MODSafe

Modular Urban Transport Safety and Security Analysis

Final Conference
25 – 26 June 2012, Cologne

Safety Functions and Safety Integrity Requirements

presented by Dr Sven Scholz
TelSys GmbH, Germany

SEVENTH FRAMEWORK PROGRAMME

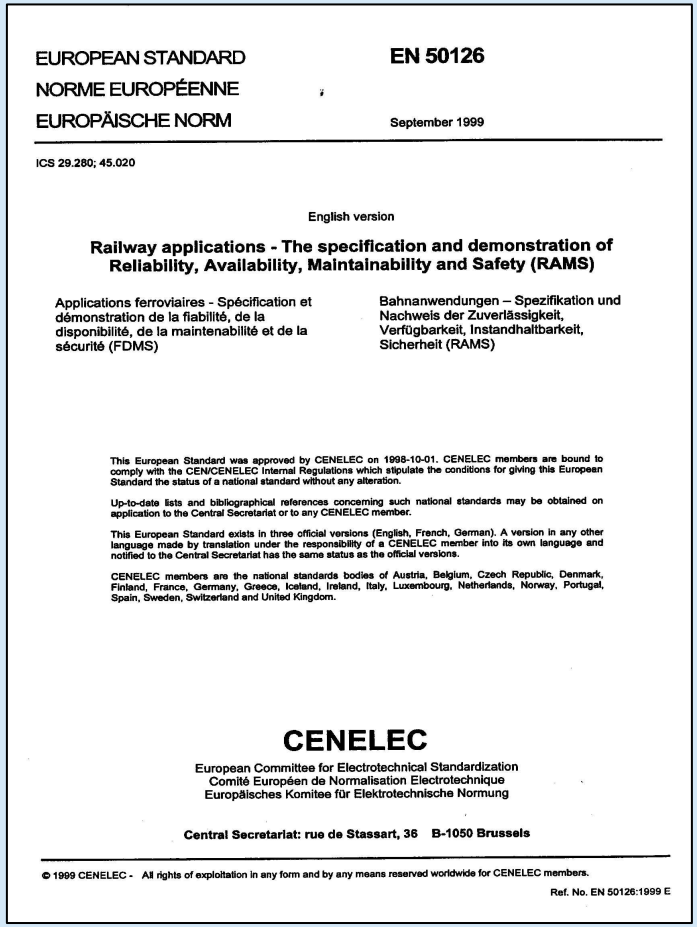
UITP EUROPEAN UNION

MODSafe

Table of Contents

Introduction

Need for systematic Safety Requirement Allocation



EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50126

September 1999

ICS 29.280; 45.020

English version

Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)

Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)

This European Standard was approved by CENELEC on 1998-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

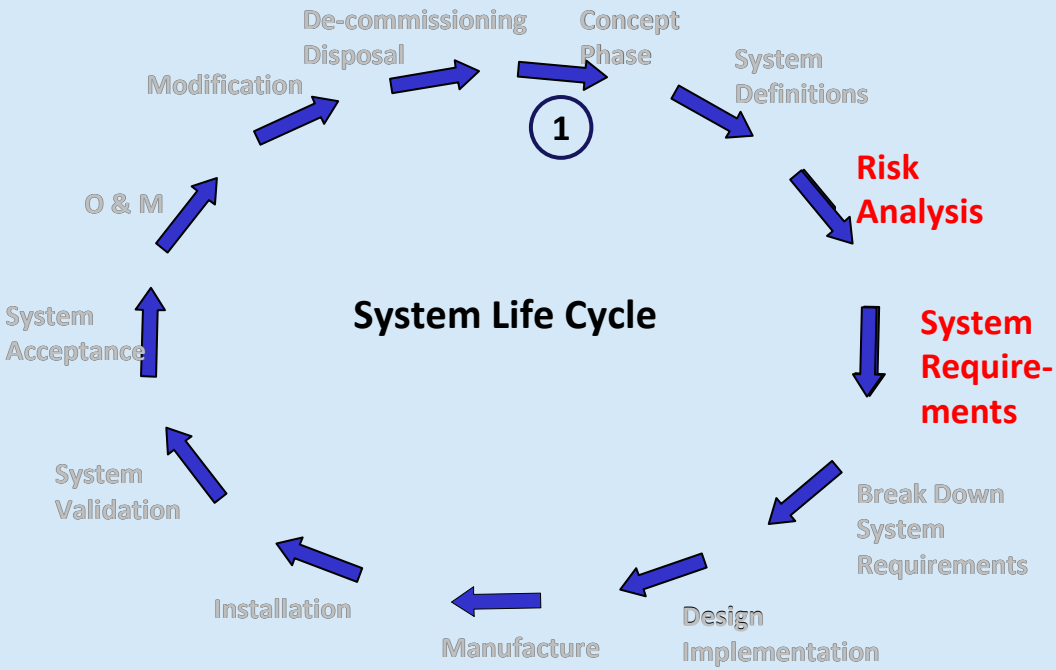
CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart, 36 B-1050 Brussels

