

# Train control systems: Trends, requirements and possibilities



SAF-SE 2008-056, 2008-10-07

**Tomas L Persson, PGR/3VEA**  
**Specialist – Product safety**

**BOMBARDIER**

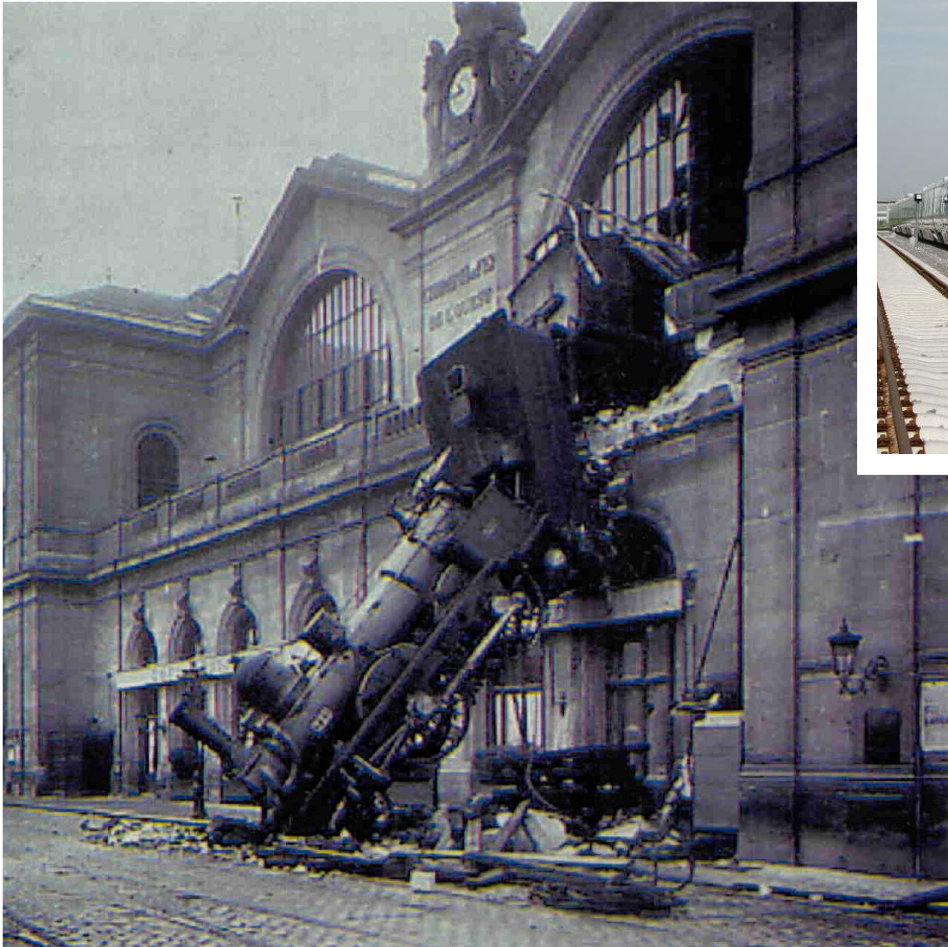
# Agenda

- **History, trains of today and in the future**
  - with respect to communication and control
- **Customer and authority requirements – cultural differences**
- **Strategies**
- **Solutions**
  - standardised hard-ware, operating systems etc.
  - SIL-classification

