

ROSA

Rail Optimisation Safety Analysis

Deutsche Bahn AG

Rüdiger PÜTTNER, Marc GEISLER

IRSC 2008, Denver



Rail Optimisation Safety Analysis

Generic Risk Analysis of the Railway System

- 1. Aims, Benefits and Partners**
- 2. The ROSA Model Consists of Four Elements**
- 3. The ROSA Model Covers Preliminary Hazard Analysis and Cause Consequence Analysis**
- 4. The Description of the ROSA Model's Elements**
- 5. ROSA Develops a Method to Consider Cost Benefit Aspects**
- 6. The Verification is Made by Examples**
- 7. The Results of ROSA are Generic**

The Aims, Benefits and Partners

Aims: generic safety model of the railway system

- Generic: adaptable to different railway systems
- Safety Model: tree structure (event / fault) and databases
- Railway system: technical systems and operation

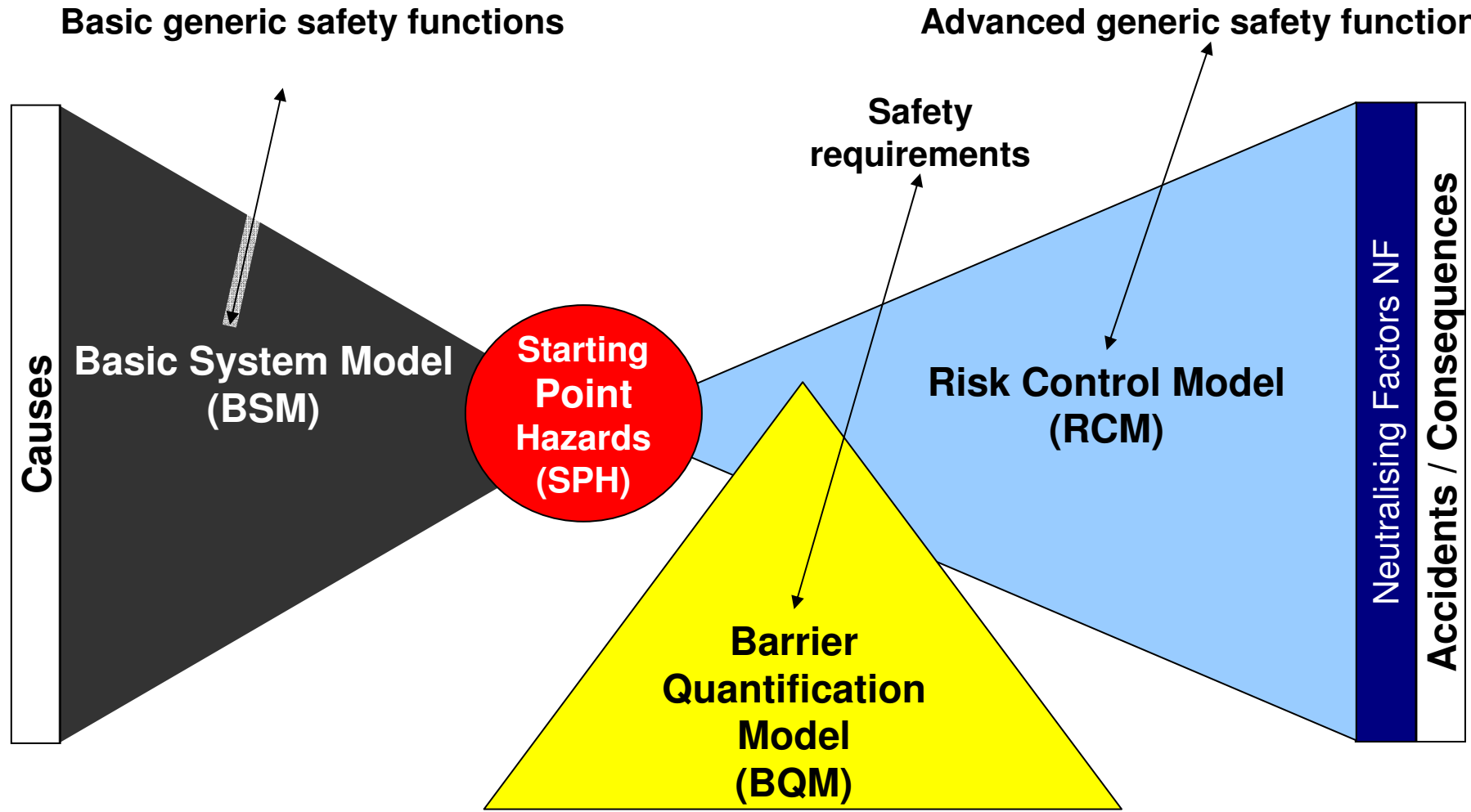
Benefits

- Effect analysis: safety targets focussed on (sub) systems
- Effect analysis: changes within the system to achieve the safety targets
- Detection of cost-efficient barriers to prevent an event / accident
- Balancing between barriers (ex ante)

