Náhled do definice hazardních stavů systému CBTC (Communication Based Train Control)

Ing. Luboš Janhuba, Ph.D.

SIEMENS

Autor

Ing. Luboš Janhuba, Ph.D.

Stavba letadel (magisterské studium FSI VUT v Brně), 2011

Procesní inženýrství (doktorské studium FSI VUT v Brně), 2011-2018

Výzkumný pracovník (VUT FSI, Letecký ústav), 2012-2019

RAMS Manager (Siemens Mobility, s.r.o.), 2020- dosud

SIEMENS

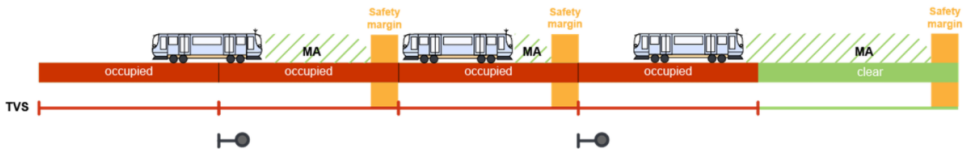
Co je CBTC?

IEC 62290-1:2025: Urban guided transport management and command/control systems (UGTMS)

SIEMENS

CBTC (Communication Based Train Control)

	Speed measurement	Position measurement	Track/train communications	Train tracking
Classic FB	-	-	Signal	per block
Intermittent FB (ITC)				
Distance to go				
Moving block (CTC)				



	Speed measurement	Position measurement	Track/train communications	Train tracking
Classic FB	-	-	Signal	per block
Intermittent FB (ITC)	continuous	continuous	Intermittent LEU/balise	per block
Distance to go	continuous	continuous	continuous, unidirectional	per block
Moving block (CTC)				

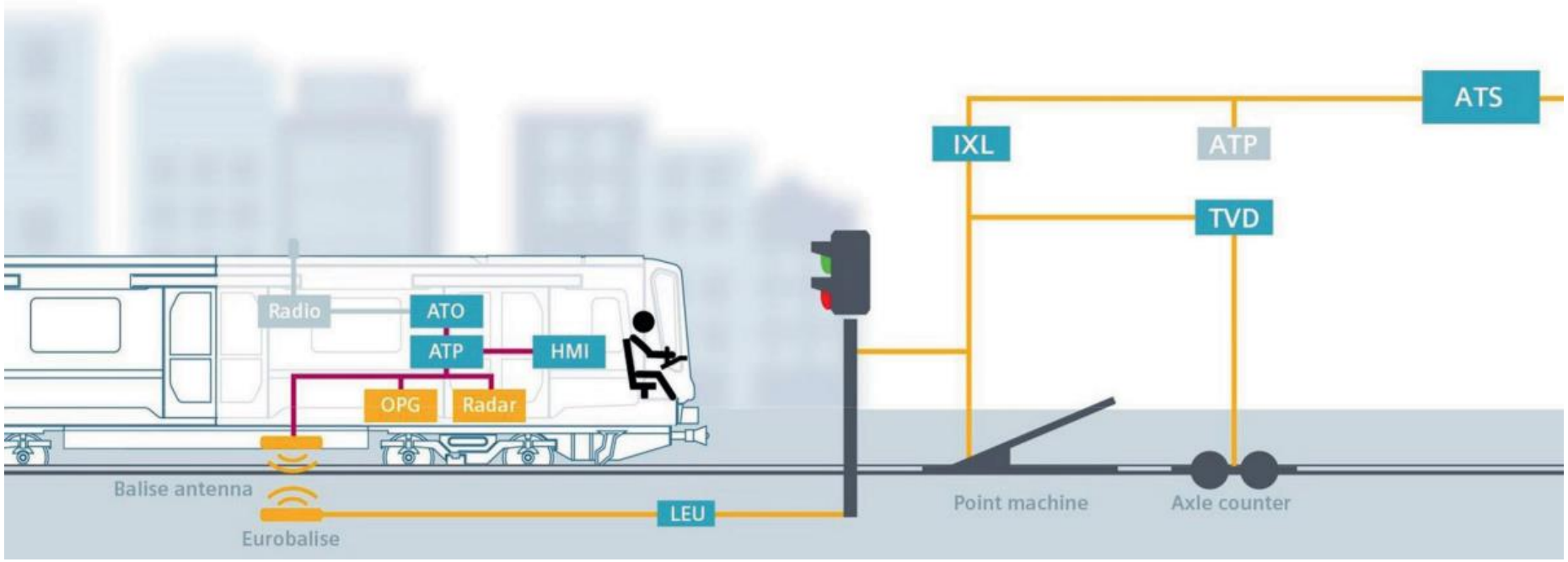
	Speed measurement	Position measurement	Track/train communications	Train tracking
Classic FB	-	-	Signal	per block
Intermittent FB (ITC)	continuous	continuous	Intermittent LEU/balise	per block
Distance to go				
Moving block (CTC)				