© 1999 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 50126:1999 E



- *"Specify System Safety Requirements (Overall)*
- *Define Safety Acceptance Criteria (Overall)*
- ***Define Safety Related Functional Requirements***
- *Establish Safety Management"* *(EN50126)*

Introduction

Involved partners

- *"Specify System Safety Requirements (Overall)*
- *Define Safety Acceptance Criteria (Overall)*
- ***Define Safety Related Functional Requirements***
- *Establish Safety Management"* *(EN50126)*

Involves
- Operators,
- Industrial Suppliers
- Independent Experts

work package leader

Introduction

“Safety Measures” shall cover HAZARDS, but

Important Questions:

- How safe do these Measures have to be? Reduce the probable worst case risk associated with the hazard to an acceptable rate!
- How to calculate/allocate? (available schemes)
- Special case of low demand functions (“rare” demands, neutralizing factors etc.) → how to calculate safety requirements

Objectives and Mode of Work

Step 1

State of the Art Analysis

Various methods to allocate safety requirements exist

- Risk Graph (IEC 61508)
- Risk Matrix (EN 50126)
- MODUrban Method
- MODTrain Method
- Recommendation by ERA (European Railway Agency)
- Recommendations by the British Yellow Book
- Methods by specific Urban Guided Transport Operators
- …

General characteristics

- repeatable (with same results),
- straight forward use
- some methods require availability of extensive statistics
- All yield identical /very similar results for classic Train Control Safety Functions,

  e.g. Interlocking and Signal safety such as Route Supervision, Signal Supervision

Step 2

Application to MODSafe Safety Functions to derive Safety Integrity Requirements

MODSafe Safety Functions

Basic functions of train operation		On-sight train operation GOA0	Non-automated train operation GOA1	Semi automated train operation GOA2	Driverless train operation GOA3	Unattended train operation GOA4
Ensuring safe movement of trains	Ensure safe route	x (points command/control in system)	system	system	system	system
	Ensure safe separation of trains	x	system	system	system	system
	Ensure safe speed	x	x (partly supervised by system)	system	system	system
Driving	Control acceleration and braking	x	x	system	system	system
Supervising guideway	Prevent collision with obstacles	x	x	x	system	system
	Prevent collision with persons on tracks	x	x	x	system	system
Supervising passenger transfer	Control passengers doors	x	x	x	x	system
	Prevent person injuries between cars or between platform and train	x	x	x	x	system
	Ensure safe starting conditions	x	x	x	x	system
Operating a train	Set in/set off operation	x	x	x	x	system
	Supervise the status of the train	x	x	x	x	system
Ensuring detection and management of emergency situations	Perform train diagnostic, detect fire/smoke and detect derailment, handle emergency situations (call/evacuation, supervision)	x	x	x	x	system and/or staff in OCC
NOTE x = responsibility of operations staff (may be realised by UGTMS system) System = shall be realised by UGTMS system						