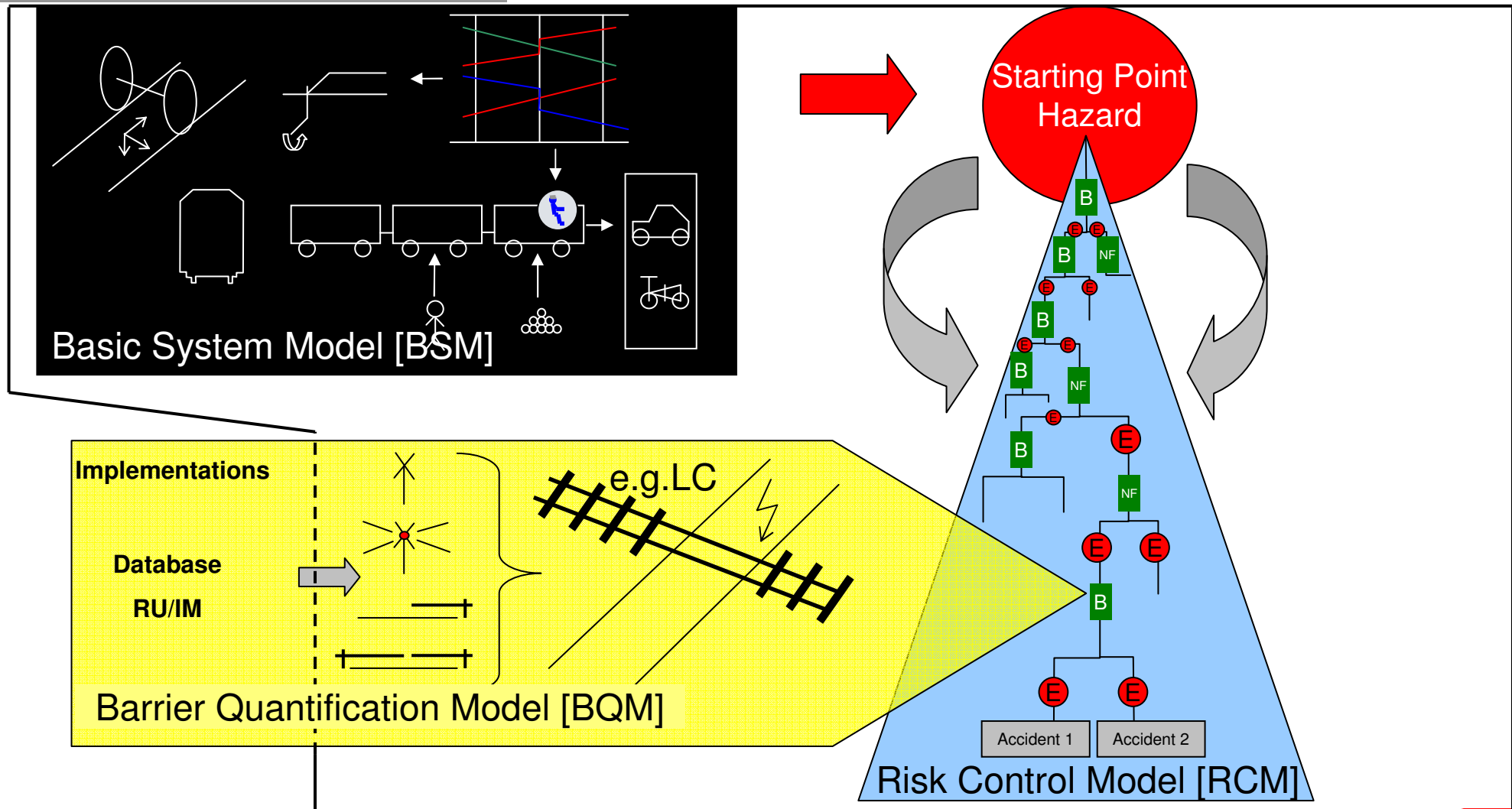
Partners

- Deutsche Bahn AG, SNCF, RFF, TUD and INRETS

The ROSA Model Consists of Four Elements

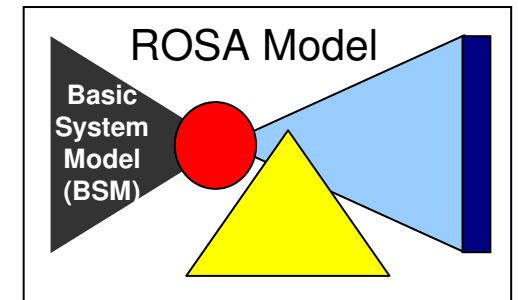


The ROSA Model Covers Preliminary Hazard Analysis and Cause Consequence Analysis



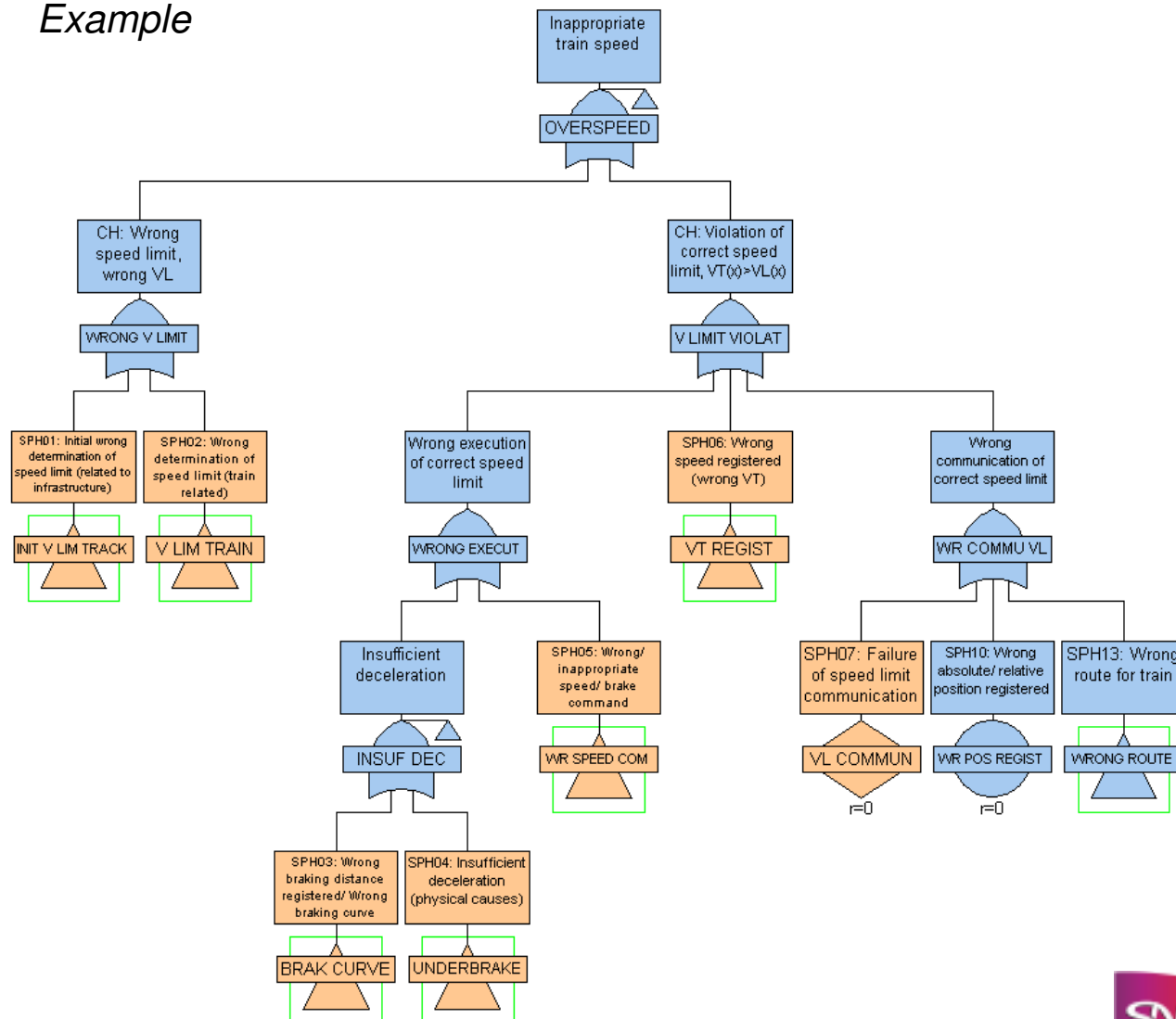
Description of the ROSA Model's Elements: Basic System Model is an Ideal and Virtual Railway System

- Ideal and virtual railway system
- System in steady state
- Includes only those safety functions
 - Which are homogeneous in most rail systems
 - Which can be derived from the physical conditions (e.g. guidance by rail, defined clearance envelope, flange of wheel, blocked traffic)
- Junctions and crossings
- Defined level crossings with other traffic systems, no separation from other traffic systems
- Defined access points for persons and goods for entering and leaving the railway system
- Rolling stock is equipped with brake systems
- General causes of accidents rise in the BSM



Example Of PHA: Fault Tree „Inappropriate Train Speed“ (Hazard Identification)

Example

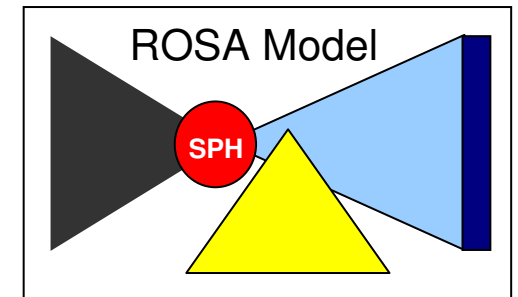


Starting Point Hazards

- SPH 01 Initial wrong Determination of speed limit (related to infrastructure)
- SPH 02 Wrong Determination of speed limit (train related)
- SPH 03 Wrong braking distance determined / wrong speed profile / Wrong braking curves
- SPH 04 Insufficient deceleration (physical causes)
- SPH 05 Wrong / inappropriate speed / brake command
- SPH 06 Wrong speed registered (wrong v_{train})
- SPH 07 Failure of speed limit communication