# Historically also conventional control systems have failed

SAF-SE 2008-056

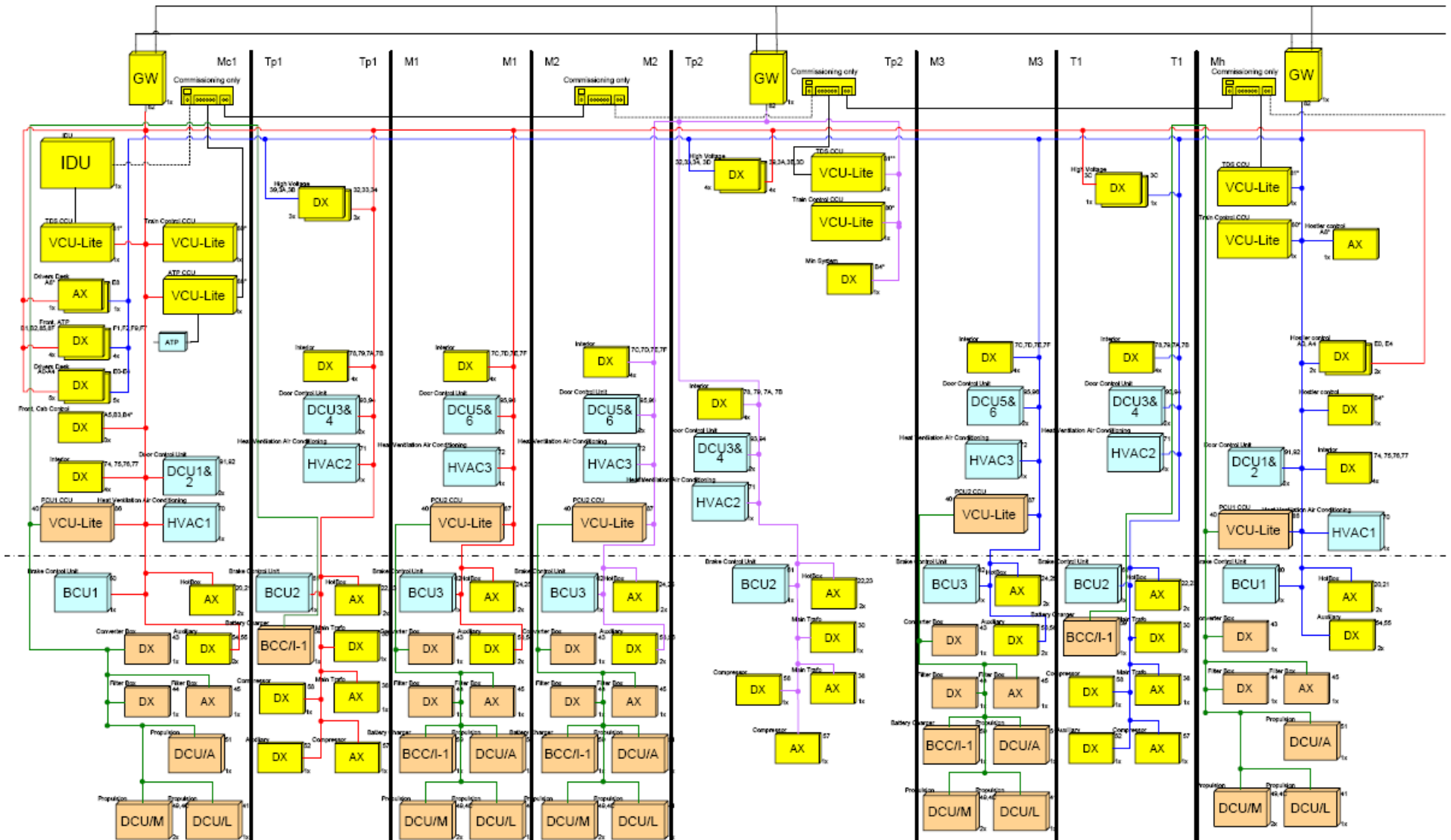
France 1895



China 2008

# Example of train control and communication network on a modern train (CRH-project for China, 50% of the network)

SAF-SE 2008-056



MLN PPC External 2008-04-15 16:57

# Control and communication through hard-wired train lines or TCMS?

## Traditional trains

- **purely hard-wired control and communication**
  - + possible to analyse
  - a lot of relays, cables and problems in couplers
- **some projects ~145 train lines**

## Modern trains of today

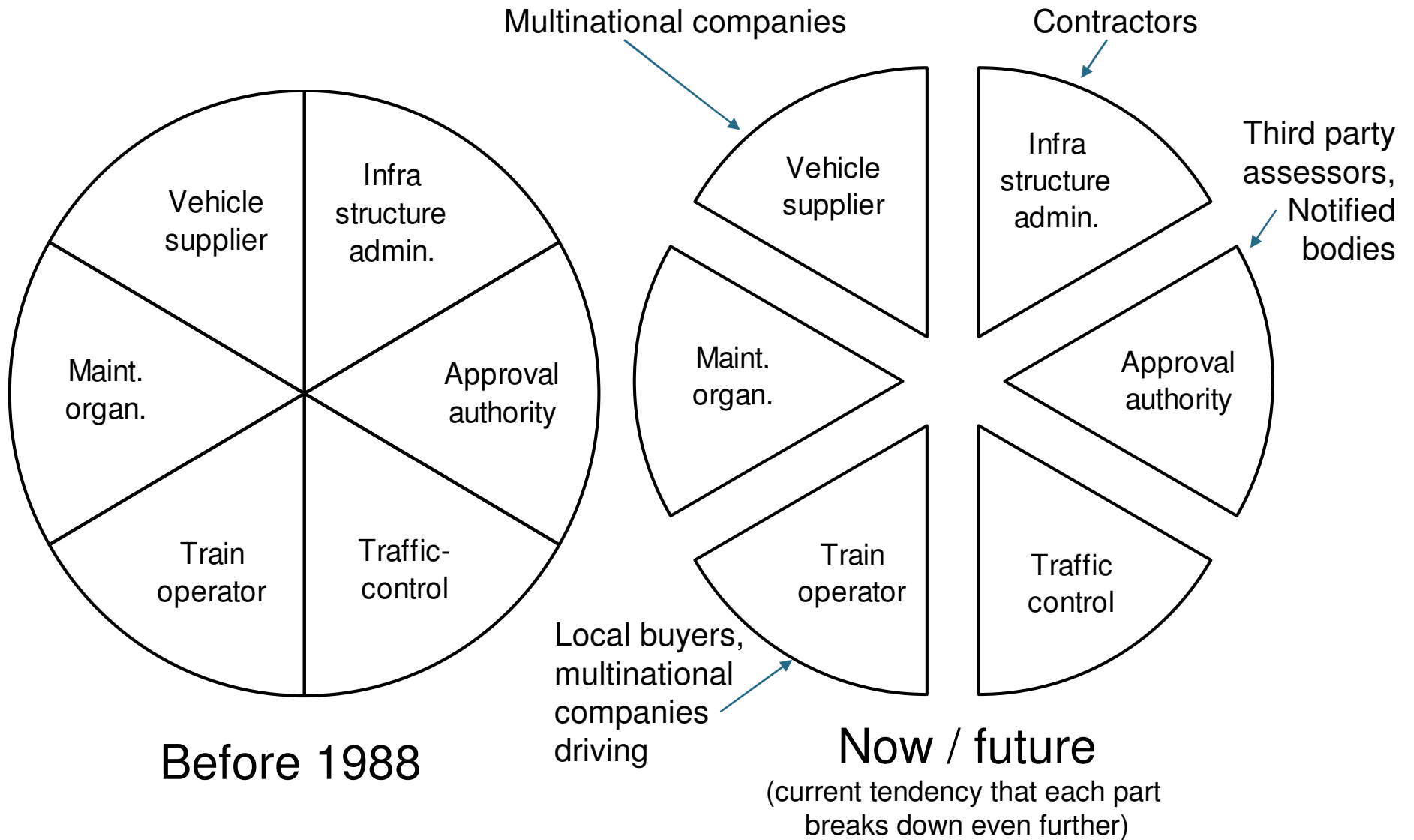
- **hard-wired control and communication of a few safety critical functions**
- **TCMS control also of safety related functions**
  - + less weight of cables
  - + easy to update functionality
  - + better reliability
  - can not be analysed (need to be SIL classified and developed according to strict processes)
- **can be enough with ~20 to 30 train lines**

