The risk assessment of each safety-critical system (product) must account not only for the risks associated with each subsystem or component, but also for the risks associated with interactions (interfaces) between such subsystems.

(c) What is the main principle in computing risk for the previous and current conditions?
The risk for the previous condition must be computed using the same metrics as for the new system being proposed. A full risk assessment must consider the entire railroad environment where the product is being applied, and show all aspects of the previous condition that are affected by the installation of the product, considering all faults, operating errors, exposure scenarios, and consequences that are related as described in this part. For the full risk assessment, the total societal cost of the potential numbers of accidents assessed for both previous and new system conditions must be computed for comparison. An abbreviated risk assessment must, as a minimum, clearly compute the MTTHE for all of the hazardous events identified for both previous and current conditions. The comparison between MTTHE for both conditions is to determine whether the product implementation meets the safety criteria as required by subpart H or subpart I of this part as applicable.

(d) What major system characteristics must be included when relevant to risk assessment?
Each risk calculation must consider the total signaling and train control system and method of operation, as subjected to a list of hazards to be mitigated by the signaling and train control system. The methodology requirements must include the following major characteristics, when they are relevant to the product being considered:

APPENDIX B TO PART 236—RISK ASSESSMENT CRITERIA

The safety-critical performance of each product for which risk assessment is required under this part must be assessed in accordance with the following minimum criteria or other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable:

(a) How are risk metrics to be expressed? The risk metric for the proposed product must describe with a high degree of confidence the accumulated risk of a train control system that operates over the designated life-cycle of the product. Each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis, and the risk value selected must be demonstrated to have a high degree of confidence.

(b) How does the risk assessment handle interaction risks for interconnected subsystems/components? The risk assessment of each safety-critical system (product) must account not only for the risks associated with each subsystem or component, but also for the risks associated with interactions (interfaces) between such subsystems.

(c) What is the main principle in computing risk for the previous and current conditions?
The risk for the previous condition must be
(1) Track plan infrastructure, switches, rail crossings at grade and highway-rail grade crossings as applicable;

(2) Train movement density for freight, work, and passenger trains where applicable, and computed over a time span of not less than 12 months;

(3) Train movement operational rules, as enforced by the dispatcher, roadway worker/Employee in Charge, and train crew behaviors;

(4) Wayside subsystems and components;

(5) Onboard subsystems and components;

(b) Consist consists such as hazardous material, oversize loads; and

(c) Operating speeds if the provisions of part 236 cite additional requirements for certain type of train control systems to be used at such speeds for freight and passenger trains.

(1) The railroad shall document any assumptions regarding the derivation of risk metrics used. For example, for the full risk assessment, all assumptions made about each value of the parameters used in the calculation of total cost of accidents should be documented. For abbreviated risk assessment, all assumptions made for MTHHE derivation using existing reliability and availability data on the current system components should be documented. The railroad shall document these assumptions in such a form as to permit later comparisons with in-service experience.

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

(3) The railroad shall document any assumptions regarding software defects. These assumptions shall be in a form that permit the railroad to project the likelihood of detecting an in-service software defect. These assumptions shall be documented in such a form as to permit later comparisons with in-service experience.

(4) The railroad shall document all of the identified safety-critical fault paths to a mishap as predicted by the safety analysis methodology. The documentation shall be in such a form as to facilitate later comparisons with in-service faults.

[75 FR 2717, Jan. 15, 2010]