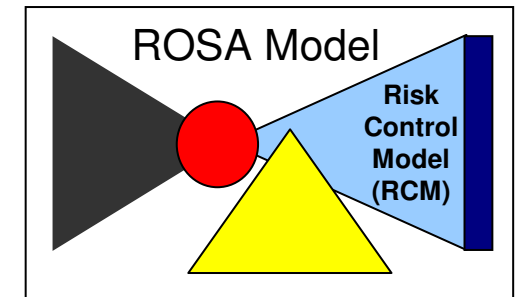
Description of the ROSA Model's Elements: The Starting Point Hazards are the Result of the PHA

- Derived from the Basic System Model by means of a Fault Tree Analysis
- Interface between Basic System Model and Risk Control Model
- Connects fault tree and event tree
- No control of the SPH by barriers in the Basic System Model
- Different barriers follow in the event tree of the Risk Control Model
- All branches of the fault tree (Basic System Model) are covered by SPH
 - List of approx. 60 SPH derived in ROSA covers passengers, staff, operation (speed, clearance envelope), rolling stock, infrastructure
- Verification with existing hazard lists


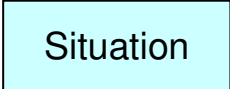
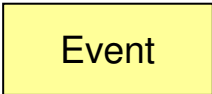

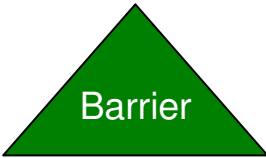
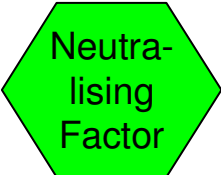


Description of the ROSA Model's Elements: The Risk Control Model Describes the Evolution of SPHs

- Describes the evolution of a hazard to an accident
- Graphic representation as event tree
- Only the accident paths are developed
- In any branch of the event tree there is at least one Barrier or Neutralising Factor
- Control of the SPHs by
 - Barriers (generic safety functions)
 - Neutralising Factors



Description of the ROSA Model's Elements: Elements of the Event Tree

 SPH	Starting Point Hazard
 Situation	Differentiation of cases within the event tree to represent different branches of hazard evolutions to diverse accidents
 Event	Follows a barrier, if the prevention is not successful
 Accident	According to European Railway Safety Directive (2004/49/EC)
 Barrier	Active mitigation of hazard evolution to an accident
 Neutra- lising Factor	Lucky mitigation of hazard evolution to an accident

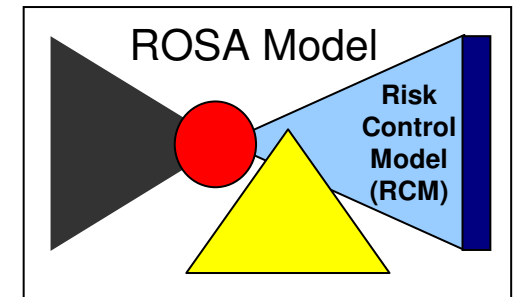
Description of the ROSA Model's Elements: Barriers and Neutralizing Factors Mitigate the Hazard Rates