	Speed measurement	Position measurement	Track/train communications	Train tracking
Classic FB	-	-	Signal	per block
Intermittent FB (ITC)	continuous	continuous	Intermittent LEU/balise	per block
Distance to go	continuous	continuous	continuous, unidirectional	per block
Moving block (CTC)	continuous	continuous	continuous, unidirectional	continuous

SIEMENS

CBTC (Communication Based Train Control)

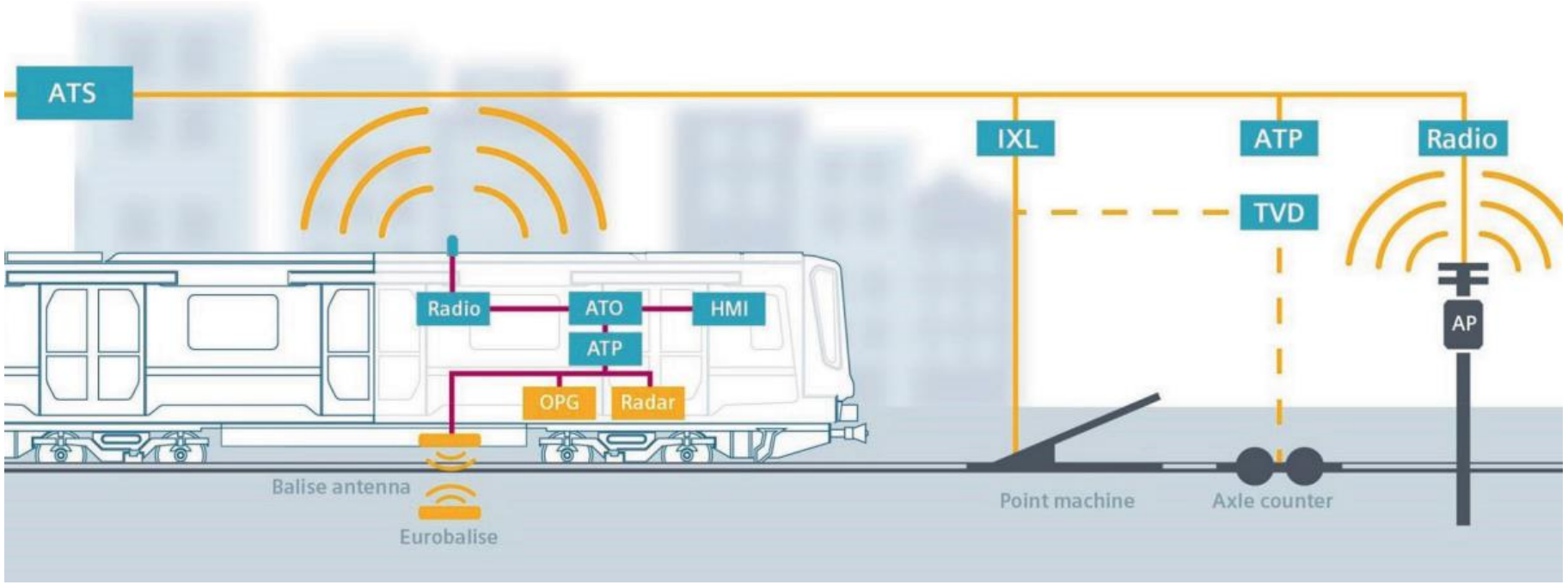
Intermittent Train Control



SIEMENS

CBTC (Communication Based Train Control)

Continuous Train Control



SIEMENS

Siemens TrainGuard MT R3

generic product
product independent of applications, fulfilling predefined boundary conditions, interfaces and functionality (black box)

EXAMPLE Point machines, axle counters, real-time operating systems, fail-safe computer platforms without application software.

