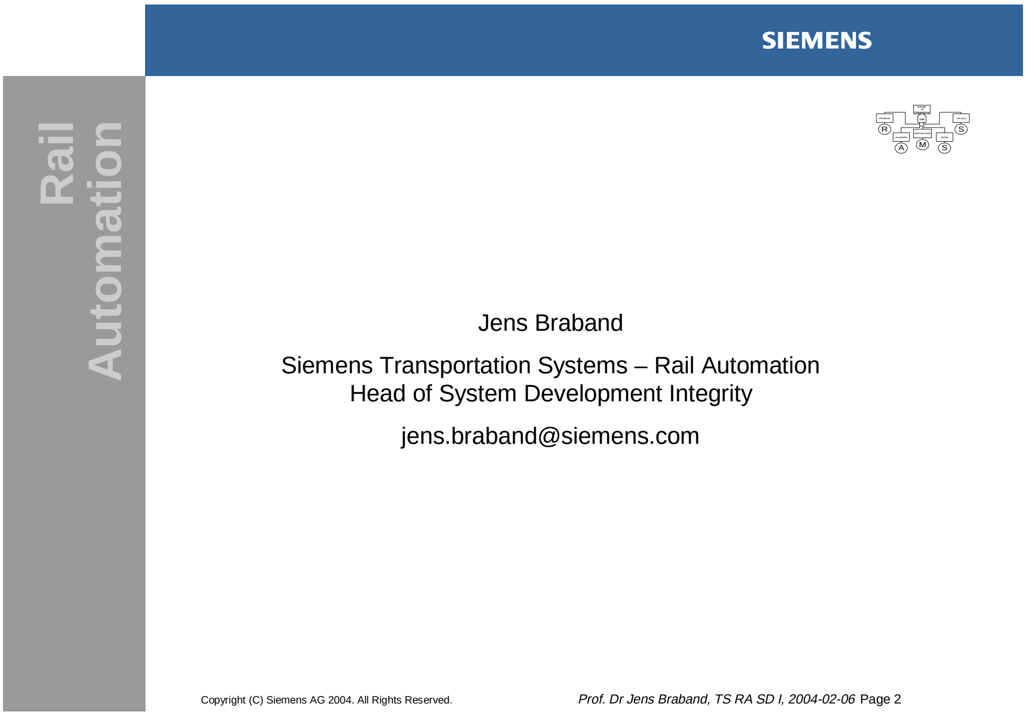
A Remedy for a Serious Flaw in the Risk Priority Number Concept

Bielefeld, 13 February 2004



SIEMENS
Rail Automation

Jens Braband

Siemens Transportation Systems – Rail Automation
Head of System Development Integrity