Source: IEC62290

Generic Safety Requirement Allocation for Continuous Mode Functions

STEP 1

Estimation of *Tolerable Hazard Rate*

Severity of consequences:

Catastrophic	THR = 10^{-9}/h
Critical	THR = 10^{-8}/h
Marginal	THR = 10^{-7}/h
Insignificant	THR = 10^{-6}/h

STEP 2

Estimation of *Risk Reduction Factors* (limit the risk by orders of magnitude)

Exposure of members:

Frequent	E = 1
Rare	E = 0.1
Very rare	E = 0.01

Accident reduction:

No barrier	A = 1
One barrier	A = 0.1
Two barriers	A = 0.01

Consequence reduction:

No barrier	C = 1
One barrier	C = 0.1
Two barriers	C = 0.01

STEP 3

Derive required Safety Integrity Requirements (SIL)

$$\mathbf{SIL} = \frac{\mathbf{Severity}}{\mathbf{E * A * C}}$$

Safety Integrity Level:

THR = 10^{-9}/h - 10^{-8}/h → **SIL 4**
THR = 10^{-8}/h - 10^{-7}/h → **SIL 3**
THR = 10^{-7}/h - 10^{-6}/h → **SIL 2**
THR = 10^{-6}/h - 10^{-5}/h → **SIL 1**

Generic Safety Requirement Allocation for Continuous Mode Functions

Item		Description
Name of safety function		**Lock route**
Description		This function is intended to lock the route against route release by operator command if a train is approaching and the movement authority allows entry into route, or a train is within the route.
Reference of functions		IEC 62290-2 – 5.1.1.1.3
Reference for risk analysis		None
Possible wrong side failure		No inhibition of movement of moveable route elements
Hazardous situation		Train movement into unsecured route
Possible hazard consequences – accidents		Derailment due to overspeed or moving switch while train passing Collision with oncoming train or flank movement
Exposure probability to hazard		Passengers are permanently onboard of trains
Accident probability reduction		No barrier can be assumed
Consequence reduction probability		Passenger cannot escape from hazard consequences
Severity of consequences due to failure of safety function		Catastrophic
Initial THR per hour		10^{-9}
Risk reduction factors	E	1
	P	1
	C	1
Final THR		10^{-9}
Final SIL		**SIL 4**

Generic Safety Requirement Allocation for Continuous Mode

Extract from overall table

	Nr.	Safety function	Safety integrity level				
			GOA0	GOA1	GOA2	GOA3	GOA4
Ensure safe movement of trains	(1)	Check route availability	---	4	4	4	4
	(2)	Set route	3	4	4	4	4
	(3)	Supervise route	---	4	4	4	4
	(4)	Supervise level crossing as secured	---	3	3	---	---
	(5)	Lock route	---	4	4	4	4
	(6)	Release route	---	4	4	4	4
	(7)	Initialise UGTMS reporting trains location	---	4	4	4	4
	(8)	Determine train orientation	---	4	4	4	4
	(9)	Determine actual train travel direction	---	4	4	4	4

(Report: *Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions*)