Automation level	Train motion initiated	Braking	Doors closing	During an interruption
GoA 1	Engineer	Engineer	Engineer	Engineer
GoA 2	Automatic	Automatic	Engineer	Engineer
GoA 3	Automatic	Automatic	Attendant	Attendant
GoA 4	Automatic	Automatic	Automatic	Automatic

Zdroj: 62267 © IEC:2009

SIEMENS

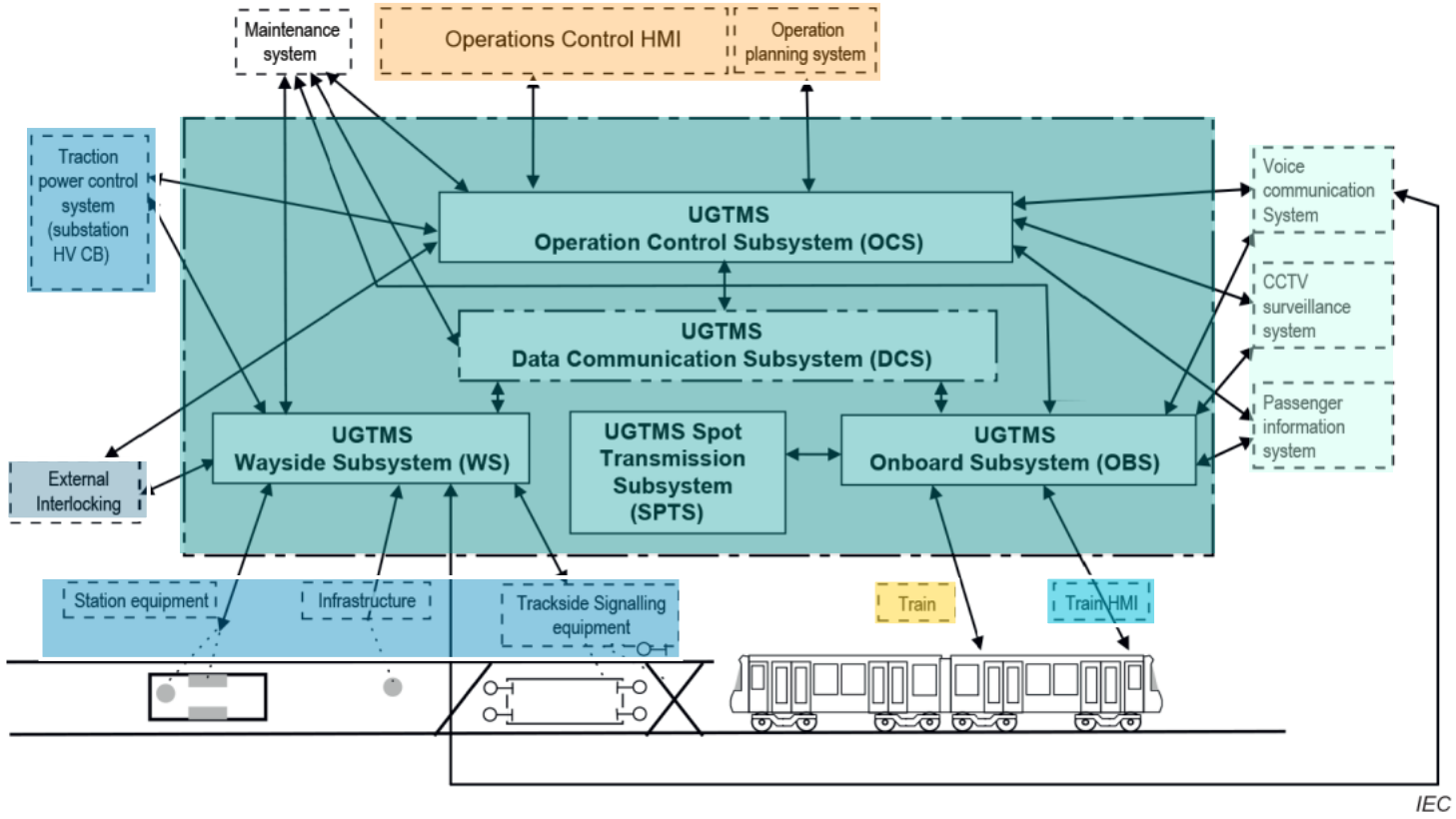
Siemens TrainGuard MT R3

Basic functions of train operation		On-sight train operation TOS GOA0	Non-automated train operation NTO GOA1	Semi-automated train operation STO GOA2	Driverless train operation DTO GOA3	Unattended train operation UTO GOA4
Ensuring safe movement of trains	Ensure safe route	X (points command/ control in system)	S	S	S	S
	Ensure safe separation of trains	X	S	S	S	S
	Ensure safe speed	X	X (partly supervised by system)	S	S	S
Driving	Control acceleration and braking	X	X	S	S	S
Supervising guideway	Prevent collision with obstacles	X	X	X	S	S
	Prevent collision with persons	X	X	X	S	S
Supervising passenger transfer	Control passengers doors	X	X	X	X or S	S
	Prevent injuries to persons between cars or between platform and train	X	X	X	X or S	S
	Ensure safe starting conditions	X	X	X	X or S	S
Operating a train	Put in or take out of operation	X	X	X	X	S
	Supervise the status of the train	X	X	X	X	S
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	S and/or staff in OCC
NOTE X = responsibility of operations staff (may be realised by technical system). S = realised by technical system.						

Zdroj: 62267 © IEC:2009

SIEMENS

Siemens TrainGuard MT R3



