16	§236.1049 (Appendix C) (b) (1)	“Hazards categorized as unacceptable or undesirable, which is determined by hazard analysis, must be eliminated by design. Those undesirable hazards that cannot be eliminated should be mitigated to the acceptable level as required by this Part.”	It is a rare situation when hazards can be “eliminated”.	“The safety order of precedence is to eliminate hazards categorized as unacceptable or undesirable. If this is not possible or practical, these hazards should be mitigated to acceptable levels as required by this Part.”
17	§236.1049 (Appendix C) (b) (2) (i)	“It must be shown how the product is designed to eliminate or mitigate or eliminate unsafe...”	Typo	“It must be shown how the product is designed to eliminate or mitigate unsafe...”



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
18	§236.1049 (Appendix C) (b) (2) (i)	“...due to human error in the software specification, design or coding phases, or both;...”	Typo	“...due to human error in the software specification, design or coding phases;...”
19	§236.1049 (Appendix C) (b) (2) (ii)	“The product must be shown to operate safely under conditions of random hardware failure. This includes single as well as multiple hardware failures, particularly in instances where one or more failures ....”	It is not possible to implement such a system (i.e., one which continues to operate safely in the presence of multiple hardware failures).	“The product must be shown to operate safely under conditions of random hardware failure. This includes single failures and multiple hardware failures where one or more failures ....”
20	§236.1049 (Appendix C) (b) (2) (iii)	“Occurrence of credible single point failures that can result in hazards must be detected and the product must achieve a known safe state before falsely activating any physical appliance.”	The meaning is not clear as a result of using the word “falsely”.	“Occurrence of credible single point failures that can result in hazards must be detected and the product must achieve a known safe state before inadvertently activating any physical appliance.”
21	§236.1049 (Appendix C) (b) (2) (iv)	“...then the second failure must be detected and the product must achieve a known safe state before falsely activating any physical appliance.”	The meaning is not clear as a result of using the word “falsely”.	“...then the second failure must be detected and the product must achieve a known safe state before inadvertently activating any physical appliance.”
22	§236.1049 (Appendix C) (b) (3)	“...closed loop design requires that failure to perform a logical operation, or	This is confusing since all system operation is a product of actions	“...closed loop design requires that failure to perform a single logical operation, or



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
		absence of a logical input, output or decision shall not cause an unsafe condition, i.e. system safety does not depend upon the occurrence of an action or logical decision.”	and decisions. We believe we understand the intent and suggest rephrasing.	absence of a single logical input, output or decision shall not cause an unsafe condition, i.e. system safety does not depend upon the occurrence of a single action or logical decision.”
23	§236.1049 (Appendix C) (c) (2)	“... (MIL-STD) 882C, “System Safety Program Requirements” (January 19, 1993)...”	This version was superceded.	“... (MIL-STD) 882C, “System Safety Program Requirements”, Notice 1 (January 19, 1996)...”
24	§236.1049 (Appendix C) (c) (3) (vii) (H)	“IEC62278”	Typo	“IEC 62278”  This will be consistent with other references to standards.
25	§236.1049 (Appendix C) (c) (3) (vii) (I)	“IEC62279”	Typo	“IEC 62279”  This will be consistent with other references to standards.
26	§236.1049 (Appendix F) (d)	“At a minimum, the reviewer shall compare the supplier processes with acceptable methodology ...”	It is unclear what “acceptable methodology” implies.	“At a minimum, the reviewer shall compare the supplier processes with methodologies typical of safety-critical systems ...”
27	§236.1049 (Appendix F) (e)	“The reviewer shall analyze the Preliminary Hazard Analysis (PHA) ...”	The PHA is not the correct document to analyze since it becomes obsolete when superceded by	“The reviewer shall analyze the Hazard Log (HL) ...”



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
			<p>the hazard log.</p> <p>It is noted that the same comment is applicable to the existing Appendix D (d)(1).</p>	
28	§236.1049 (Appendix F) (f)	<p>“The reviewer shall analyze all Fault Tree Analyses (FTA), Failure Mode and Effects Criticality Analysis (FMECA), and other hazard analyses for completeness, correctness ...”</p>	<p>Analyzing “all” FTA and FMECA for “completeness” and “correctness” will be difficult and/or prohibitive for both the supplier and the reviewer.</p> <p>FMECA expansion is incorrect.</p> <p>It is noted that the same comments are applicable to the existing Appendix D (d)(2).</p>	<p>“The reviewer shall analyze sample Fault Tree Analyses (FTA), Failure Mode, Effects and Criticality Analysis (FMECA), and other hazard analyses for completeness, correctness ...”</p>
29	§236.1049 (Appendix F) (i) (7)	<p>“Methods employed by PTC system manufacturer to develop safety-critical software, such as use of structured language, code checks, modularity...”</p>	<p>The cited examples are not particular to safety-critical software.</p> <p>It is noted that the same comments are applicable to the existing Appendix D (f)(2)(vii).</p>	<p>“Methods employed by PTC system manufacturer to develop safety-critical software, such as use of requirements analysis, requirements traceability to functional and derived safety requirements, design analysis, documented peer reviews, peer review checklists, language</p>



Comment #	NPRM Section	Existing Text	Comments	Recommended Text
				subsets, coding guidelines, static and dynamic code analysis, complexity metrics, software assertions, information hiding, high module strength/cohesion, loose module coupling, robust design, hardware checks, CRCs, white box testing, hardware-in-the-loop automated testing, ...”
30	General	“safety critical”, “safety-critical”	Less optimal string search of rule.	Use “safety-critical” consistently.
31	General	“fail-safe”, “fail safe”, “failsafe”	Less optimal string search of rule.	Use “fail-safe” consistently.