Specific Safety Requirement Allocation for Low-Demand Mode

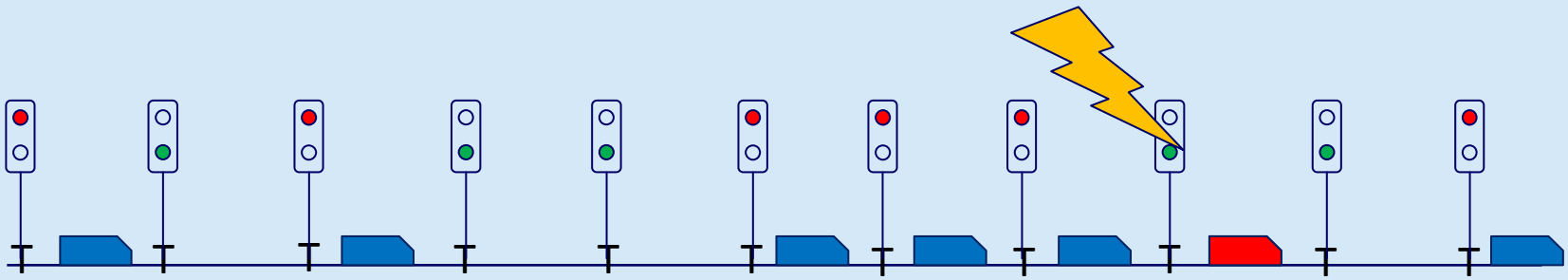
Typically, most safety functions are required to work all the time (continuously)

– hazardous situations are immanent (immediate prevention from accidents necessary)

– Examples:

- Stop Signal Supervision
- Route Lock Supervision
- Flank Protection

usually vital functions,
i.e. SIL3/SIL4 safety integrity requirement



Specific Safety Requirement Allocation for Low-Demand Mode

Some (special) safety measures exist, which are not continuously required

- failure of safety measure does not immediately lead to a dangerous situation
- high safety requirements probably too conservative,
- safety function used only at a low rate

- Examples:
  - Fire Detection
  - Derailment Detection
  - Guideway Intrusion Detection