TGMT R3
Onboard interface
Driver interface
Rolling stock interface
Static infrastructre int.
Interlocking interface
ATS interface

Zdroj: IEC 62290-1

UGTMS- Urban Guided Transport Management and Command/control Systems

SIEMENS

Demonstrace bezpečnosti a spolehlivosti

SIEMENS

Safety targets

Reference of the function or subfunction from IEC 62290-2	Headline of the function or subfunction from IEC 62290-2:	GOA1	GOA2	GOA3	GOA4
5	Functions for train operation				
5.1	Ensure safe movement of trains				
5.1.1	Ensure safe route	M_IF	M_IF	M_IF	M_IF
5.1.1.1	Set and protect route				
5.1.1.1.1	Set route	M	M	M	M
5.1.1.1.2	Supervise route	M	M	M	M
5.1.1.1.3	Lock route by train	M	M	M	M
5.1.1.2	Release route	M	M	M	M
5.1.2	Ensure safe separation of trains				
5.1.2.1	Locate UGTMS reporting trains				
5.1.2.1.1	Initialise UGTMS reporting trains location	M	M	M	M
5.1.2.1.2	Determine train orientation	M	M	M	M
5.1.2.1.3	Determine actual train travel direction	M	M	M	M
5.1.2.1.4	Determine train location	M	M	M	M

Zdroj: IEC 62290-1:2025

generic product
product independent of applications, fulfilling predefined boundary conditions, interfaces and functionality (black box)

A generic product can be designed for use in different applications. A generic product is independent from generic or specific applications.

generic application
application which contains all mandatory and all or a subset of optional functions, with predefined configurability and customisable for different specific applications