■ Barrier

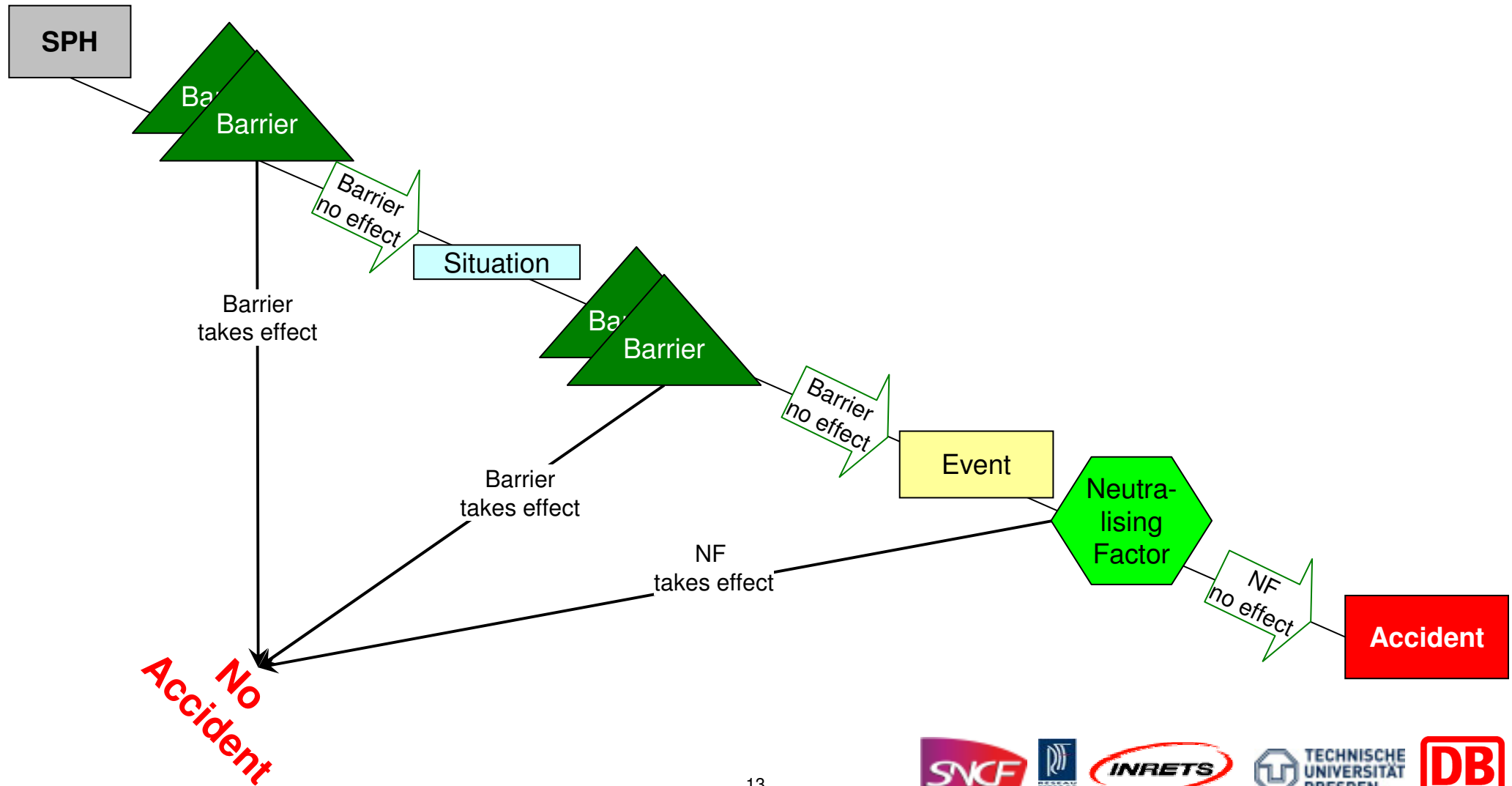
- Mitigates the evolution of hazards
- Technical or operational measure (safety function)
- Characterized by
 - functionality (immanent function of the barrier)
 - occurrence
 - effectiveness

■ Neutralising Factor

- Mitigates the evolution of hazards
- Is no barrier
- Is characterized as (lucky) circumstance, e.g. no train motion



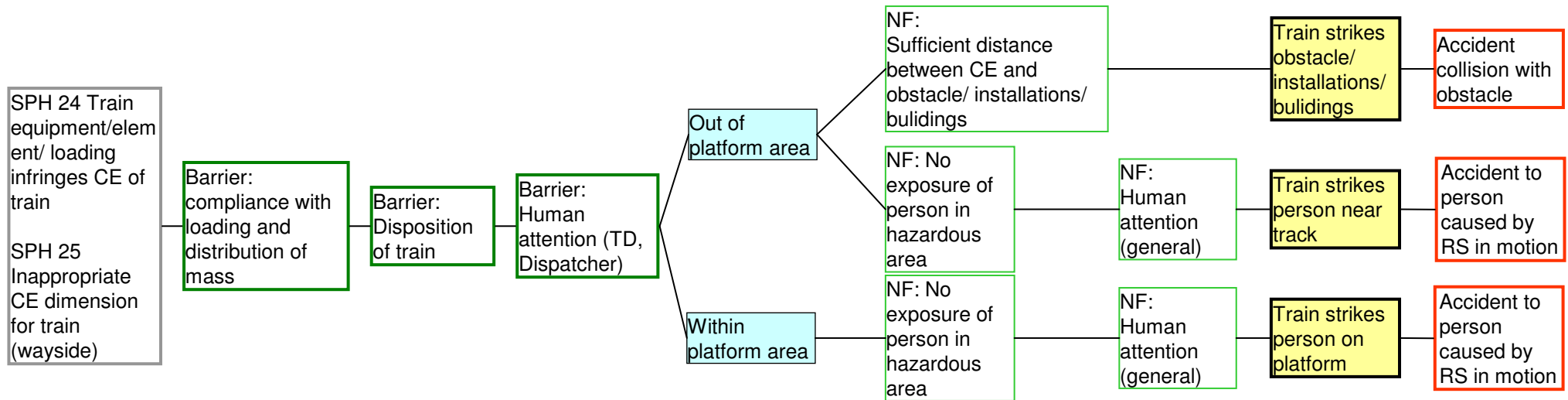
Description of the ROSA Model's Elements: Logical Structure of the Event Trees



Description of the ROSA Model's Elements: Example of an Event Tree

SPH 24
SPH 25

Train equipment/ element/ loading infringes CE of train
Inappropriate CE dimension for train (wayside)



BQM – Barrier Quantification Model

What is the input?