Analysis of Low-Demand Safety Functions

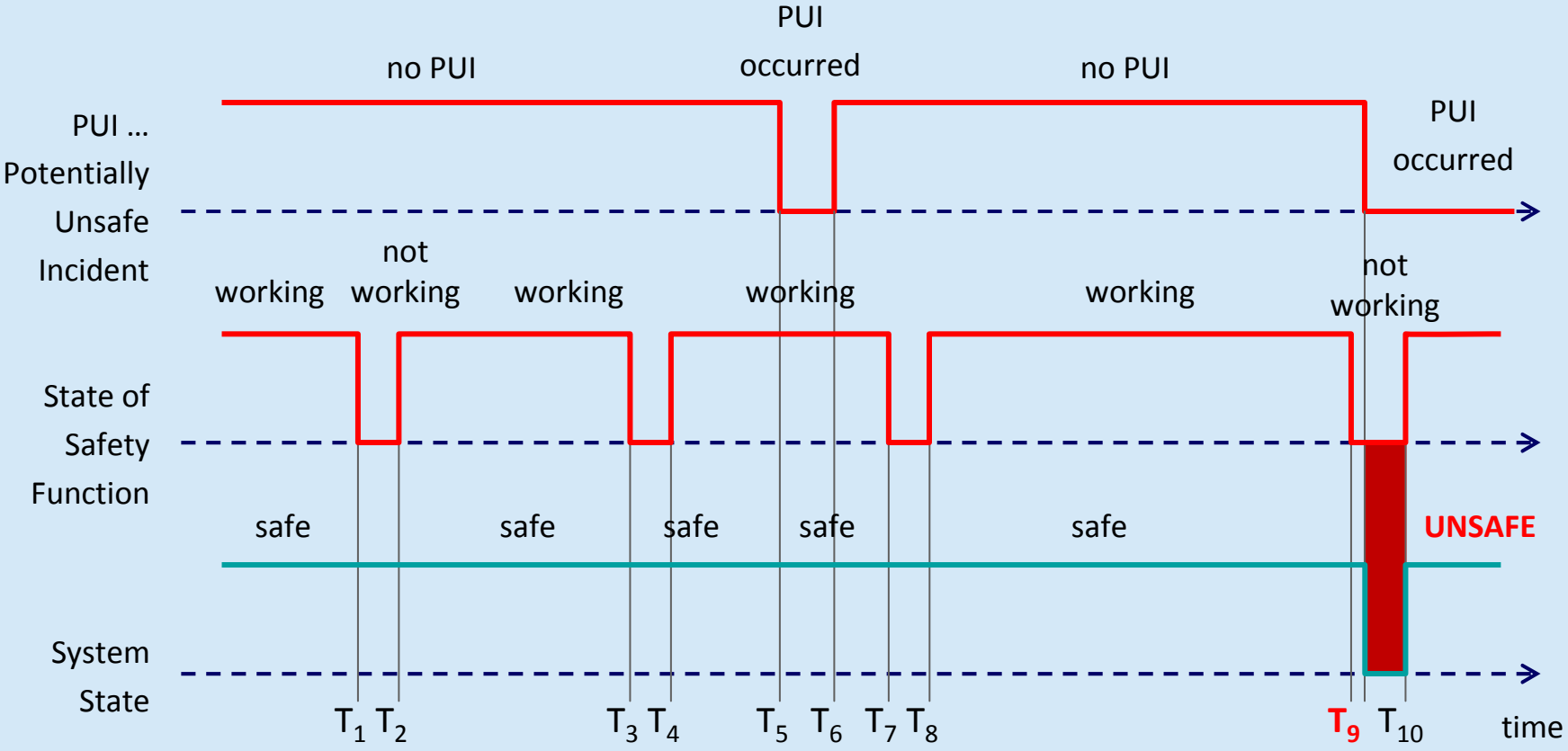
→ Identify impacting factors

→ Develop method for safety requirements

→ Apply method to example safety measures

Specific Safety Requirement Allocation for Low-Demand Mode

Context of system failure and utilization of safety function over time



Unsafe System State due to failure of Safety Function at T_9 and occurrence of Incident at T_{10}

Specific Safety Requirement Allocation for Low-Demand Mode

Context of system failure and utilization of safety function

In principle, we have two independent variables

1. state of the safety function
2. potentially unsafe incident

which can have 2 states each

1.working / failed
2. not occurred / occurred

this yields 4 different states in total

State of the safety function / safety element

Potentially Unsafe Incident (hazardous situation)

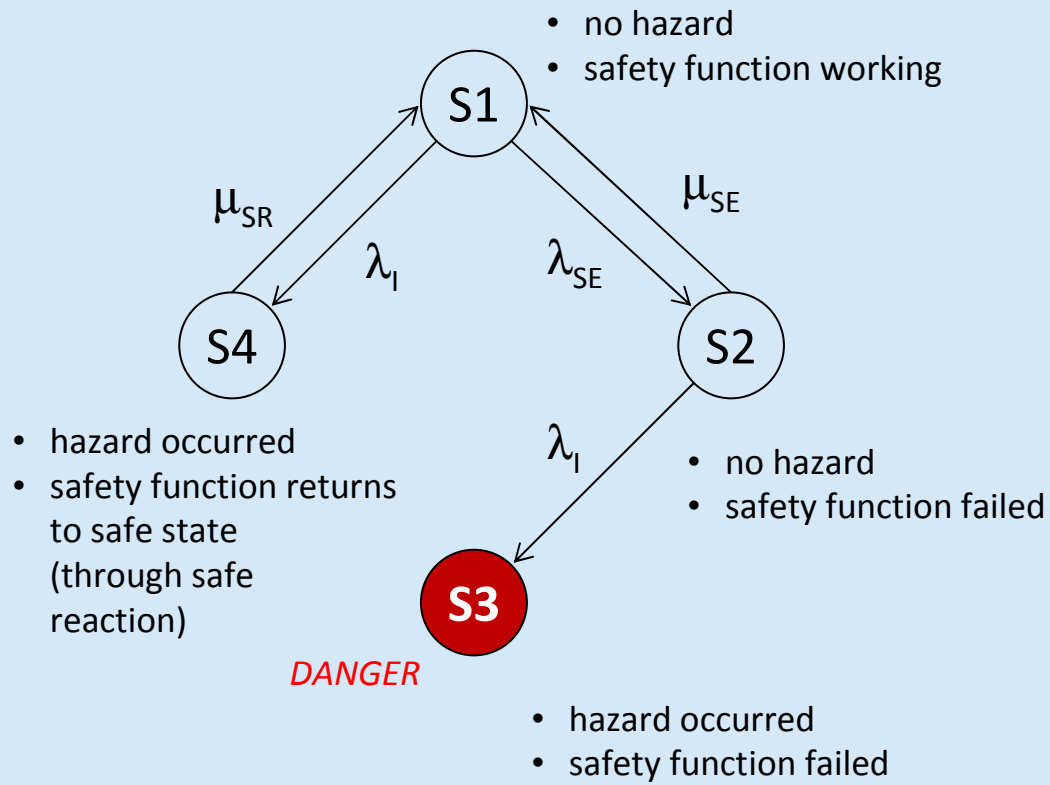
	Working	failed
not occurred	S1	S2
occurred	S4	**S3**