## “Future” trains

- **completely controlled by TCMS /software**
- **no hard-wired train lines**
  - + very few train lines (power supply and data buses)
  - some functions require higher SIL-levels on both hardware and software in TCMS
- **can be enough with ~10 train lines**

TCMS = “Train Control and Communication System”

# Railway industry in Sweden (and Europe)



# Railway Safety Standards

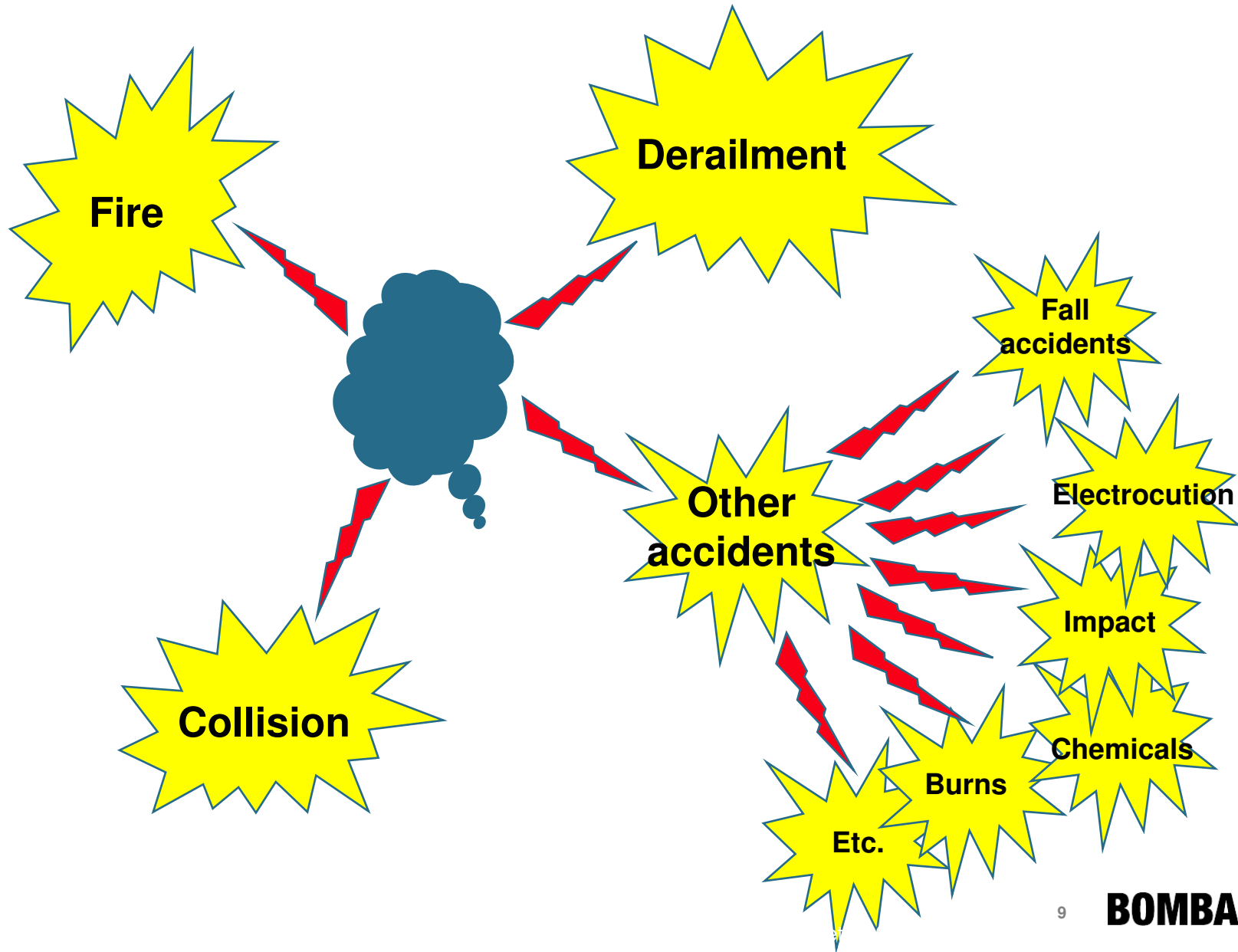
- **EN 50126 – The Specification and Demonstration of RAMS**
  - Process requirements
- **EN 50128 – Communication, Signalling and Processing System Software for Railway Control and Protection Systems**
  - Software
- **EN 50129 – Safety Related Electronic Systems for Signalling**
  - System and Hardware
  - Standard specifying the format of a Safety Case
- **IEC 61508 – Functional Safety of electrical / electronic / programmable electronic safety-related systems**
  - 50126, 50128, 50129 is the railway specific interpretation of 61508
  - 61508 used for guidance
- **EN 50159 – Safe Communication**
  - Railway applications. Communication, signalling and processing systems. Safety related communication in open transmission systems
- **Various TSI's – Technical Specification for Interoperability**
  - EN process for interoperable railway traffic

