US Department
of Transportation

Federal Railroad
Administration

Research Results

RR 09-17
September 2009

A Practical Risk Assessment Methodology for Safety-Critical Train Control Systems

SUMMARY

This project has two objectives: one is to develop a methodology for quantitative risk analysis of a proposed safety-critical train control system (proposed case), and the other is to build a software tool to help automate the process of data preparation and risk comparison between the current system operation (base case) and the proposed case. This comparison enables the calculation of tolerable hazard rates that the proposed system must be designed not to exceed. That is, the proposed safety-critical train control system will be at least as safe as the system it replaces, in accordance with the requirements of Title 49 Code of Federal Regulations Part 236 Subpart H.

The Practical Risk Assessment Methodology (PRAM) is a cause-consequence analysis supported by event tree analyses, and by statistical analysis of available historical data from FRA's Railroad Accident/Incident Reporting System (RAIRS). First, the accident probabilities and consequences are calculated for each hazard, and then the collective risks are calculated in the form of total cost of accidents per train-mile for the base case and proposed system. The use of a standard tool makes this iterative process transparent to all reviewers. Where a lack of data exists for new systems, this standard process allows the user to collect new data and test new scenarios, and at the same time, maintain the data references between the old and new scenarios.

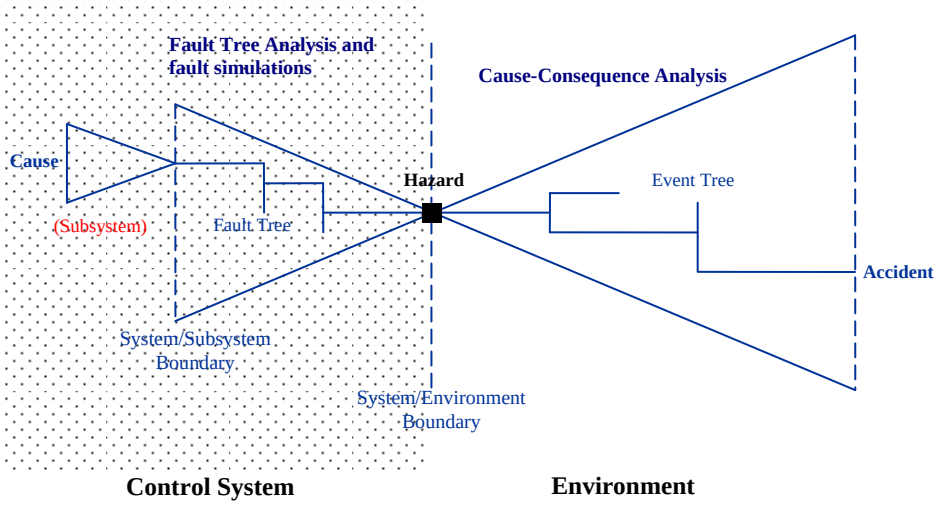

Figure 1. The relationship between control system faults and their consequences. Hazards are caused by system faults and may lead to accidents when the system interacts with its environment. PRAM is associated with the non-shaded area and leads to estimation of tolerable rates for all identified hazards, which in turn become a part of the safety requirements specification for the system to be designed.

BACKGROUND

Every signaling and train control project that introduces new technologies and systems replacing conventional train control systems is required to provide a full risk assessment. The need, then, is to come up with a sound risk assessment methodology for determining the level of safety that the new system must provide. This determination must be made before starting the system design to avoid the cost of redesign at later stages because of not conforming to standards and/or the lack of clarity of the system safety requirements at the beginning of the design phase.

The risk assessment methodology should be one that can be applied before new or replacement system design begins. Currently, no such "pre-design" risk assessment methodologies are in use by the North American rail industry. Moreover, general methods, such as simulation modeling that require significant design details to be available before they can be applied, are not yet working satisfactorily and can be costly to apply. The Practical Risk Assessment Methodology (PRAM) is intended to solve this problem.

This method does not require the development of detailed models or numerous simulations to generate statistically significant probabilities for various event sequences. Such simulations with fault injections, based on fault tree-derived probabilities of system failure, are eliminated and replaced by the sequence of events that begins with the interaction of the faulty system with its environment. Thus, it only requires an understanding of how the system will interact with its environment during various hazardous conditions. The resulting accident probabilities and severities are then used to determine the collective risks (or proposed case risk), which are used in designing the system. This difference in the two modeling approaches is illustrated in Figure 1.

