SIEMENS

Transportation Systems

Rail Automation

Engineering a Simple, Yet Rigorous, Risk Analysis Method

Prof. Jens Braband
Stephan Griebel

Siemens Transportation Systems – Rail Automation

Rail automation systems for mass transit and main line:

- Operations control systems
- Interlockings
- Automatic train control systems
- Components
- Telecommunications systems for rail applications

Interlockings and operations control systems

Automatic train control systems

Components

Telecommunications systems for rail applications

Objectives

- Presentation of a new, user-friendly and well-founded risk analysis approach (Best Practice (BP) risk approach), which combines the most advantageous properties of the popular approaches.

- Validation of the new approach by means of a particular example from a safety-relevant railway application.

I. Introduction

II. FMECA and Risk Priority Numbers

III. Criticality and basic requirements

IV. An engineering approach to risk analysis

V. An Example for safety-relevant railway application

VI. Applications and Conclusions

Introduction

- Many international safety standards offer a variety of methods for risk analysis, yet lack the theoretical background information or clear-cut criteria necessary for the selection of an appropriate method.
- The authors have researched the possibility of combining the most beneficial properties of commonly used approaches to create a new, user-friendly and well-founded approach, which we call the **Best Practice (BP) risk approach**.
- This approach is based on a variation of the risk priority number concept, in which the corresponding tables are generated using **sound engineering rules** in order to **guarantee certain essential properties**.

I. Introduction

II. FMECA and Risk Priority Numbers

III. Criticality and basic requirements

IV. An engineering approach to risk analysis

V. An Example for safety-relevant railway application

VI. Applications and Conclusions

FMECA based on Risk Priority Numbers (RPN)

- Failure Modes, Effects, and Criticality Analysis (FMECA) based on the risk priority number (RPN) concept
  - Qualitative Analysis for identifying failure modes, its causes and its effects
  - It is widely used to identify and prioritize critical issues

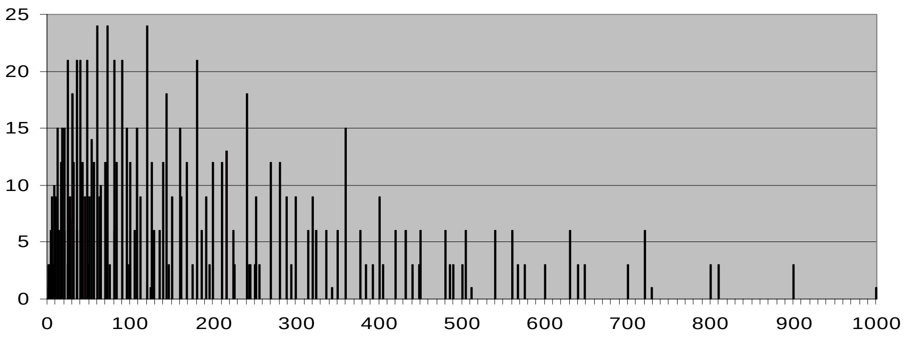
- RPN using descriptive terms to rank the
  - frequency of occurrence (O),
  - failure effect with severity (S) and
  - probability of the failure being undetected (D).

$$R = S \times O \times D$$

Inadequacies of the Conventional RPN Concept 1

- <u>Gaps in the ranges</u>

  The RPN scale is not continuous and 88% of the range is missing.