## The SIL System

- SIL comprises two aspects of the products
  - **Quantitative** (system and hardware) EN50129
  - **Qualitative** (mainly software , but also hw process) EN50128
- Both aspects need to be fulfilled to claim a SIL level
- **In simple terms**
  - **Make the software sufficiently free from systematic errors so the hardware platform random failures dominate**
  - Then the SIL level can be used to determine the hazard rate for the hardware platform on which the software is executed
- **Hardware** -> Functional: FMEA, FMECA, FTA for random failures to fulfil **EN50129**
- **Software** -> Procedural: Process for systematic failures to fulfil **EN50128**

SIL = “Safety Integrity Level”

# Identified accident types 1(2)



## Identified accident types 2(2)

### Accident causes

- Infrastructure failures
- Human errors
- Vehicle failures

### Influencing factors

- infrastructure
  - tunnels, bridges, level crossings, signalling
- traffic situation
  - traffic density, traffic control, drivers, passengers, vandalism
- owner situation
  - maintenance
- vehicle design

### Accident types

#### *Major accidents*

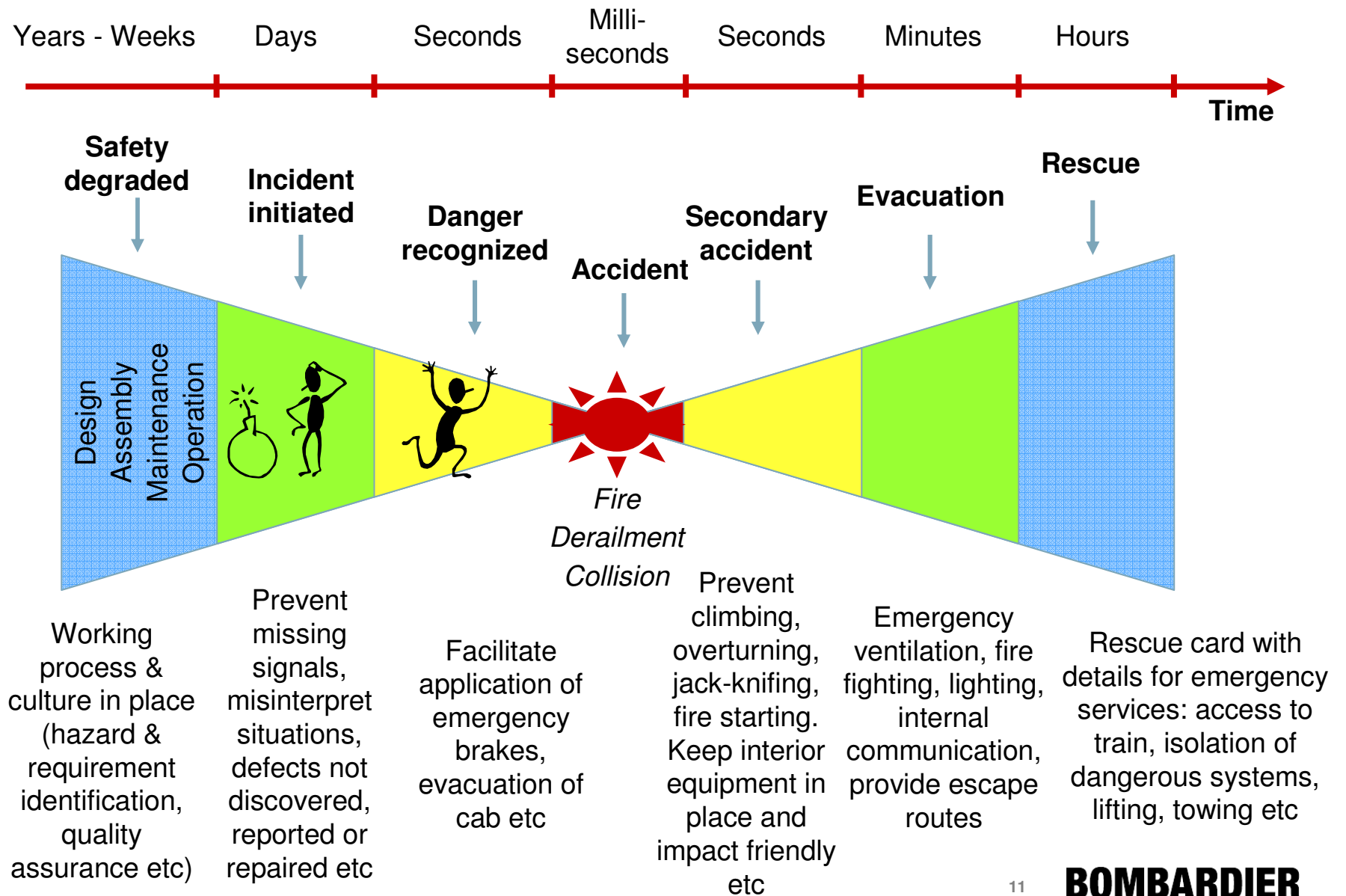
- fire
- derailment / overturning
- collision

