Challenges and Opportunities for Rail Safety

Risk management in complex railway systems considering the human factor

Presentation for the 19th International Railway Safety Conference

Deutsche Bahn AG, Germany

Fritz Schröder and Rüdiger Püttner

Divisions TBS and TTZ 111

Båstad, September 2009

Table of contents

Safety as the basic principle of railway systems

RESPONSIBILITY FOR SAFETY

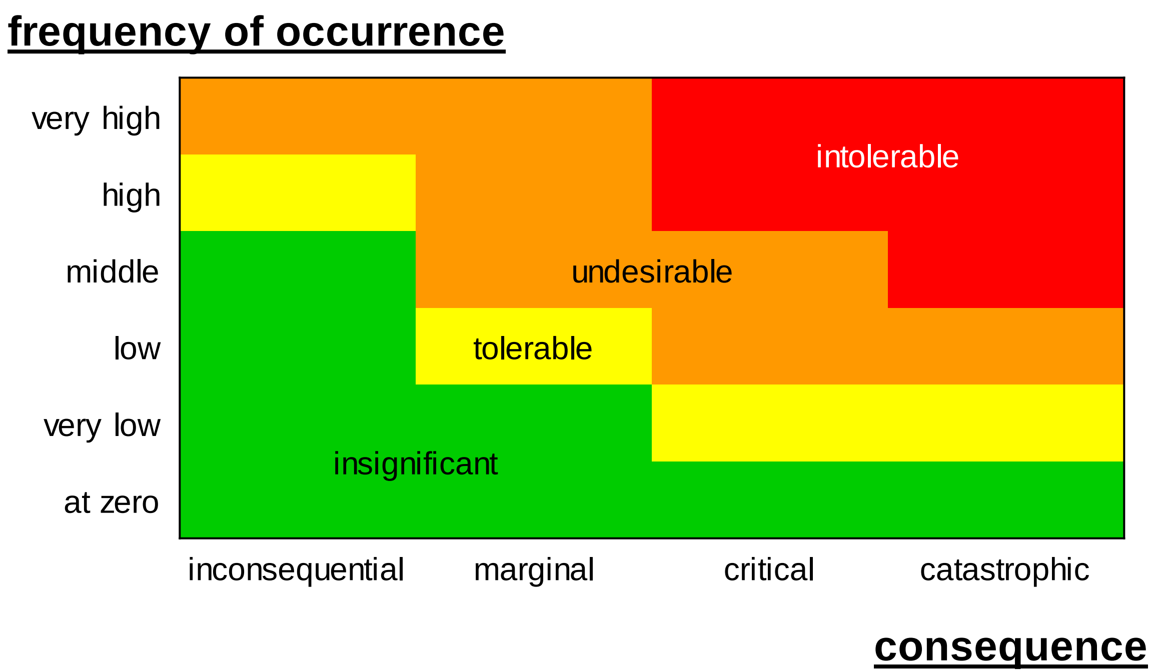
- Railway companies are required to ensure the safety of operating and the safety of construction and maintenance of their infrastructure, their vehicles and their equipment

- Safety is the absence of indefensible risks (IEC 61508)

- Risk **=** frequency of occurrence **x** consequence

- The risk of suffering damages caused by railway systems has to be reduced to an acceptable level

- Which level is acceptable?



Technical systems have to fail to the safe side

RISK CATEGORY I: TECHNICAL SYSTEM

Requirement

- Technical systems have specific failure rates.
- With less than 10^{-9} failures per operating hour, signaling equipment generally procures the lowest failure rates.
- In individual cases it is possible to downscale even this failure rate.

Risk acceptance criteria (RAC)

- **RAC for technical systems are almost defined.**

- Technical systems must fail to the safe side (fail-safe-principle).
- Is it necessary to consider the fallback system for assessment of the technical system?

Rules have to comply with the users' requirements of quality

RISK CATEGORY II: RULES

Requirement

- Rules must give instructions:
  - correctly,
  - completely,
  - understandably and
  - currently.
- One single error may not cause a disaster.

RAC

- **RAC for rules only consist of general requirements.**

- How can we ensure that the rules fulfill this demands?
- What does this mean to the author of this rules?

Personnel has to comply with the operating requirements of railway systems

Mobility
Networks
Logistics

RISK CATEGORY III: HUMAN

Requirement

Railway systems make high demands on the personnel:

- They have to pass qualifying examinations.
- They have to pass medical checkups.
- They have to prove their knowledge by passing exams.
- They have to show that they are able to realize their skills.

