A PRACTICAL RISK ASSESSMENT METHODOLOGY FOR SAFETY-CRITICAL TRAIN CONTROL SYSTEMS

Chinnarao Mokkapati
Ansaldo STS USA Inc.
Union Switch & Signal Building
1000 Technology Drive
Pittsburgh, PA 15219

Terry Tse
Federal Railroad Administration
1200 New Jersey Avenue
Washington D.C. 20590

Alan Rao
USDOT RITA Volpe Center
National Transportation Systems Center
55 Broadway, Kendall Square
Cambridge, MA 02142

Abstract
This paper presents a methodology for quantitative risk analysis of a proposed safety-critical train control system (or Proposed Case), and describes a software tool that has been developed under a grant from the Federal Railroad Administration to implement the methodology. The tool automates 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 the Standards for Development and Use of Processor-Based Signal and Train Control Systems (49 CFR Parts 209, 234 and 236) issued by the FRA.

The Practical Risk Assessment Methodology (PRAM) is a Cause-Consequence Analysis supported by a statistical analysis of 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 two Cases. The use of a standard tool makes this iterative process transparent, so that the sources of data and assumptions are available for all to review. Where there is a lack of data 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. The PRAM provides a uniform tool for the railroads, suppliers and regulators for risk assessment of safety-critical train control systems.

1 BACKGROUND

Every signaling and train control project that introduces new technologies and systems replacing conventional train control systems (or methods) is required to provide a full risk assessment according to Reference [1]. 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 prior to starting the system design in order to avoid the cost of redesign at later stages due to not conforming to standards and/or due to lack of clarity of the system safety requirements at the beginning of the design phase.

The risk assessment methodology should therefore be one that can be applied before new or replacement system design begins. There are currently no such ‘pre-design’ risk assessment methodologies 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 PRAM is intended to solve this problem.

This method does not require the development of detailed models or large numbers of 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 is used in designing the system.
2 METHODOLOGY

The steps involved in Risk Assessment as detailed in Reference [3] are presented in Figure 1. This is an iterative process that begins with the definition of the proposed system and an identification of the hazards $H_j$, $j = 1, \ldots, n$, associated with that system. The proposed system is typically defined in documents such as: System Requirements Specification, System Architecture Description and System Design Description. Hazard identification is done via a structured Hazard Identification Study using techniques such as Brainstorming, HAZOPS (Hazard and Operability Study), and FMECA (Failure Modes, Effects and Criticality Analysis), as described in AREMA C&S Manual 17.3.5 [4].

The potential consequences (accidents) of the hazards must then be identified. Each hazard may lead to one or more types of accidents $A_{jk}$, $k = 1, \ldots, m$, 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 Event Tree Analysis method) and from historical data. Then the collective risks due to the accidents are calculated. These steps are expressed in the following equations:

$$\text{AR}_{jk} = N \times (HR_j \times D_j) \times C_{jk}, \quad j = 1, \ldots, n; \quad k = 1, \ldots, m$$  \hspace{1cm} (Eq.1)

$$\text{CR}_{jk} = \text{AR}_{jk} \times S_{jk}, \quad j = 1, \ldots, n; \quad k = 1, \ldots, m.$$  \hspace{1cm} (Eq.2)

where $N$ is the number of times the system interacts with its environment while it is 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 due to 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 [2], 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.

3 ACCIDENT PROBABILITY AND SEVERITY ESTIMATES

Before the calculation of the collective risks, the probability $C_{jk}$ and severity $S_{jk}$ for each hazard resulting accidents need to be processed from the historical data in [2] on all U.S. Class 1 railroads. The calculation procedure is detailed in [3]. The values of $C_{jk}$ and $S_{jk}$ for various Accident Cause Codes are presented in the PRAM Final Report [6].

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 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.

4 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
The Base Case risk $R_B$ as given by the following expression in [5] can be calculated using data from the RAIRS Database [2].

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

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 [3]. The values of $R_B$ for some U.S. Class I Railroads are presented in the PRAM Final Report [6].

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.

5 COMPARISON OF RISKS

FRA’s PTC Rules (49 CFR 236H and 236l) 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 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 [4], the expression for the proposed system risk,

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

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. Reference [5] states that “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, based on 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, \( \text{THR}_j, j = 1, ..., n \), 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.

6 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 PRA Tool has the following features:

1. Accepts inputs on hazards at System, Subsystem or Function levels;
2. Provides the means to conduct Cause-Consequence Analyses (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 on-line help and User Manual;
8. Contains appropriate error-handling and data validation mechanisms.

© AREMA 2009 ®
The PRA Tool has been tested using a number of test cases, each involving several hazards. A demonstration of the tool has been given to the FRA. The final report [6] on this project includes details on the use of the PRA Tool, which can be obtained from the FRA’s Office of R&D.

The value of the PRA Tool for risk assessment of new safety-critical train control systems depends on the completeness of the data it has from the RAIRS database; that is, data for all the relevant cause codes (identified by the FRA as the different types of causes of accidents) found in the database, which enable accident rates to be determined for each hazard. Furthermore, the more accident/incident data that can be obtained, whether over longer periods of time, or from other data sources, the more accurate the risk assessment will be.

To enhance the PRA tool - extending the database, improving the man-machine interface, making it easier to use, providing online help - so that it will be more likely to be widely adopted will require additional work. The intent is for the tool to become a standard for risk assessment and the basis for product safety plans for all new safety-critical train control systems.

7 CONCLUSIONS

This paper has presented a risk assessment methodology that can be implemented with the help of a software tool. Any safety-critical system can be analyzed with the help of this methodology. A set of safety requirements are derived upfront, allowing a disciplined approach to the design of the system right from the beginning, thus minimizing the risk of costly re-designs in later phases of the design life-cycle.

Railroads intending to procure Positive Train Control Systems that must be designed in compliance with Regulations such as the FRA Rules 236 Subparts H and I, as well as suppliers of such systems, are encouraged to consider using the methodology presented in this paper.

ACKNOWLEDGEMENTS

The PRAM project was funded by the Federal Railroad Administration’s Office of Research & Development, and was executed under the guidance of Mr. Terry Tse. Dr. Alan Rao of The © AREMA 2009 ®
Volpe National Transportation Systems Center acted as Technical Monitor, providing technical oversight and support to this project.

CONTACT
Terry Tse
Federal Railroad Administration
Office of Research and Development
1200 New Jersey Avenue, SE
Washington D.C. 20590
Email: terry.tse@dot.gov

REFERENCES


© AREMA 2009 ©
Figure 1. PRAM Procedure

INPUTS:
- Functional Requirements
- Type of Operation (signaling principles)
- Operational Parameters (speed, traffic volume...)

METHODS:
- Brainstorming
- FMECA
- HAZOPS

OUTPUTS:
- Hazard Rates HR_{ij}
- Accident Rate AR_{jk}

INPUTS:
- Hazard Durations D_i
- Accident Probabilities C_{jk}
- Interactions with Environment N

INPUTS:
- Accident Severities S_{jk} (costs of equipment loss, fatalities/injuries, commercial loss...)

OUTPUTS:
- Collective Risk CR_{jk}

REFERENCES:
- Base Case Risk R_B
- Proposed Case Risk R_P
- Acceptable Safety Performance Limit (ASPL)

OUTPUTS:
- Tolerable Hazard Rates THR_{ij}

NOTES:
- Ensure that THRs are not unrealistically low
- Keep the system design practical (low costs)