#### *Minor accidents*

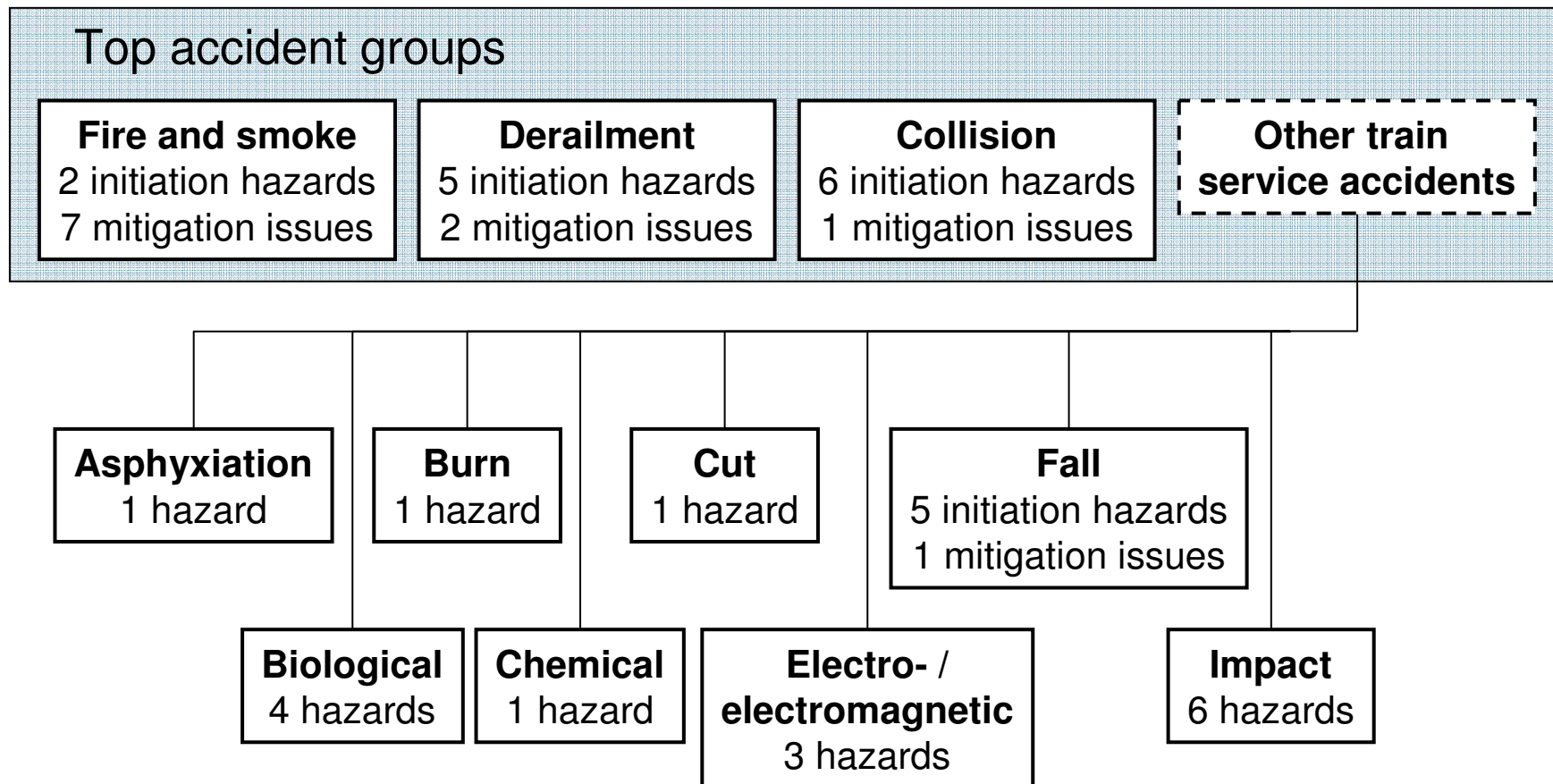
- falls from exterior doors
- maintenance accidents
- other accidents