- <u>Duplicate RPNs</u>

  Many different combinations of the factors generate the same RPN

- <u>Sensitivity to small changes</u>

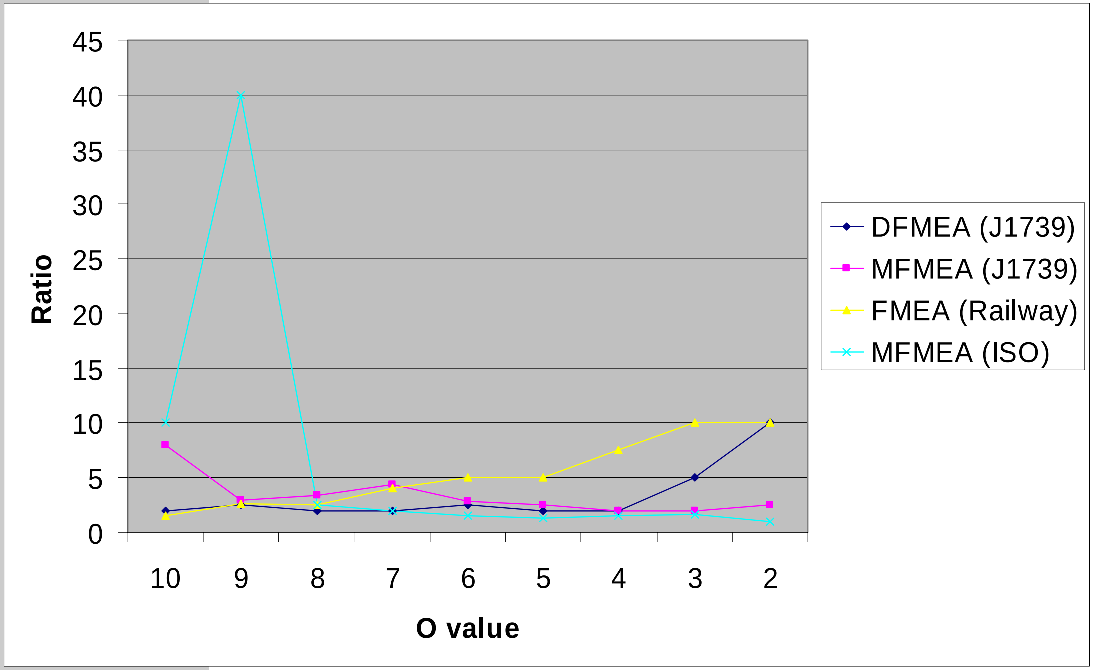
  A small change in one factor has a much larger effect when the other factors are larger than when they are small

- <u>Misleading conclusions from RPN comparison</u>

  Calculation of the RPN implies that trade-offs can be made between the factors

Inadequacies of the Conventional RPN Concept 2

Bandwidth:
All scales are stretched to a bandwidth ranging from 1 to 10,
no matter whether this can be justified or not. It is in fact highly questionable whether the parameters D and S should have the same range.



Varying ratios:
Within the same parameter, the ratios behind the different values are not the same, which means that a reduction in one parameter by one has a different effect depending on the starting point used.

Criticality

- Criticality is a **measure of risk**
  - Less rigorous and less costly approach
  - Less complex interaction between the contributing factors
- Criticality is a **combination of the severity** of an effect, the **frequency** of its occurrence and the probability of **detection**.
- Criticality is a **subjective measure** conducting the ranking on the basis of descriptive terms.

The Way to an Engineering Approach

- **FMECA** usually results in a **relative ranking** of the factors to the overall risk, so that **priorities can be set for actions** aimed at eliminating or containing the failures.
- **Risk analysis** for high-risk systems generally **focuses on risk acceptability**.
- Thus far no analysis method has been proposed which **combines simplicity for the user with the rigor or flexibility offered by the PRA**
- Therefore an **engineering approach** was chosen:
  Insights and observations from the railroad and aviation sectors were evaluated and railway operators as well as regulatory authorities asked what they considered to be the **basic requirements for a risk analysis approach**.

Basic Requirements for a Risk Analysis Approach

1. Risk tolerability criterion based on GAME (Globalement Au Moins Equivalent)
2. No necessity of a statement of residual risk
3. Incorporation of human factor
4. Independent assessment of the various system functions
5. Qualitative implementation of severity and consequence analysis
6. Adherence to consistent categories or standardized risk reduction factors (as in FHA method)
7. All relevant parameters taken into account
8. Accuracy in the region of one order of magnitude