- Specification of potential input data and input mask
- Specification of data structure

How to structure?

- Specification of object model
- Specification of descriptors/ declarations/ nomenclatures/ codes

How to calculate?

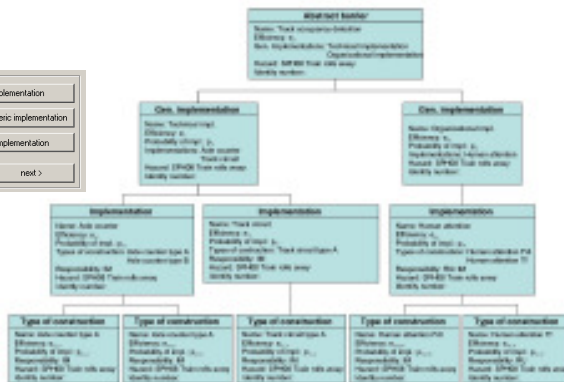
- Specification of algorithms within the BQM

- Specification of interface Database - FaultTree+

$$F = \frac{\sum a_i b_i}{\sum a_i \sum b_i}$$

What is the output?

- Specification of output data and their presentation
- impacts on input / operation/ algorithm

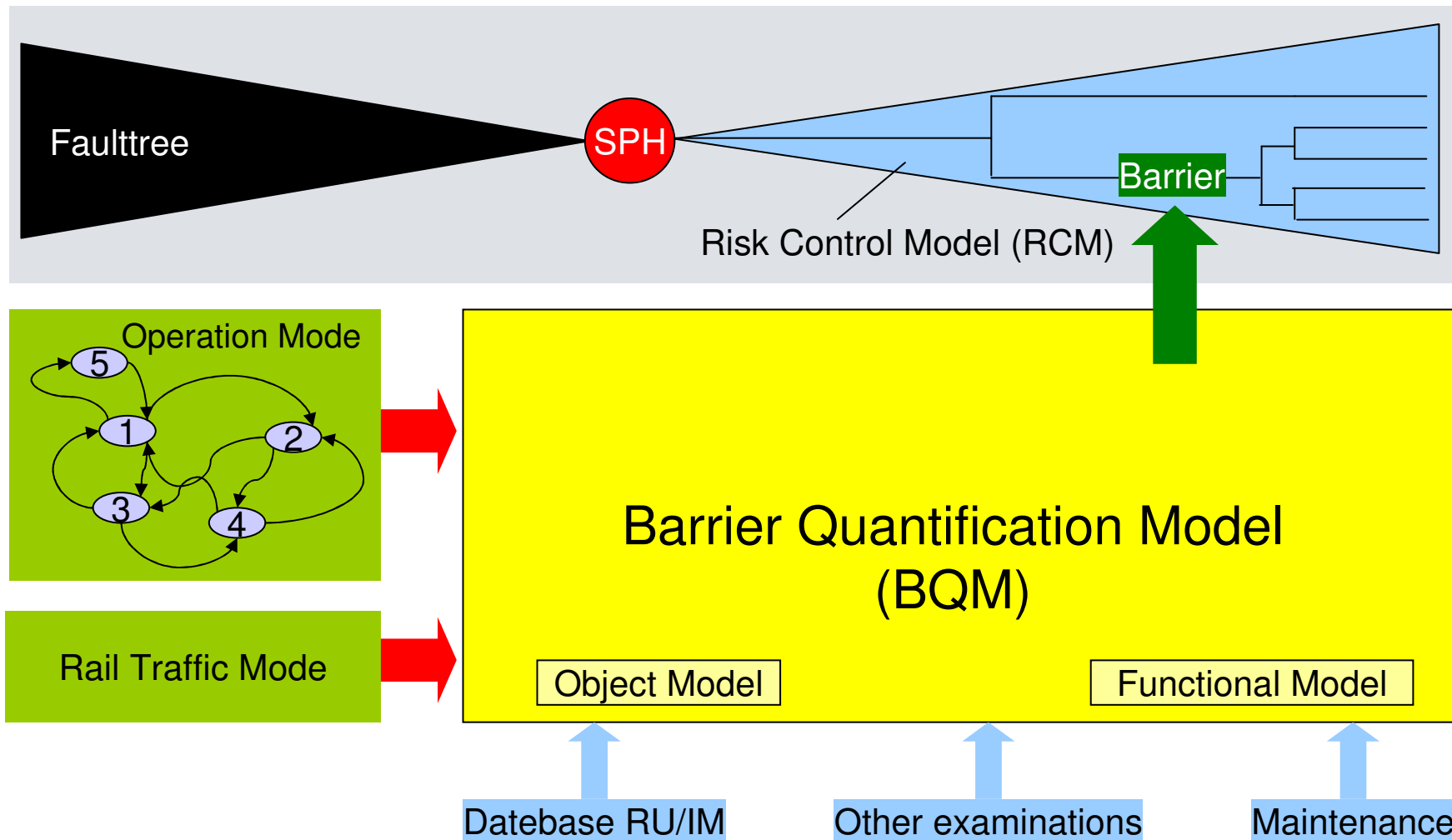


tep 2

Barrier B1	Barrier B2	Init. Event Situation/Location	Barrier B3	Barrier B4	Event
		Event 11			Event 111