# Accident Development

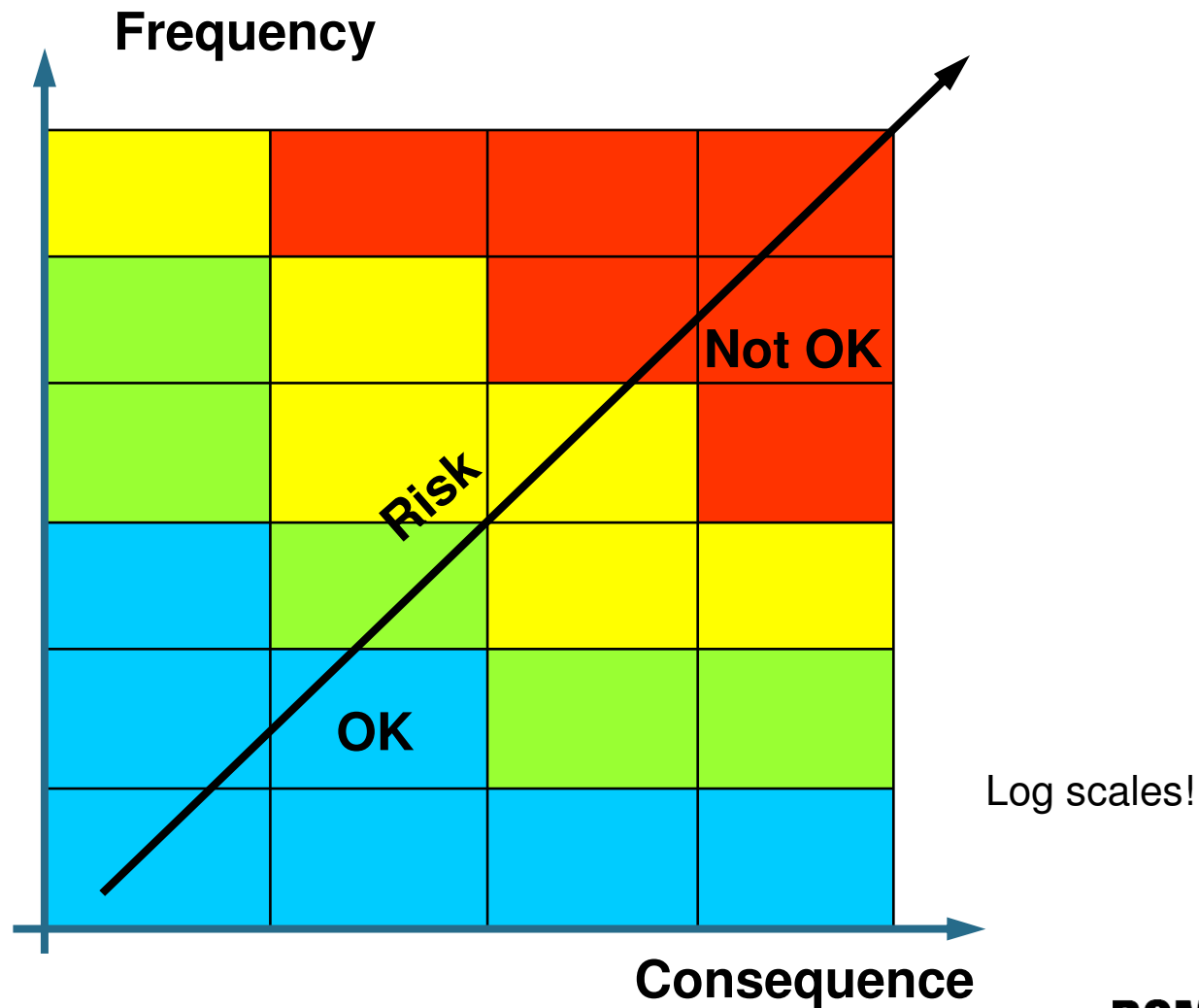
SAF-SE 2008-056



## Generic top level hazards for preliminary hazard analysis (PHA)



# EN 50126 (European railway RAMS standard): Safety = Freedom from unacceptable risk of harm



## Perception of risk

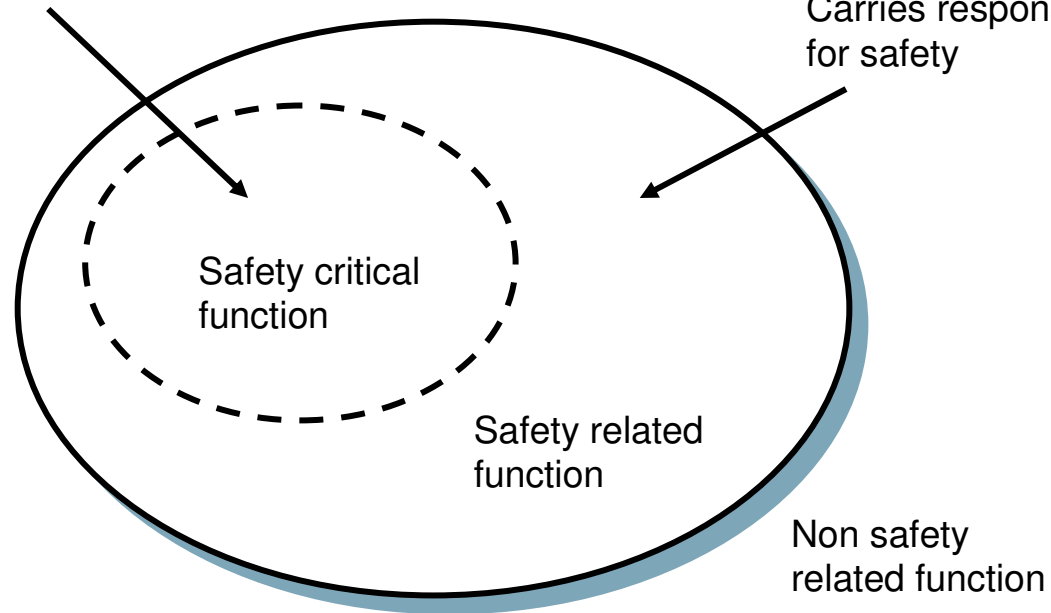
- **Safety and acceptable level of risk differ between countries and activities**



## Definition of Safety related vs safety critical functions (EN 50129)

Carries direct responsibility for safety and  
has a potential severity class S3 - S4

Carries responsibility  
for safety



## In what ways can the train control system cause severe accidents?

- **Failing emergency brake**
- **Traction applied uncontrolled**
- **Exterior doors open at speed**
- **(Failure to cut out power supply)**

can be handled by  
hard-wired relay  
redundancy!