METHODOLOGY

The steps involved in risk assessment are presented in Figure 2. This is an iterative process that begins with the definition of the proposed system and an identification of the hazards H_j , j = 1,….,n, associated with that system. Hazard identification is done via a structured hazard identification study using techniques such as brainstorming, *Hazard and Operability Study* (known as HAZOPS), and *Failure Modes, Effects and Criticality Analysis* (known as FMECA), as described in AREMA C&S Manual 17.3.5.

The potential consequences (accidents) of the hazards must then be identified. Each hazard may lead to one or more types of accidents A_{jk}, k = 1,…., m, depending on how the system operates and interacts with its environment while

it is in a hazardous state. The probability (C_{jk}) and severity (S_{jk}) of each accident are estimated using techniques such as cause-consequence analysis (using the event tree analysis method) and from historical data. Then, the collective risks as a result of accidents are calculated.

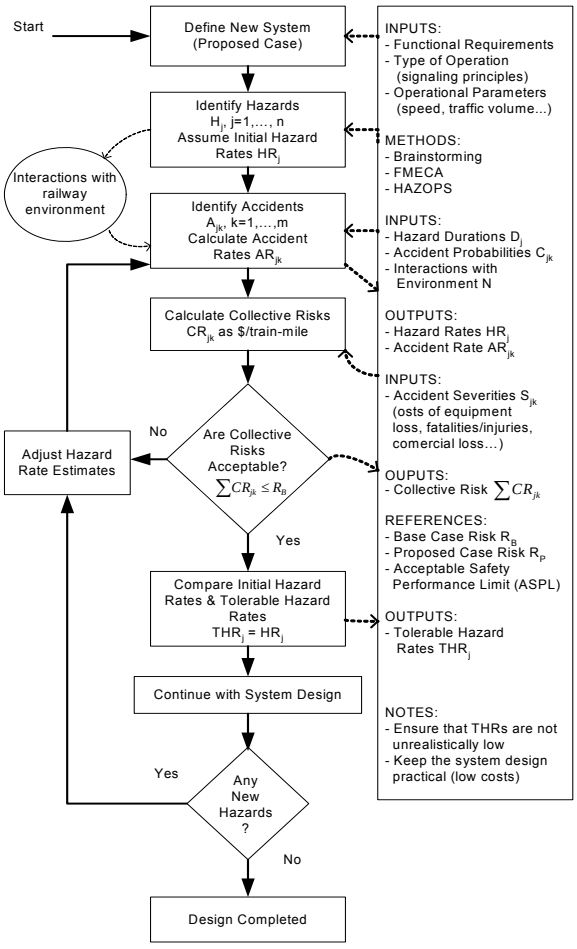

Figure 2. PRAM Iterative Process

These steps are expressed in the following equations:

$$CR_{jk} = AR_{jk} \times S_{jk} \text{ , } j = 1,\ldots..,n; \quad k = 1,\ldots\ldots,,m. \quad \text{(Eq.2)}$$

where N is the number of times the system interacts with its environment while in a hazardous state.

As the key goal of risk assessment, the sum of the collective risks is compared with the base case risk R_B, which is also termed the target acceptable safety performance level (ASPL). Given the initial estimates, if the sum of the collective risks associated with the identified hazards is less than or equal to the target ASPL, then the corresponding hazard rates are considered tolerable and together represent a level of safety that the system must be designed to meet.

Additional hazards are likely to be identified during the design phase of the new system because of expanded functionality and/or planned changes in the method of operation of the railway after the new system is deployed. The risk assessment is then repeated, with a new set of THRs derived. The design is then completed to satisfy the new set of THRs, and the overall risk for the railway with the new system in place should be estimated and shown to be equal to or less than the base case risk.

PRAM utilizes railway historical data, primarily the FRA RAIRS database, for deriving the probabilities (C_{jk}) and severities (S_{jk}) of the mishaps that could result from the hazards associated with the new system. Rather than assessing the internal failure mechanisms of the system that lead to hazards, which would require it to be designed already, only external factors such as fallback methods of operation, given that the system is in a failed state, need to be analyzed in determining consequences of the hazards. Safety-related system design requirements are therefore imposed from the "outside" before the system is designed, making it easier and cheaper to develop new systems.

ACCIDENT PROBABILITY AND SEVERITY ESTIMATES

Before the calculation of the collective risks, the probability (C_{jk}) and severity (S_{jk}) for each hazard-resulting accident must be processed from the historical data on all U.S. Class 1 railroads. The calculation procedure is detailed in Reference 3. The values of C_{jk} and S_{jk} for various accident cause codes are presented in the PRAM final report.