RAC

- **RAC for human factor have to be adapted on the basis of general values.**

- What is the human error rate in spite of these requirements?
- Which influences have an effect on this error rate?
- How can we reduce this error rate?

Common safety methods are a consistent way to evaluate railway systems

COMMON SAFETY METHODS (CSM) DECREED BY EU

Observation of rules

- The railway system is safe if it complies with the laws, the TSI and other rules.
- It is a precondition that these rules are safe.

Comparison of safety levels

- The railway system is safe when its safety level is at least as high as the safety level of an established railway system.
- It is a precondition that this established system is accepted by the stakeholders

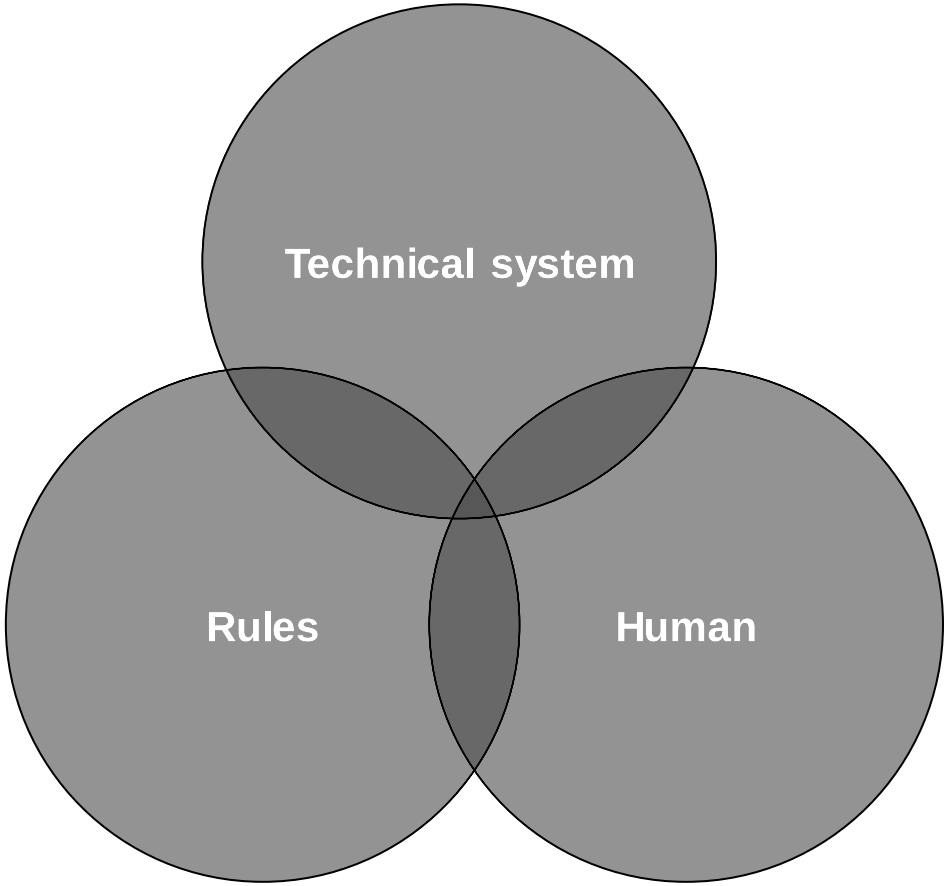
Risk assessment

- The railway system is safe when a risk assessment proves the compliance of the risk acceptance criteria (RAC).
- It is a precondition that RAC are already defined.

Identification of potential risks

BASIC RISK CATEGORIES

- To identify potential risks, it is necessary to analyze the three basic risk categories
  - Technical system:
    Safety functions are executed by technical systems.
  - Rules:
    Rules define how to operate technical systems.
  - Human:
    Humans execute rule based safety functions by operating the technical system.