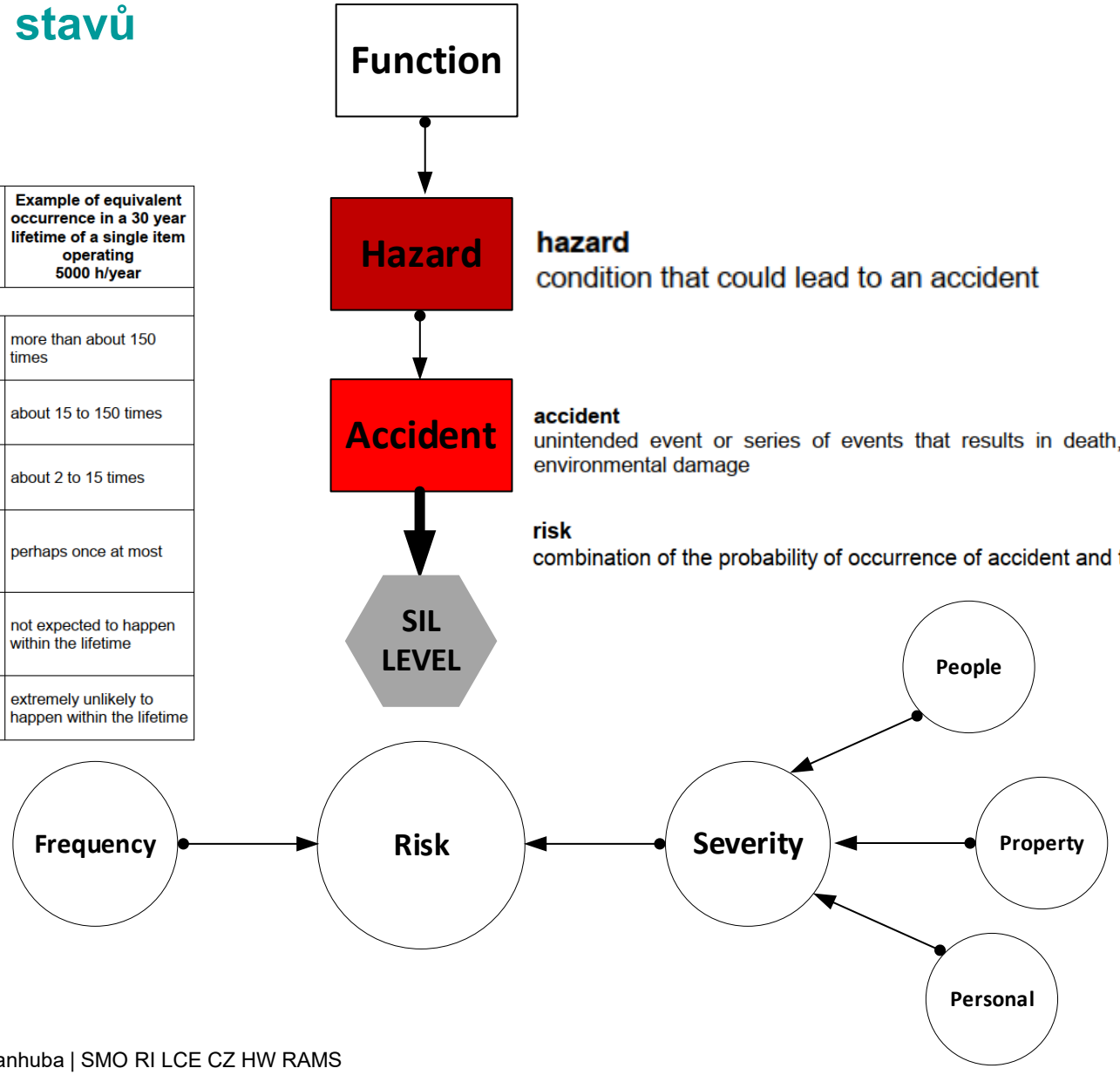
A specific application of UGTMS is designed for only one particular installation and can be based on a customised generic application. A specific application may contain additional specific functions, which are not defined in this document. The specific application takes into account the local conditions like track layout, headway requirements as well as climate and environmental conditions.

SIEMENS

Analýza rizik a hazardních stavů

Frequency level	Description
Frequent	Likely to occur frequently. The event will be frequently experienced.
Probable	Will occur several times. The event can be expected to occur often.
Occasional	Likely to occur several times. The event can be expected to occur several times.
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.