Specific Safety Requirement Allocation for Low-Demand Mode

Relevant from safety point of view:

Limit value for State S3:

- "failure rate" λ_{sys}
- frequency with which the system develops into a dangerous state (accident)



Total System Failure Rate

$$\boxed{\lambda_{sys} = \frac{\lambda_{SE}\lambda_I}{\mu_{SE}}}$$

$$\lambda_{sys} \triangleq THR \rightarrow \frac{THR}{\lambda_I} = \frac{\lambda_{SE}}{\mu_{SE}}$$

λ_{SE} … failure rate of the safety function, e.g. /h

μ_{SE} … repair/inspec. rate of the safety function, e.g. /h

λ_I … hazard occurrence rate, e.g. /h

Specific Safety Requirement Allocation for Low-Demand Mode

Item	Description
Name of safety function	**Supervise platform tracks**
Description	This function is intended to supervise the actions of an external platform track detection device to stop the train in case of intrusion of person.
Reference of functions	IEC62290-2
Reference for risk analysis	None
Possible wrong side failure	Device does not detect person on platform tracks
Hazardous situation	Person on platform tracks while train is approaching the station.
Possible hazard consequences	Collision of train with person on track. Maximum one fatality

1. Severity of consequences in case the safety function fails — Critical → required THR $10^{-8}/h$
2. hazard occurrence rate λ_I — assume a hazard occurrence rate for a person on the track, once a year — $\lambda_I = 10^{-4}/h$
3. required failure probability on demand

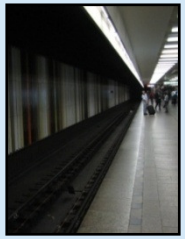
$$\frac{THR}{\lambda_I} = \frac{10^{-8}/h}{10^{-4}/h} = 10^{-4}$$

4. required wrong side failure rate λ_{SE} of the safety function
5. required inspection rate μ_{SE}

$$\frac{\lambda_{SE}}{\mu_{SE}} = \frac{10^{-3}/h}{10^{+1}/h} = 10^{-4} \triangleq \frac{THR}{\lambda_I}$$

Summary

1. Survey of existing Safety Requirement Allocation Methods & Safety Requirements Allocation scheme agreed among MODSafe partners
2. Safety Integrity Requirements defined for most of MODSafe Continuous Safety Functions (Classical Train Control Functions)
   - can be used as guideline for Urban Transport System Stakeholders
   - specific conditions of different applications can be respected
3. New quantitative Requirement Allocation method for Low Demand Safety Systems



TelSys

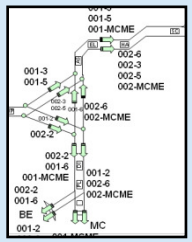
Railway Systems Engineering

RAMS / LCC Engineering

Guideway Intrusion Detection Systems

ETCS Engineering

Thank you for your attention.



TelSys GmbH
Werdauer Str. 1-3
01069 Dresden, Germany
Tel.: +49 (351) 47 55 110
Fax.: +49 (351) 47 55 120
office@telsys-gmbh.de