- Risks may result from each of the risk categories or from their interdependency

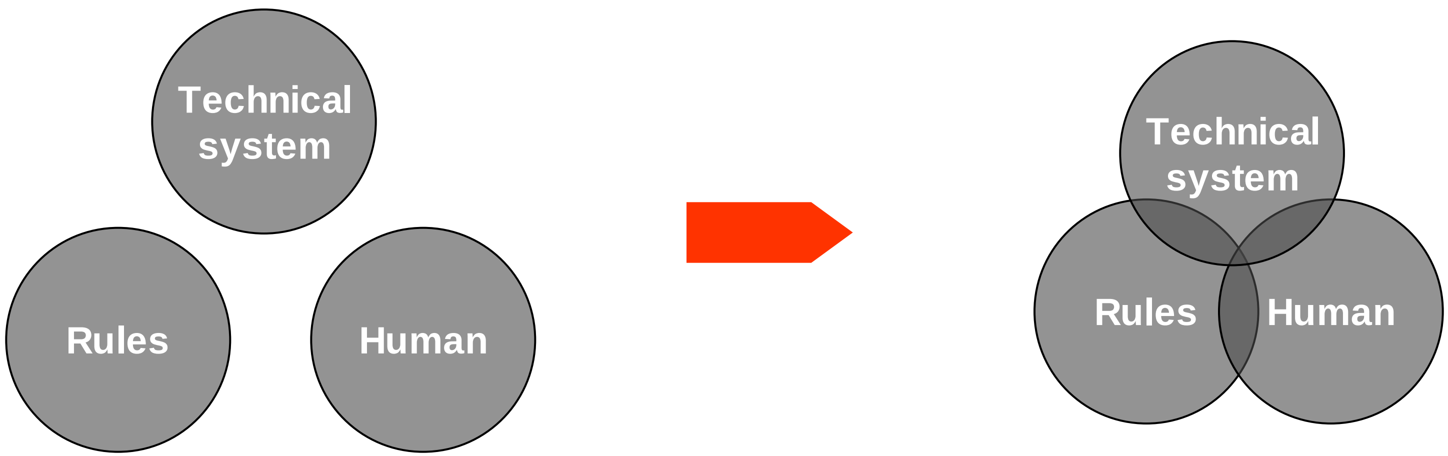
How can we reach an Europe-wide validity of common safety targets?

COMMON SAFETY TARGETS (CST) DECREED BY EU

CST

- If the railway companies would reach comparable safety levels AND if these safety levels would be broadly accepted, we could deduce the RAC from the accident statistics.

Overall view



- The separate consideration of one risk category can not detect the general risk of a railway system.
- Therefore it is necessary to develop a method which allows an overall view.

Inhaltsübersicht

To quantify the effectiveness of a safety barrier its functional type should be considered

Safety functions of technical systems

- quantification by RAMS-data
- quantification by using relevant databases / experience
- quantification by failure rates or probabilities

Safety operations with operational functionalities

- classification by considering rules

Combination of safety operations and safety functions

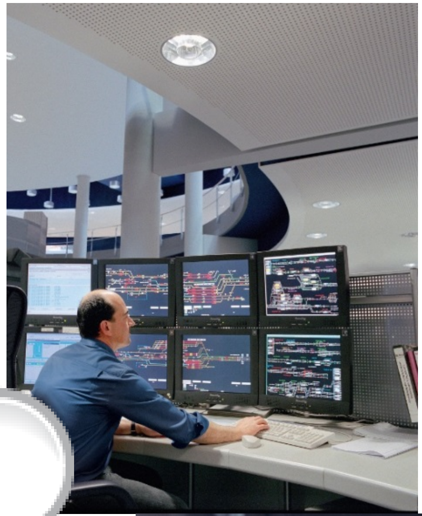
- demands a correlation of technical based rates and the safety related quantification of human actions