I. Introduction

II. FMECA and Risk Priority Numbers

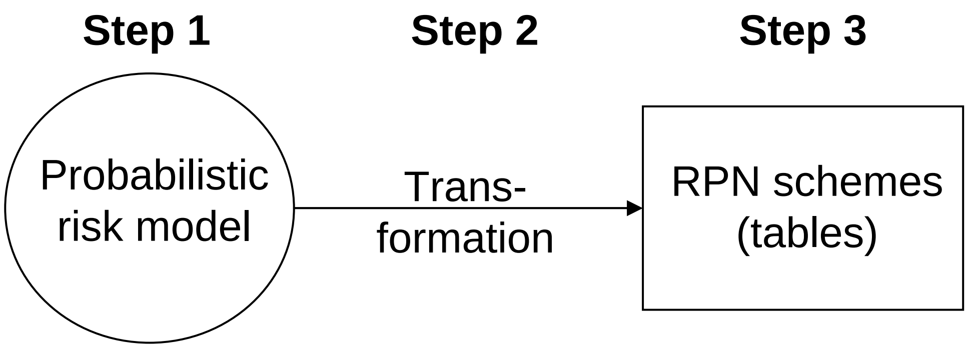
III. Criticality and basic requirements

IV. An engineering approach to risk analysis

V. An Example for safety-relevant railway application

VI. Applications and Conclusions

An Engineering Approach to Risk Analysis 1



Step 1

A generic probabilistic risk model is defined, together with the relevant parameters and assumptions about the model.

$$R = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} s_i \times o_i \times d_i$$

s_i (severity of the damage)

o_i (frequency of occurrence)

d_i (probability for non-detection or non-avoidance)

An Engineering Approach to Risk Analysis 2

Step 2

The generic risk model is then mapped by a mathematical transformation with guaranteed properties (such as monotony, similarity and simplicity) to an RPN scheme.

$$\log_b(R_i) \approx C_i = [\log_b(s_i)] + [\log_b(o_i)] + [\log_b(d_i)]$$

⇩

IRPN = S + O + D

Step 3

The value ranges of the tables are adjusted so as to minimize discretization errors and allow meaningful verbal comments to be attached to each parameter value.

I. Introduction

II. FMECA and Risk Priority Numbers

III. Criticality and basic requirements

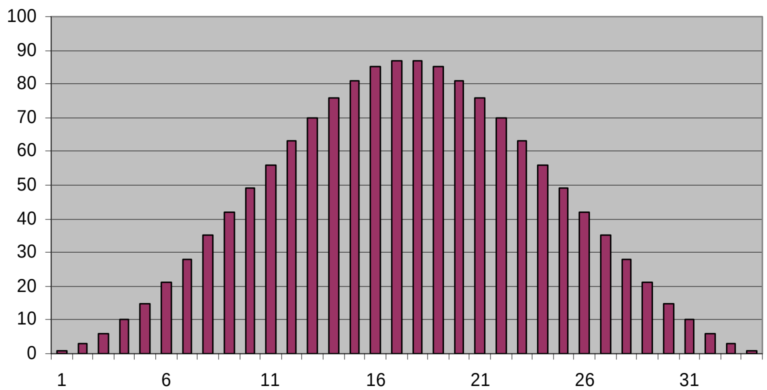
IV. An engineering approach to risk analysis

V. An Example for safety-relevant railway application

VI. Applications and Conclusions

Putting it into Practice

- Construction of tables for safety-relevant railway applications
- Selection of a passenger train as the object under consideration
- Derivation of a set of scales, where S ranges from 0 to 13, O from 0 to 14, and D only from 0 to 6.
- The smoothing effect of the summation produces a bell-shaped normal distribution.
- S, O and D are determined on the basis of **several subparameters**



Example of a Transformation of the Severity S

- Step 1:
  Subparameters for severity s:
  - number of people exposed (denoted by e)
  - energy involved in the accident (denoted by v)
  - type of accident (denoted by t)

- Step 2:
  Vast improvement over classical “full-size” approach:

$$s_i = c \times e_i \times v_i^{\,2} \times t_i \Longrightarrow S = E + 2 \times V + T$$

- Step 3:
  Estimation of the three subparameters based on three simple tables, each of which has a comment column for additional guidance.