A risk analyst can use the cause-consequence analysis to define the C_{jk} and S_{jk} parameters for all cause codes that may result in a reportable accident. The PRAM tool can also assist the analyst to identify those cause codes that will be eliminated or reduced by deploying a new train control system. For a practical purpose, only these positive train control (PTC) preventable accidents are needed for the risk comparison on PTC-proposed case studies. Cause codes with a high probability and severity of accident are the priority for risk assessment.

BASE CASE RISK CALCULATION

References 1 and 5 provide the description of various base case scenarios to be used when a Railroad is considering replacement of an existing system with a new system, such as a PTC system. The base case risk R_B, as given by the following expression, can be calculated using data from the RAIRS database.

$$R_B = \Sigma(n_{B(x)} \times \$_{B(x)})/V_B \text{ dollars/train-mile} \quad \text{(Eq. 3)}$$

Where $n_{B(x)}$ is the number of accidents of type x during some period of time, $\$_{B(x)}$ is the average severity of accident type x, and V_B is the volume of traffic measured in terms of the number of train-miles over the same period. The sum is over all accident types. Details of the calculation are presented in Reference 3. The values of R_B for some U.S. Class I railroads are presented in the PRAM Final Report.

The base case method of operation is with a traffic control system when the proposed system is a PTC system. It is important for the risk analyst responsible for computing the base case risk to use caution in selecting the cause codes that represent the base case under consideration, and to justify the assumptions made. Also, R_B can be computed for a division, a zone or a line of a given railroad rather than for the entire railroad.

COMPARISON OF RISKS

FRA's PTC rules (49 CFR 236H) requires the total risk to be measured by the accident cost

per train-mile. A successful system proposal must present the value of the risk for the proposed system, which is the same as or less than the corresponding base case risk (i.e., the proposed system must be at least as safe as the one it is replacing). This is mathematically represented by,

$$R_P \leq R_B \quad \text{(Eq. 4)}$$

where R_P is the proposed system risk. From Reference 4, the expression for the proposed system risk,

$$R_P = \Sigma(n_{P(x)} \times \$_{P(x)})/V_P \text{ dollars/train-mile} \quad \text{(Eq. 5)}$$

where $n_{P(x)}$ is the number of accidents of type x that could occur in the proposed system, $\$_{P(x)}$ is the average severity of that type of accident, and V_P is the planned traffic volume for the proposed system. The value $n_{P(x)}$ for newly introduced hazards is a function of proposed system equipment configuration, equipment hazardous failure rates, operating plans, and human factors considerations. PRAM uses the sum of the collective risks calculated using Eq. 2 as an equivalent form of Eq. 5, enabling the design of the proposed system to begin, on the basis of an initial set of tolerable hazard rates.

If the calculated sum of collective risks (or R_P) turns out to be much larger or smaller than R_B, or if additional hazards are found during design, adjustments to the hazard rates must be made until R_P is smaller than, but reasonably close to, R_B.

The result will be a set of tolerable hazard rates, THRj, j = 1,..., n, which become part of the safety requirements specification for the proposed system. Design of the proposed system concludes when verification and validation of the design indicates that all THRs have been satisfied.

TOOL IMPLEMENTATION AND TESTING

A software tool has been developed to implement the PRAM for use by risk analysts to assess the risks of new and existing safety-critical train control systems. The PRAM tool has the following features:

1. Accepts inputs on hazards at system, subsystem, or function levels;
2. Provides the means to conduct CCA using the event tree analysis approach;
3. Contains databases for each parameter required;
4. Enables the risk analyst to derive the necessary probability and severity parameter values for the CCA under consideration;
5. Enables the risk analyst to derive the necessary R_B parameter value as an input to the calculation of tolerable hazard rates (THRs);
6. Generates reports;
7. Contains online help and user manual;
8. Contains appropriate error-handling and data validation mechanisms.

The PRAM tool has been tested using several test cases, each involving several hazards. A demonstration of the tool has been given to FRA. A final report submitted to FRA on this project includes details on the use of the PRAM tool.

ACKNOWLEDGEMENTS

The PRAM project was funded by FRA's Office of Research and Development. The Volpe National Transportation Systems Center acted as technical monitor and provided technical oversight and support.

CONTACT

Terry Tse
Federal Railroad Administration
Office of Research and Development
1200 New Jersey Ave. SE, Mail Stop 20
Washington, DC 20590
Email: terry.tse@dot.gov

KEYWORDS

Safety-critical, hazard, risk assessment, base case risk, proposed case risk, cause-consequence analysis, event tree analysis, FRA Rule 49CFR-236H

* Click here to download the public domain PRAM Tool for installation on your computer. The tool is dis-semminated in the interest of information exchange and does not imply endorsement by U.S. Government.