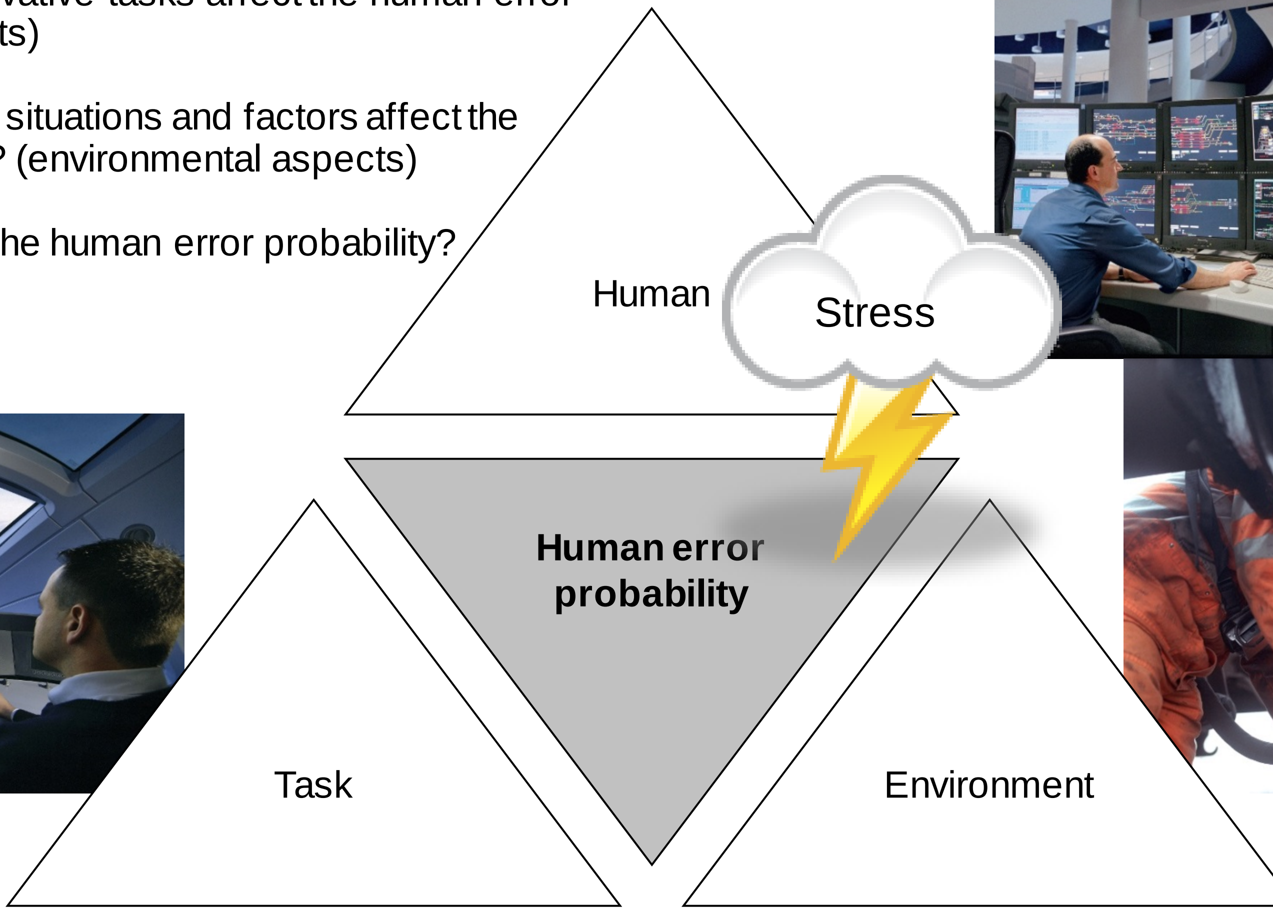
Safety operations with human actions (usually executed by railway staff)

- classification by considering human factors

Human actions and human error probability
What are the impacts?

- How do human characteristics and behaviour affect the human error probability? (human aspects)
- How do complex or innovative tasks affect the human error probability? (task aspects)
- How do error-promoting situations and factors affect the human error probability? (environmental aspects)
- How does stress affect the human error probability?





Fotos:
Maximilian Lautenschläger
Heiner Mülller-Elsner

Which aspects should be considered?

Human aspects
- staff fulfilling tasks should be adequately physically and mentally capable persons (physical properties)
- education and training (cognitive properties)
- social properties

Task aspects
- described in operational rule books or scenarios
- existing and available rules
- simple but varying tasks

Environmental aspects
- positive conditions reduce the human error probability

Stress aspects
- monotony
- difficult environment
- too little or too much stress

Fotos: Christian Bedeschinski

Approach:
How to quantify the impacts on human actions?

Mobility Networks Logistics

This is a proposal for reduction/increasing factors for barriers realized by human actions:

- Three reduction factors:
  - Existence = factor 0,1
  - Absence = factor 1
- One increasing factor:
  - Existence = factor 10
  - Absence = factor 1

Human aspect	Consideration and calculation	
Education and training E	Yes/existence No/absence	E=0,1 E=1
Simplicity of task T	Yes/existence No/absence	T=0,1 T=1
Good environmental conditions C	Yes/existence No/absence	C=0,1 C=1
Stress S	Yes/existence No/absence	S=10 S=1

Reduction factor: $F_{red} = E \cdot T \cdot C \cdot S$

Range: $10^{-3} \leq F_{red} \leq 1$ assumed initially staff is not able to perform any notable reduction on hazard rates ($F_{red\ i} = 1$)

The range is applicable together with reduction factors of technical systems (e.g. $F_{red\ of\ train\ control\ systems} \approx 10^{-7}$)

How to combine rule based human action & technical systems?