Example of User-friendly Tables for Subparameters of S

The parameter E is described in detail as the number of people who can credibly be harmed in a typical accident.

E	People exposed *e*	Comment
0	Single person	
1	Few people	Typical of an accident at grade crossings
2	Several people	
3	Many people	All passengers of one or few cars
4	Very many people	All passengers of a train

The parameter V for the relative velocity:

V	Relative velocity *v*	Comment
0	Very low	Walking pace
2	Low	Switching (shunting)
3	Moderate	Fall-back or unsupervised mode
4	Medium	Branch line
5	High	Regional line
6	Very high	Main line

Example of User-friendly Tables for Subparameters of S

The third subparameter of the severity is the type of accident.

T	Type of accident *t*	Comment
0	Impact with obstacle	An impact with an obstacle is the impact of a train with a person or some other obstacle that does not fall into a higher category.
1	Grade crossing impact	This is the impact of a train with a road vehicle at a grade crossing.
2	Derailment	A derailment is any sliding or lifting of the train from the track.
3	Collision	A collision is any impact of two trains.

Example of a Safety-relevant Railway Application

- The function we shall consider is the function “protection of the train at a grade crossing”.
- A failure of this function results in a lack of warning signals for the road traffic and a missing indication to the monitoring system.
- Using the tables presented, a railway expert would obtain E=1, V=5 and T=1, yielding S=7.
- Applying an analogous procedure to the other parameters O an D and their subparameters, yields an IRPN of 17.
- What does this tell us and what can this be used for?

I. Introduction

II. FMECA and Risk Priority Numbers

III. Criticality and basic requirements

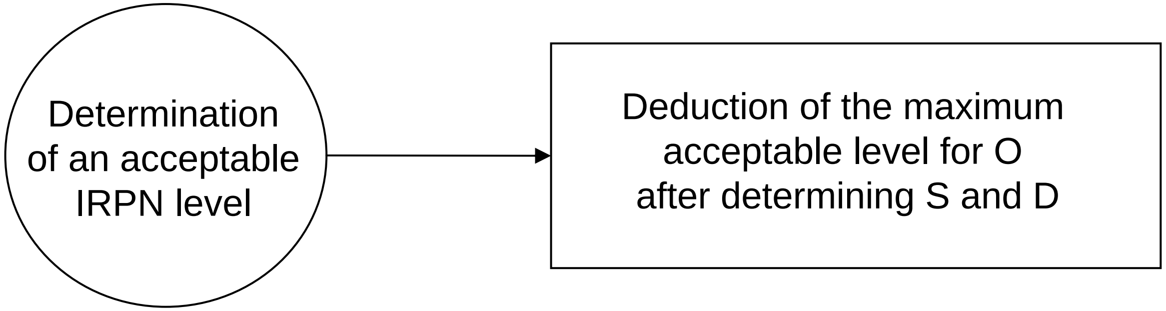
IV. An engineering approach to risk analysis

V. An Example for safety-relevant railway application

VI. Applications and Conclusions

Applications of the New Concept

- Simple ranking or prioritization criterion:
  - IRPNs of different functions could be compared and ranked.
  - Additional advantage: Correspondence between the difference in the IRPN and the factor for the risk (better comparability of results of different analyses)
- Providing a measure of risk acceptance:
  - Using the GAME principle, existing functions could be analyzed on the basis of the acceptable IRPN level.



e.g. 17

$O = 17 - S - D$

Conclusions

- The BP Risk Approach represents an easy-to-handle method of Risk Analysis based on an Improved Risk Priority Number concept
  - The approach is based on a sound model with a proper mathematical treatment.
  - Engineered construction of individual tables for the subparameters
  - The user obtains user-friendly interfaces that reflect his expertise and experience in the qualitative description of the various consequences.
  - The tables can be constantly readjusted by means of the various parameters in response to feedback from railway experts, i.e. it is engineering-oriented.
- The approach can also serve as a measure of risk acceptance based on the GAME principle.
  - Possibility of deducting the maximum acceptable level for the frequency of occurrence