	B2 effective	Event 12	B3 effective		Event 121
		Event 13		B4 effective	Event 131
B1 effective	B2 effective			B4 effective	

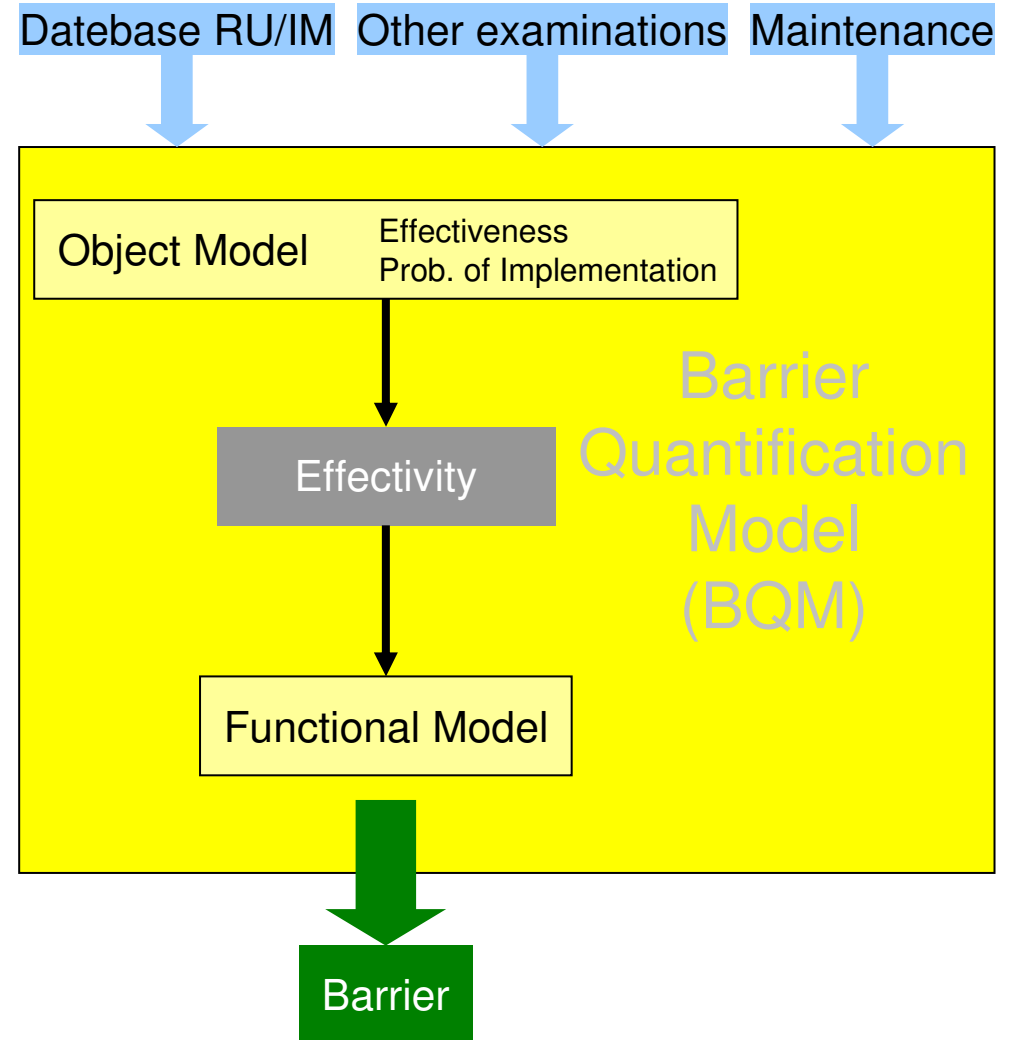


The Barrier Quantification Comprises Two Main Elements



The Barrier Quantification Model Links Generic Safety Functions and their Implementations

- Link between the generic safety functions and their implementations
- Methods of the barrier's quantification
 - Summarises the implementations of the generic safety functions of different subsystems.
- Calculation tool
- Interface between the ROSA model and databases of RU and IM using
 - object model (implementations)
 - functional model (dedicated functions)