Execution of a safety barrier by both:
rule based human action & technical systems

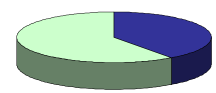
Example:

- A diagnostic system recommends a safety operation, which has to be executed by staff:
  - Onboard system triggers fire-alarm – staff stops the vehicle and initializes a rescue programme

Approach:

- Estimation / calculation of the reduction factors
- Estimation of the safety related contributions and apportionment:
  - Human action (rule based)
  - Technical function
- Calculation of the resulting reduction factor

$F_{red\ human}$ $F_{red\ technical}$



$F_{red\ res}$

Limitations of this approach
Comparison with other analyses

This approach

- can approximate only
- classifies
- uses “yes / no” decisions only

Compared with other analyses

- Example train driver: train has to stop at “red” signal:

Education and training	**Yes**	**E= 0,1**
Simplicity of task	**Yes**	**T= 0,1**
Good environmental conditions	**Yes**	**C= 0,1**
Stress	**No**	**S= 1**

$F_{red} = 10^{-3}$

Bubb, Heiner (ed.), „Ergonomy and traffic safety“, Presentation at the autumn conference 2000 in TU Munich, Herbert Utz publisher, 2000

$F_{red} = 10^{-3}$

- Example dispatcher: approval of track occupancy

Education and training	**Yes**	**E= 0,1**
Simplicity of task	**Yes**	**T= 0,1**
Good environmental conditions	**Yes**	**C= 0,1**
Stress	**No**	**S= 1**

$F_{red} = 10^{-3}$

Hinzen, Albrecht „The influence of human error on the safety of railways “, VIA - RWTH Aachen, book 48, 1993

$F_{red} = 10^{-3}$

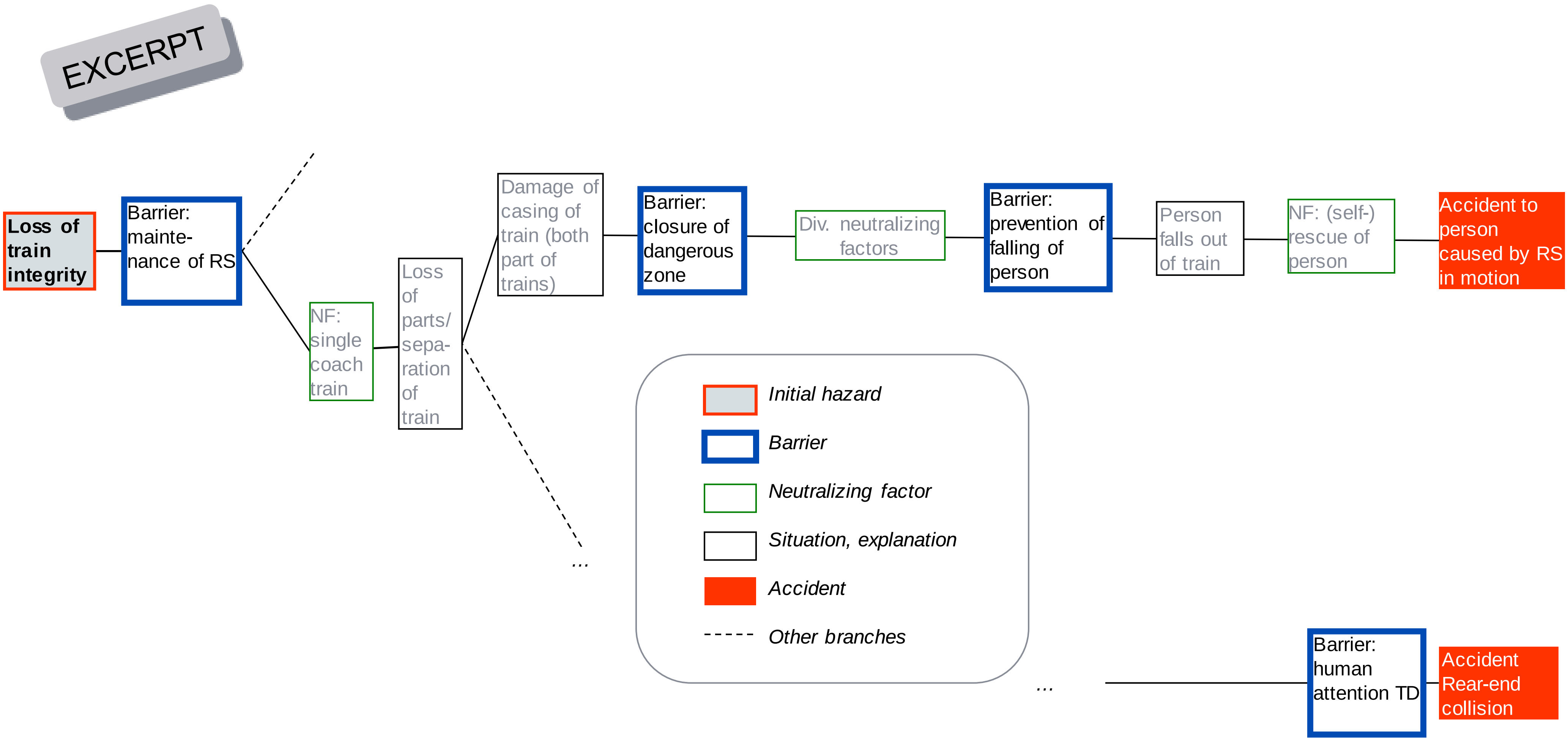
A pragmatic approach to quantify human safety functions to mitigate hazard rates