Example of a frequency range based on a single item operating 24 h/day	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000 h/year
Expected to happen	
more than once within a period of approximately 6 weeks	more than about 150 times
approximately once per 6 weeks to once per year	about 15 to 150 times
approximately once per 1 year to once per 10 years	about 2 to 15 times
approximately once per 10 years to once per 1 000 years	perhaps once at most
approximately once per 1 000 years to once per 100 000 years	not expected to happen within the lifetime
once in a period of approximately 100 000 years or more	extremely unlikely to happen within the lifetime



hazard
condition that could lead to an accident

accident
unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

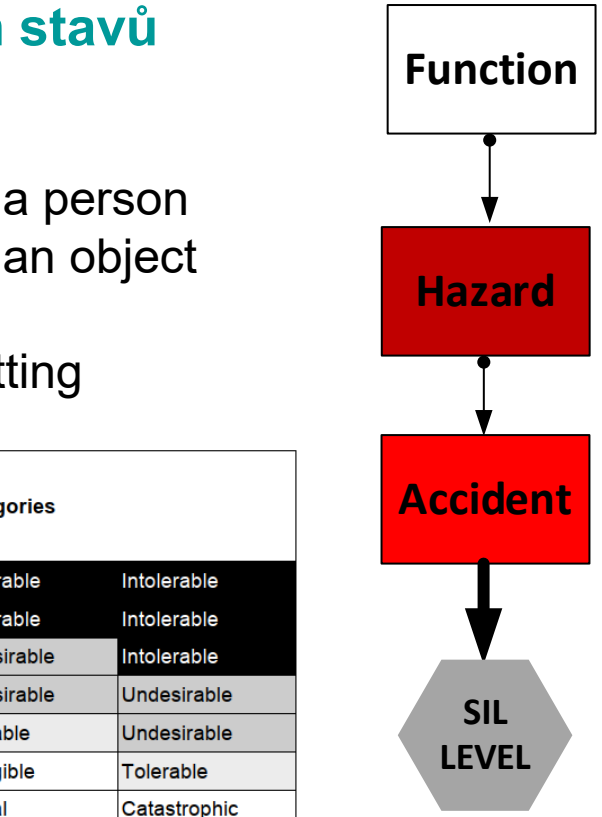
risk
combination of the probability of occurrence of accident and the severity of that accident