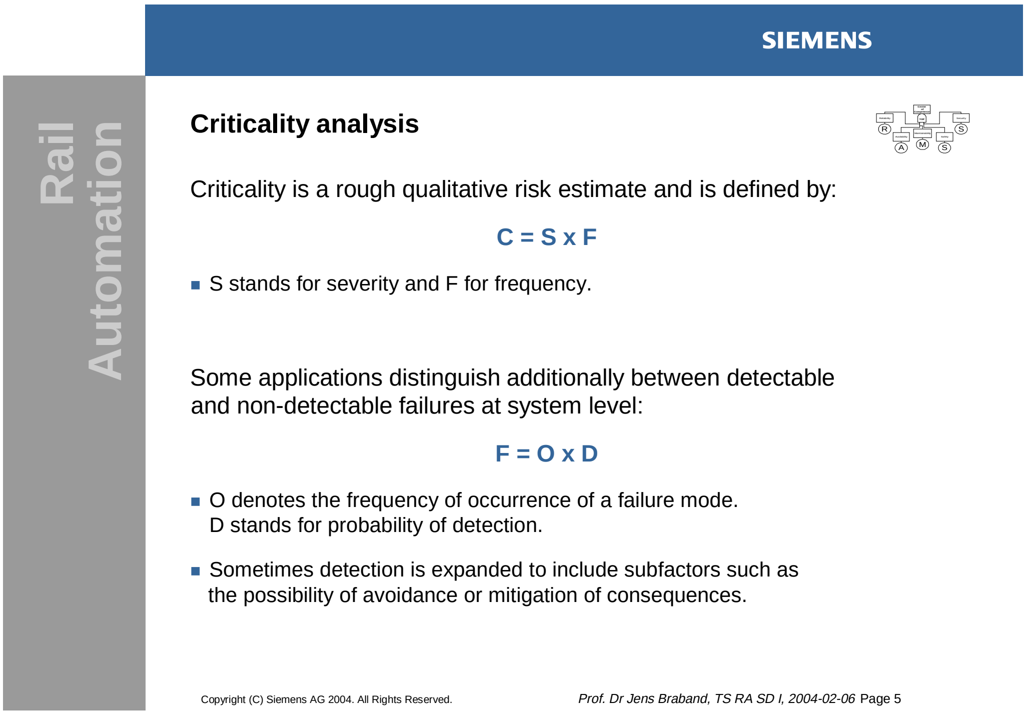
jens.braband@siemens.com

References

- Bowles, J.: An Assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis, Proc. RAMS2003, Tampa, January 2003
- Bowles, J.: Failure Modes, Effects, And Criticality Analysis: What It Is And How To Use It, Tutorial, RAMS1999
- Braband, J.: Improving the Risk Priority Number Concept, Journal of System Safety, no. 3, 2003
- FMEA für Software, Software Quality Systems, Tutorial, 2001
- Potential Failure Mode and Effects Analysis In Design (Design FMEA) and Potential Failure Mode and Effects Analysis In Manufacturing and Assembly Processes (Process FMEA) Reference Manual, Society of Automotive Engineers, Surface Vehicle Recommended Practice, J1739, July 1994.
- Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), IEC 60812

Introduction

- Failure Modes, Effects, and Criticality Analysis (FMECA) is potentially one of the most beneficial and intuitive tasks in a well-organized safety or reliability programme.
- It is a structured, qualitative analysis of a system for the purpose of identifying potential system failure modes, their causes, and the effects associated with each potential failure mode's occurrence.
- Particularly when applied in the early design phases of a system, an FMECA can save a great deal of time and money by helping to identify and prioritize critical issues.
- The excellent tutorial by Bowles on FMECA should be consulted for a more detailed discussion of the topic.



SIEMENS

Rail Automation

Criticality analysis

Criticality is a rough qualitative risk estimate and is defined by:

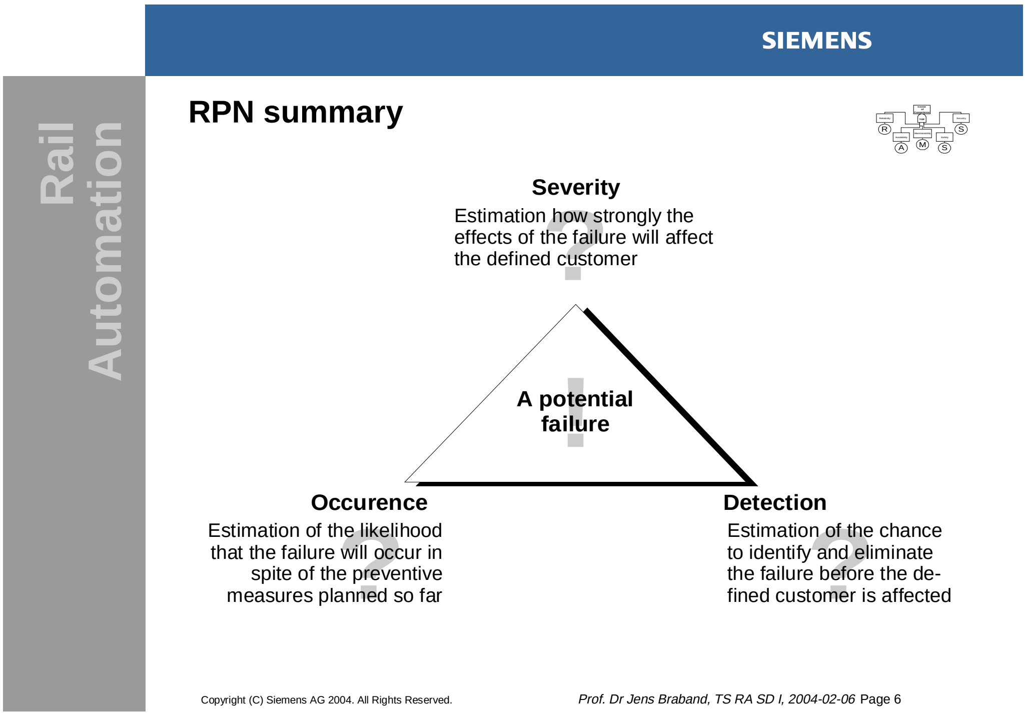
C = S x F

- S stands for severity and F for frequency.