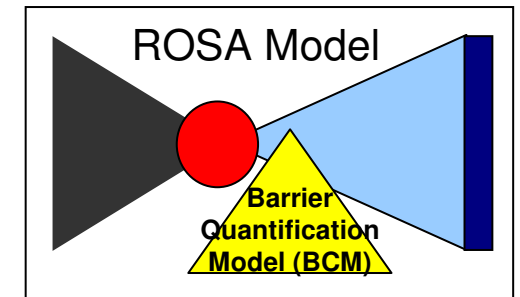
The Main Elements of the Barrier Quantification Model are the Object- and the Functional Models

■ Object Model

- Description of safety components
- Probability of implementation of a safety related component
- Safety related effectiveness of the implied component (related to operation mode and rail traffic mode)
- Resulting effectivity of the implementation (combination of probability of implementation and safety related effectivity)

■ Functional Model

- Apportionment of the implementation's safety related functions to the generic barriers



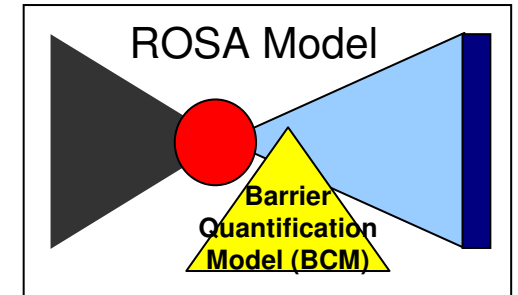
The Barrier Quantification Model Covers Different Modes of Operation and Traffic

■ Operation Mode

- Characterized by certain levels of safeguarding (technical, human)
 - Normal: operation with full safety protection
 - Degraded mode 1: operation with reduced safeguarding level 1
 -
 - Degraded mode n: operation with minimal safeguarding

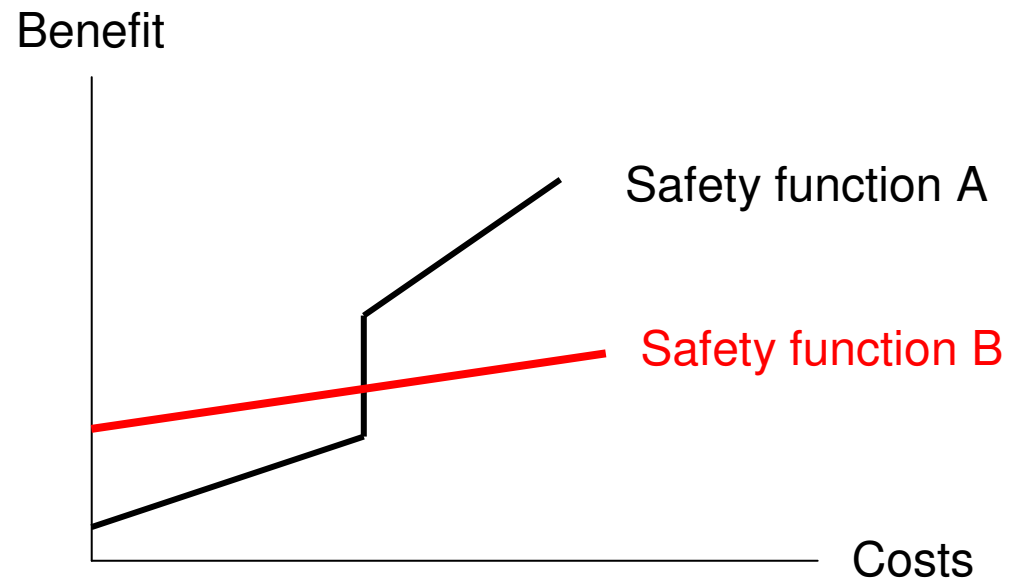
■ Rail Traffic Mode

- Distinguished rail traffic modes characterized by certain safety requirements
 - High speed, conventional, freight, shunting, etc.



ROSA Develops a Method to Consider Cost Benefit Aspects

- Correlation between costs for safety measures and their benefit
- Benefit as combination of safety profit and allocation of safety responsibility
- Balance of several safety measures
- Verification of the CBA with 3 case studies concerning
 - Level Crossing
 - Tunnel
 - SPAD



The Verification is Made by Examples

- Methodology and guideline for introduction of new or modified safety functions (barriers)
- Data available (number of accidents, incidents and failure) before and after the introduction / modification
- Examples
 - Hot axle detection
 - technical sub-system without operator and requiring specific maintenance conditions
 - Automatic Train Control
 - technical sub-system with operator and requiring easy maintenance conditions

The Results of ROSA are Generic

- List of Hazards
- List of Barriers
- List of Barriers related to a Hazard and Accident(s)
- List of implementations mapped to Barriers
- Method of cross system CBA related to safety aspects

ROSA
Rail Optimisation Safety Analysis

Thank You for Your Attention!

Deutsche Bahn AG

Rüdiger PÜTTNER, Marc GEISLER

IRSC 2008, Denver