**And that is sometimes all... (if more critical functions = put in a separate, higher SIL-classified system, in parallel)**

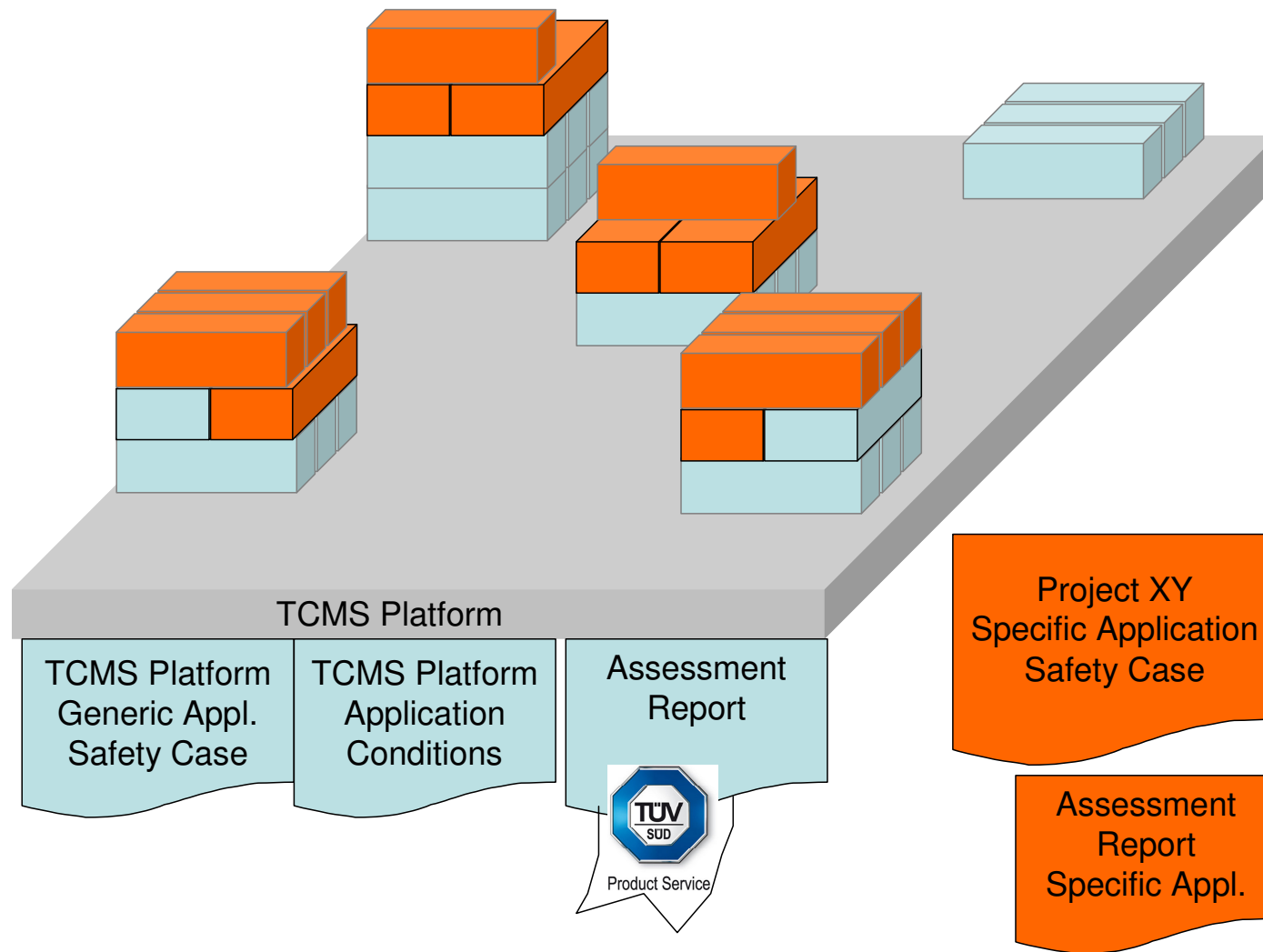
**= the rest of TCMS can be treated as safety related, SIL1 functions (provided that there is a working ATP system and that fire hazards etc. are handled within each local function)**