Some applications distinguish additionally between detectable and non-detectable failures at system level:

F = O x D

- O denotes the frequency of occurrence of a failure mode. D stands for probability of detection.
- Sometimes detection is expanded to include subfactors such as the possibility of avoidance or mitigation of consequences.



SIEMENS

Rail Automation

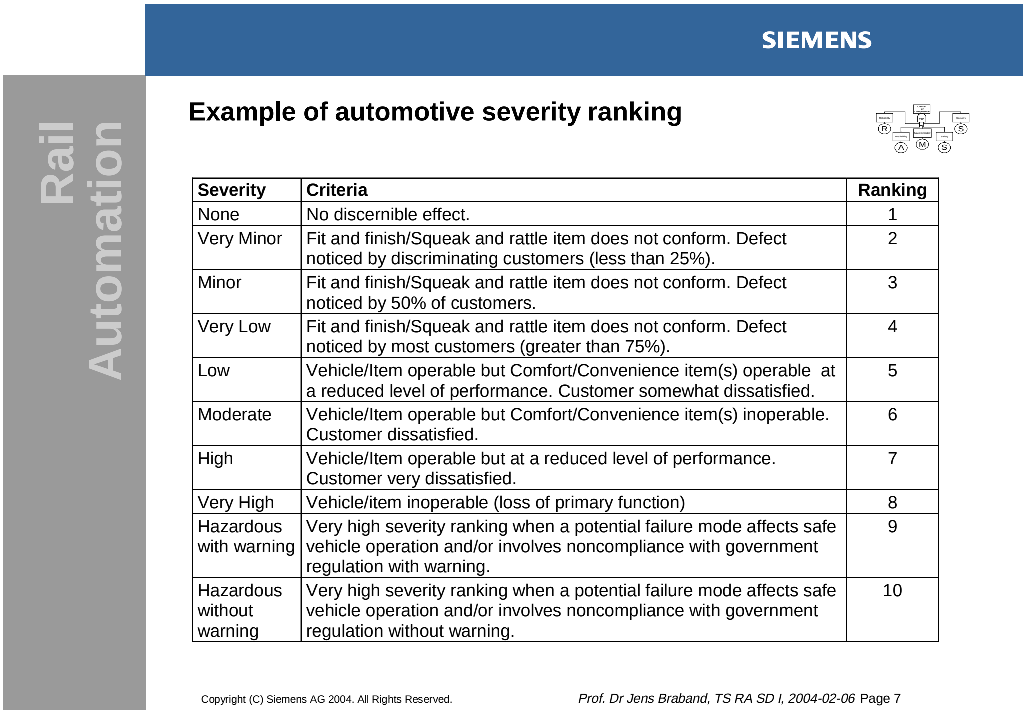
RPN summary

Severity
Estimation how strongly the effects of the failure will affect the defined customer

A potential failure

Occurence
Estimation of the likelihood that the failure will occur in spite of the preventive measures planned so far

Detection
Estimation of the chance to identify and eliminate the failure before the defined customer is affected