Backup

Different barriers in an event tree (1)

Safety functions/operations can be understood as barriers in event trees which determine accident rates

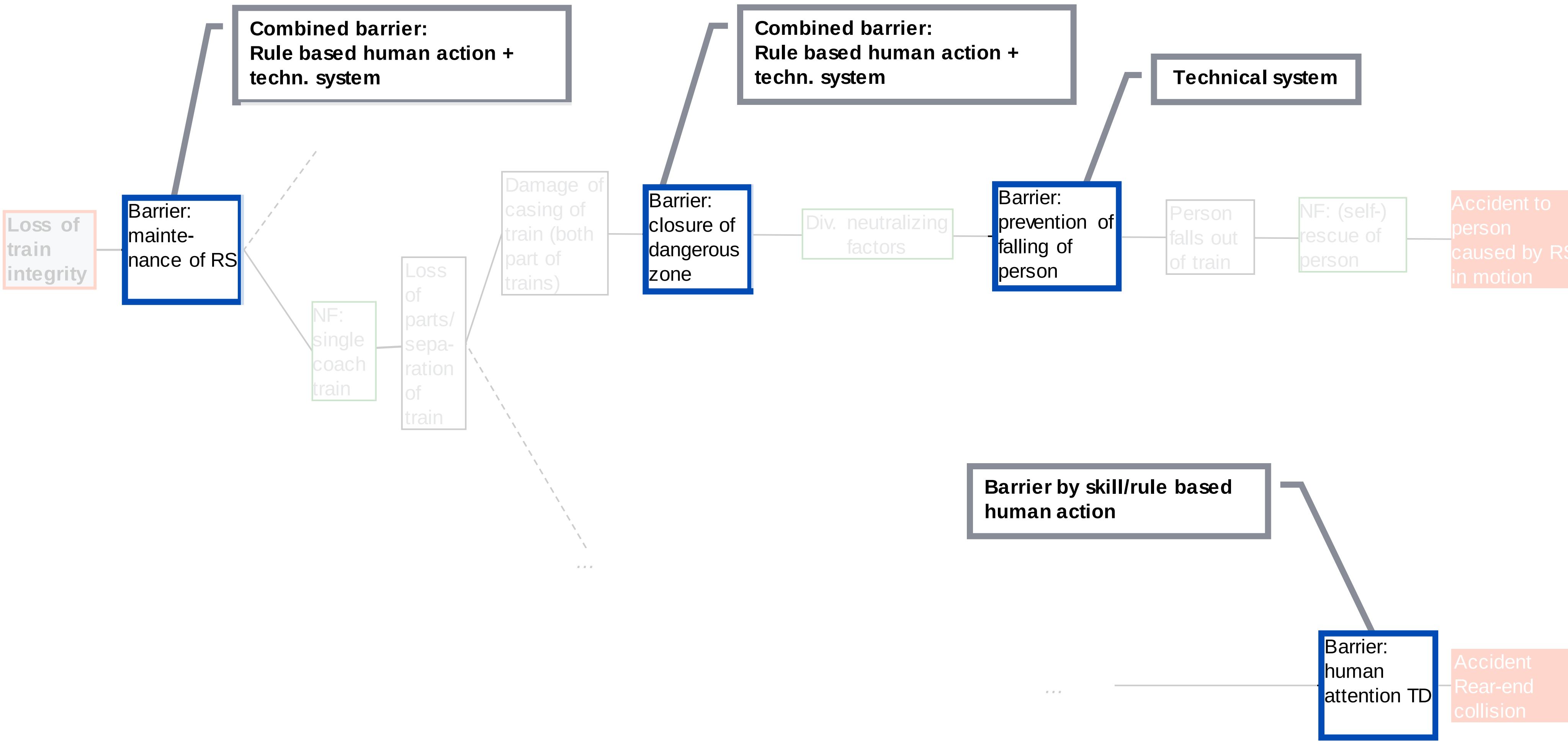
Example of an event tree (excerpt of project ROSA [1])