**ATP = “Automatic Train Protection system”**

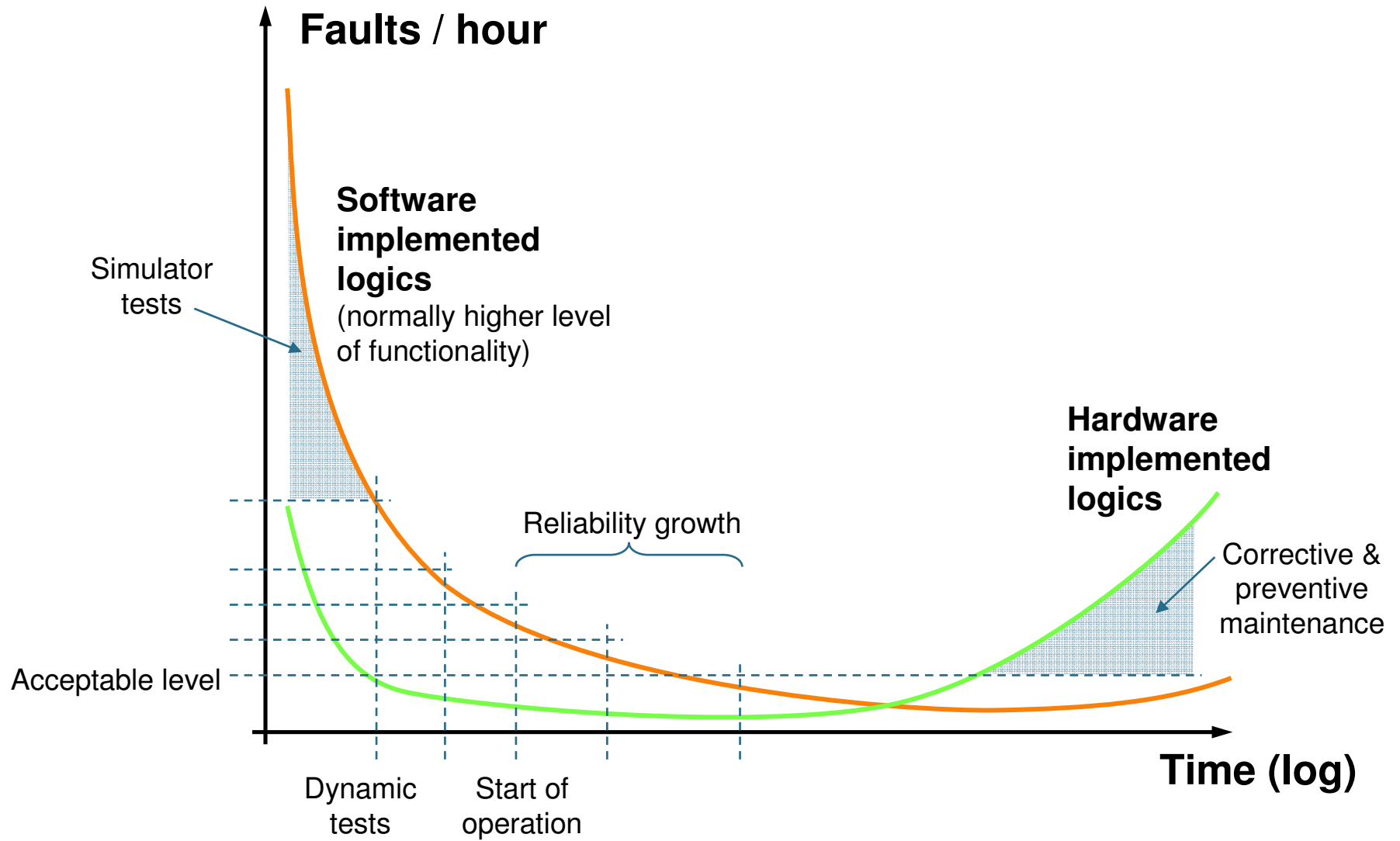
## Development of new TCMS platform

- **BT is currently working on a TÜV certified SIL2 platform for TCMS, including hardware, operating system, compilers etc., based on four “sharp” pilot projects**
- **This will be used in most project in the future, easier to follow the same development processes, independent of customer / authority requirements**
- **Application software is already being developed in accordance to SIL requirements >0 in some projects**
  - in DM2 project all TCMS software is developed according to SIL1 processes, independent of function
- **Five basic TCMS requirements are identified:**
  1. Read and store information
  2. Safe data communication
  3. Read inputs and set outputs for digital and analogue TCMS interfaces, including virtual inputs and outputs on the display devices
  4. Recognise train configuration, inauguration and direction
  5. Provide logic and processing functions for train level systems

# TCMS Application for one project, with the specific application software (red) built on the platform



# Improvement of reliability – TCMS versus train line logics for control



## Conclusion

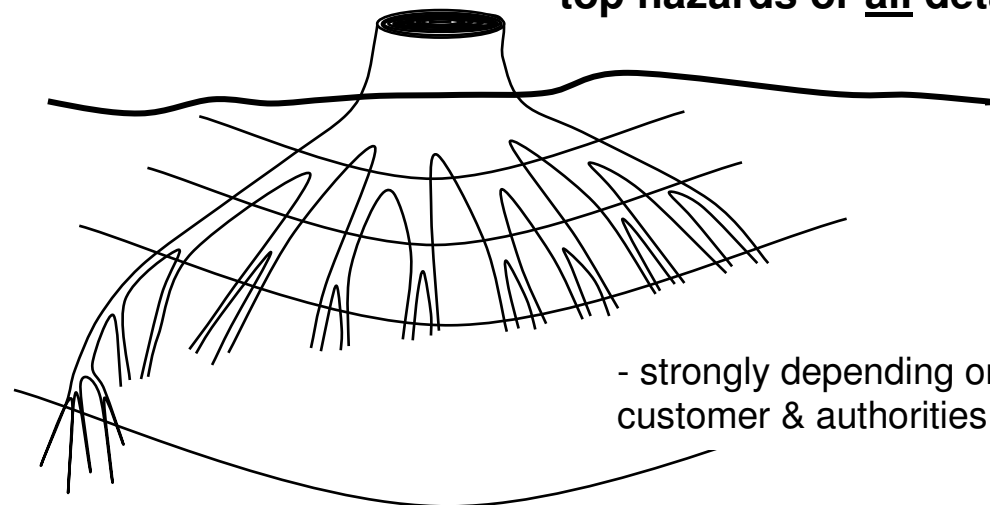
**Future trains will be increasingly software controlled and this, in combination with:**

- increased authority requirements
- globalisation
- complex organisations

**will put focus on software development and SIL processes to ensure safety**

**(...and ensure approval)**

**How deep do we need to dig? Documentation of top hazards or all details?**



- strongly depending on customer & authorities