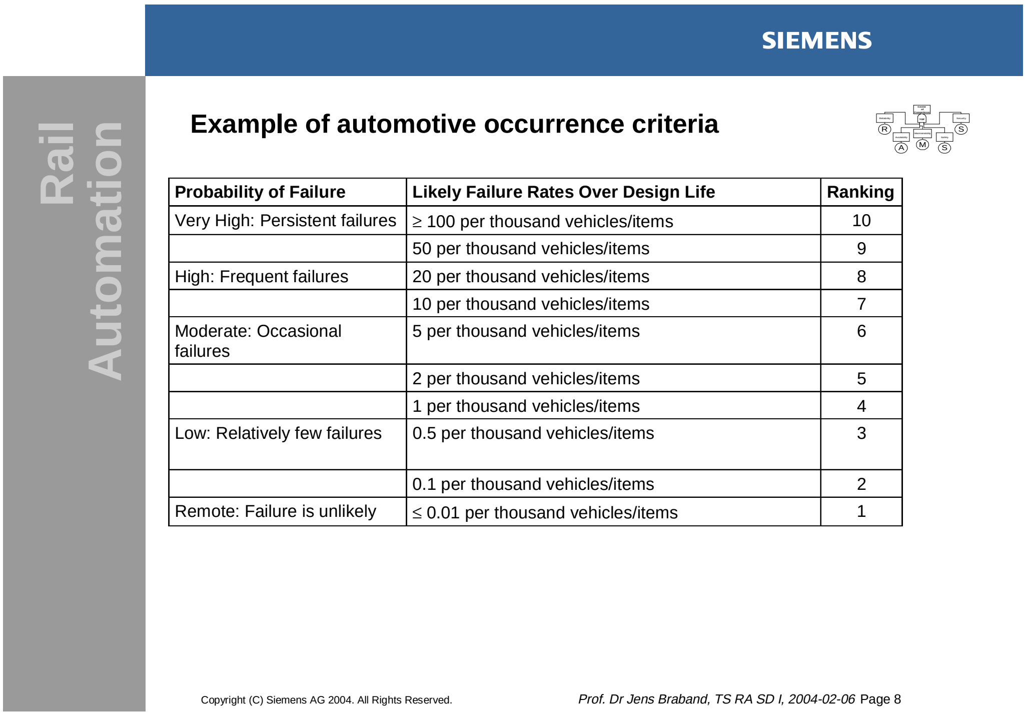


SIEMENS

Rail Automation

Example of automotive severity ranking

Severity	Criteria	Ranking
None	No discernible effect.	1
Very Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by discriminating customers (less than 25%).	2
Minor	Fit and finish/Squeak and rattle item does not conform. Defect noticed by 50% of customers.	3
Very Low	Fit and finish/Squeak and rattle item does not conform. Defect noticed by most customers (greater than 75%).	4
Low	Vehicle/Item operable but Comfort/Convenience item(s) operable at a reduced level of performance. Customer somewhat dissatisfied.	5
Moderate	Vehicle/Item operable but Comfort/Convenience item(s) inoperable. Customer dissatisfied.	6
High	Vehicle/Item operable but at a reduced level of performance. Customer very dissatisfied.	7
Very High	Vehicle/item inoperable (loss of primary function)	8
Hazardous with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9
Hazardous without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10



SIEMENS

Rail Automation

Example of automotive occurrence criteria

Probability of Failure	Likely Failure Rates Over Design Life	Ranking
Very High: Persistent failures	≥ 100 per thousand vehicles/items	10
	50 per thousand vehicles/items	9
High: Frequent failures	20 per thousand vehicles/items	8
	10 per thousand vehicles/items	7
Moderate: Occasional failures	5 per thousand vehicles/items	6
	2 per thousand vehicles/items	5
	1 per thousand vehicles/items	4
Low: Relatively few failures	0.5 per thousand vehicles/items	3
	0.1 per thousand vehicles/items	2
Remote: Failure is unlikely	≤ 0.01 per thousand vehicles/items	1

Rail Automation

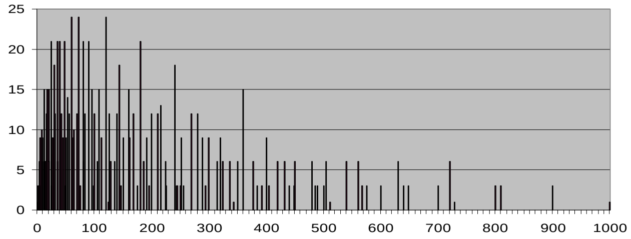
Example of automotive detection evaluation ranking

Detection	Criteria: Likelihood of Detection by Design Control	Ranking
Absolute Uncertainty	Design Control will not and/or can not detect a potential cause/mechanism and subsequent failure mode; or there is no Design Control	10
Very Remote	Very remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	9
Remote	Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	8
Very Low	Very Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode	7
Low	Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	6
Moderate	Moderate chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	5
Moderately High	Moderately High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	4
High	High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	3
Very High	Very High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	2
Almost Certain	Design Control will almost certainly detect a potential cause/mechanism and subsequent failure mode.	1

Rail Automation

Flaws in the RPN concept

- **Gaps in the ranges:** 88% of the range is empty; only 120 of the 1000 numbers are generated.
- **Duplicate RPNs:** for several combinations it is hard to see how such different factors can lead to the same RPN.
- **Sensitivity to small changes:** A small change in one factor has a much larger effect when the other factors are larger than when they are small.
- **Misleading conclusions from RPN comparison**: in order to make any sense the scale would have to be rational, not ordinal. Otherwise, wrong conclusions could be drawn.