[1] ROSA CCA, DB AG/TU Dresden, 2008

Different barriers in an event tree (2)

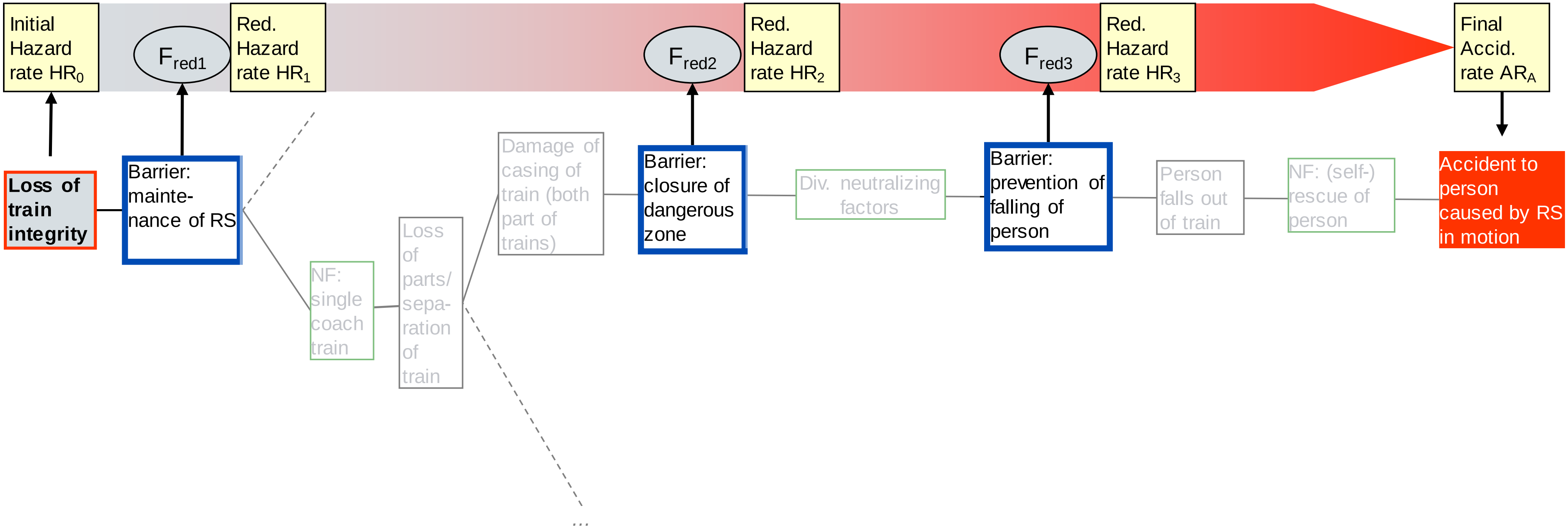
Example of an event tree (excerpt of project ROSA [1])



[1] ROSA CCA, DB AG/TU Dresden, 2008

Calculation of an event tree

Example of an event tree (excerpt of project ROSA [1])



Formula:

$$HR_{n+1} = HR_n \cdot (1 - F_{red\ n})$$

[1] ROSA CCA, DB AG/TU Dresden, 2008