A risk-based approach to RPNs

- RPN as a simple means of estimating risk:

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

- The natural way to solve this is a logarithmic transformation:

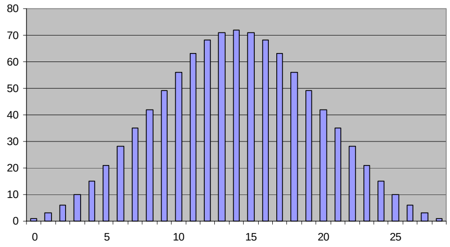
$$\boxed{\log_b(R_i)\approx C_i=\left[\log_b(s_i)\right]+\left[\log_b(o_i)\right]+\left[\log_b(d_i)\right]}$$

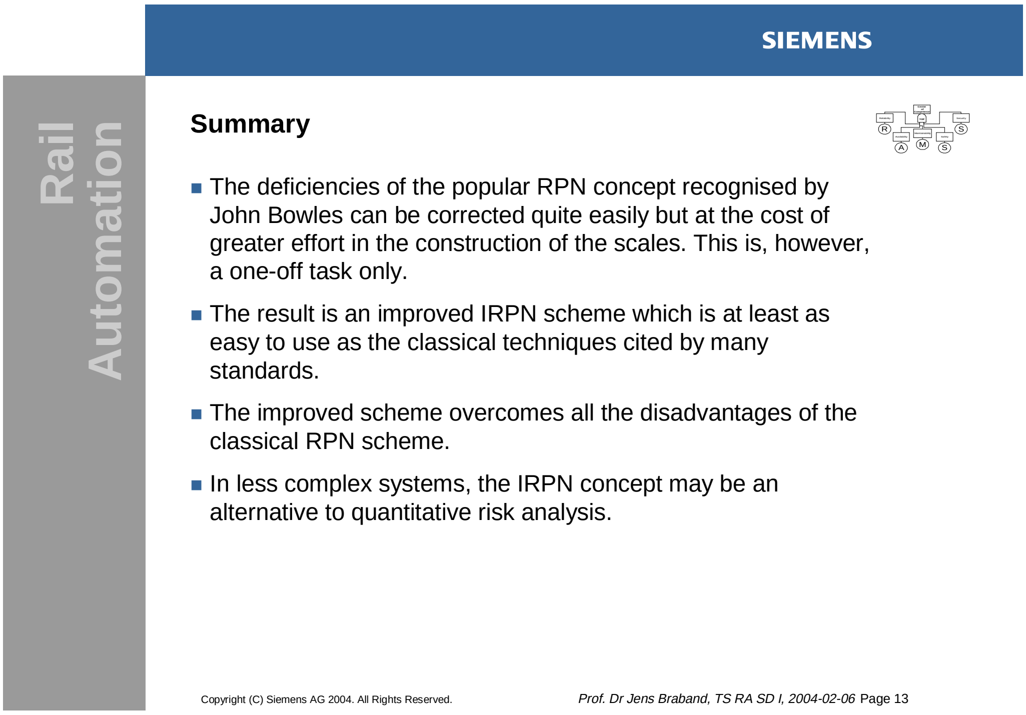
- This results in an even simpler RPN concept:

$$\boxed{\text{IRPN} = \text{S} + \text{O} + \text{D}}$$

IRPN: An Improved RPN Concept

- New approach uses a ratio scale, which is rounded and transformed into natural numbers.
- Choice of logarithmic base *b* is crucial and must be optimized.
- This results in different bandwidth ranges for the different parameters.
- All drawbacks can be overcome:
  - The range is continuous.
  - There are more identical IRPNs, but they represent equivalent risks (up to rounding effects).
  - Small variations in one ranking have the same effect on the IRPN, independently of the values of the other factors.
  - Correct conclusions are drawn.





SIEMENS

Rail Automation

Summary

- The deficiencies of the popular RPN concept recognised by John Bowles can be corrected quite easily but at the cost of greater effort in the construction of the scales. This is, however, a one-off task only.
- The result is an improved IRPN scheme which is at least as easy to use as the classical techniques cited by many standards.
- The improved scheme overcomes all the disadvantages of the classical RPN scheme.
- In less complex systems, the IRPN concept may be an alternative to quantitative risk analysis.