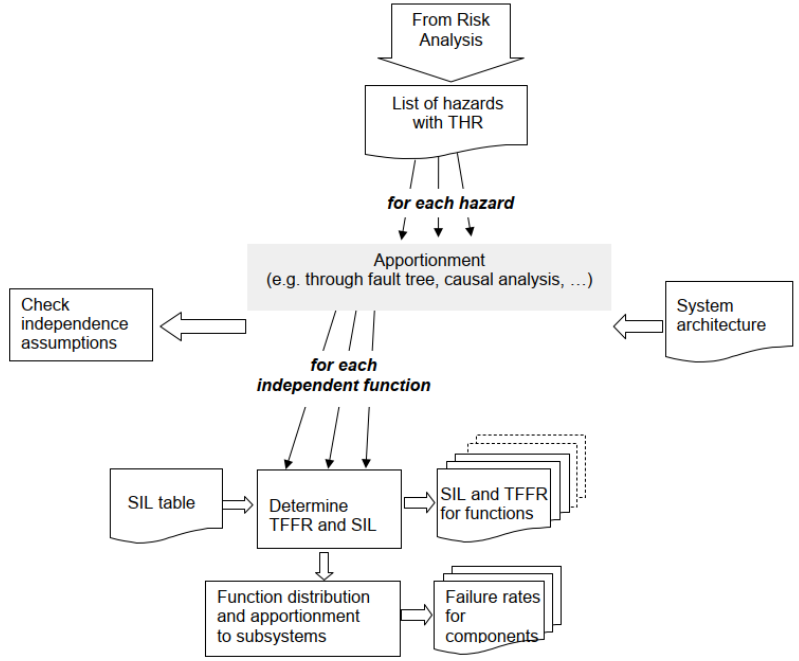
SIEMENS

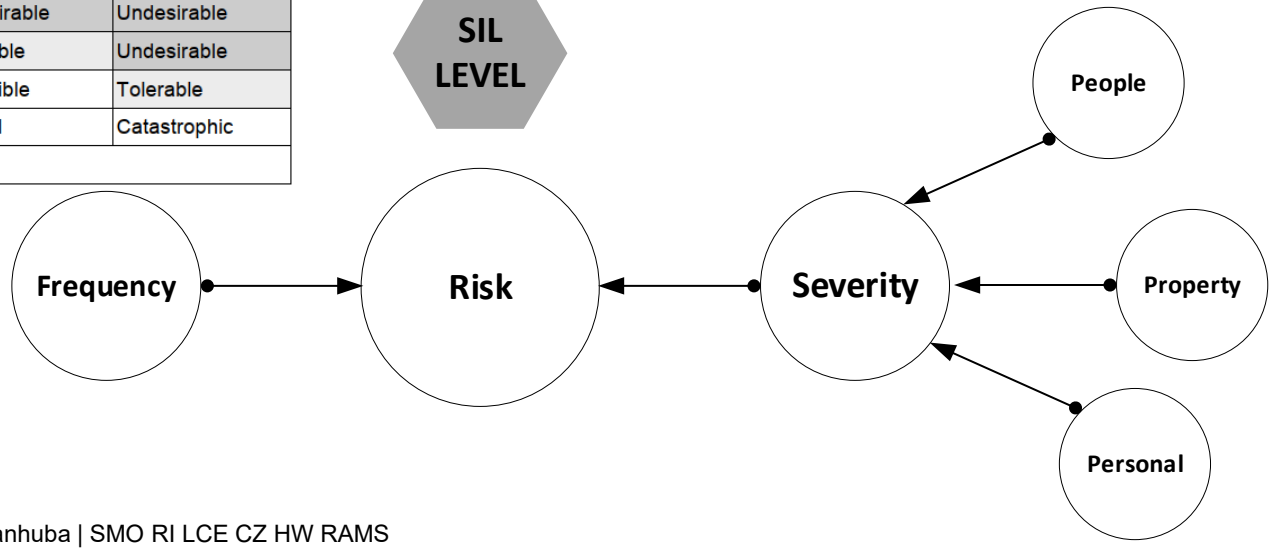
Analýza rizik a hazardních stavů

- Collision between trains
- Collision between a train and a person
- Collision between a train and an object
- Derailment
- Passengers falls, drags or cutting

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			







SIEMENS

Stručné srovnání s procesem v leteckém průmyslu (do roku 2020)

INDICATIOM SYSTEM EXAMPLE						
Function	*Failure Mode Description*	*Flight Phase*	*Preliminary Failure Condition Classification*			*Note*
			Complete loss of function	*Loss of Primary Means of providing function*	*Misleading and/ or malfunctio n without indication*	
Display of Engine tachometer (RPM)[1]	-	***ALL***	**MINOR**	**MINOR**	**MINOR**	Assumes fixed pitch propeller and reciprocating engine; otherwise, a propeller governor will maintain the engine r.p.m. Refer to 14 CFR part 23, § 23.1311.
Display of Manifold pressure[1]	-	***ALL***	**MINOR**	**MINOR**	**MINOR**	Assumes backup use of CHT, Engine Gas Temperature (EGT), and possible fuel flow readings if installed. Based on FAA AC23.1309-1E
Display of Oil temperature[1]	-	***ALL***	**MINOR**	**MINOR**	**MINOR**	Assumes as oil pressure as back up. Based on FAA AC23.1309-1E
Display of Oil pressure[1]	-	***ALL***	**MINOR**	**MINOR**	**MINOR**	Assumes as oil temperature as back up. Based on FAA AC23.1309-1E
Display of Cylinder head temperature[1]	-	***ALL***	**MINOR**	**MINOR**	**MINOR**	Assumes a CHT indicator is required. Refer to 14 CFR part 23, § 23.1305. Based on FAA AC23.1309-1E

Classification of Failure Conditions	**No Safety Effect**	**<----Minor------>**	**<-----Major----->**	**<--Hazardous--->**	**< Catastrophic>**
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation

Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.
Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for Primary System (P) and Secondary System (S). For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.
Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.
Note 4. Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria.

FAA AC 23.1309-1E

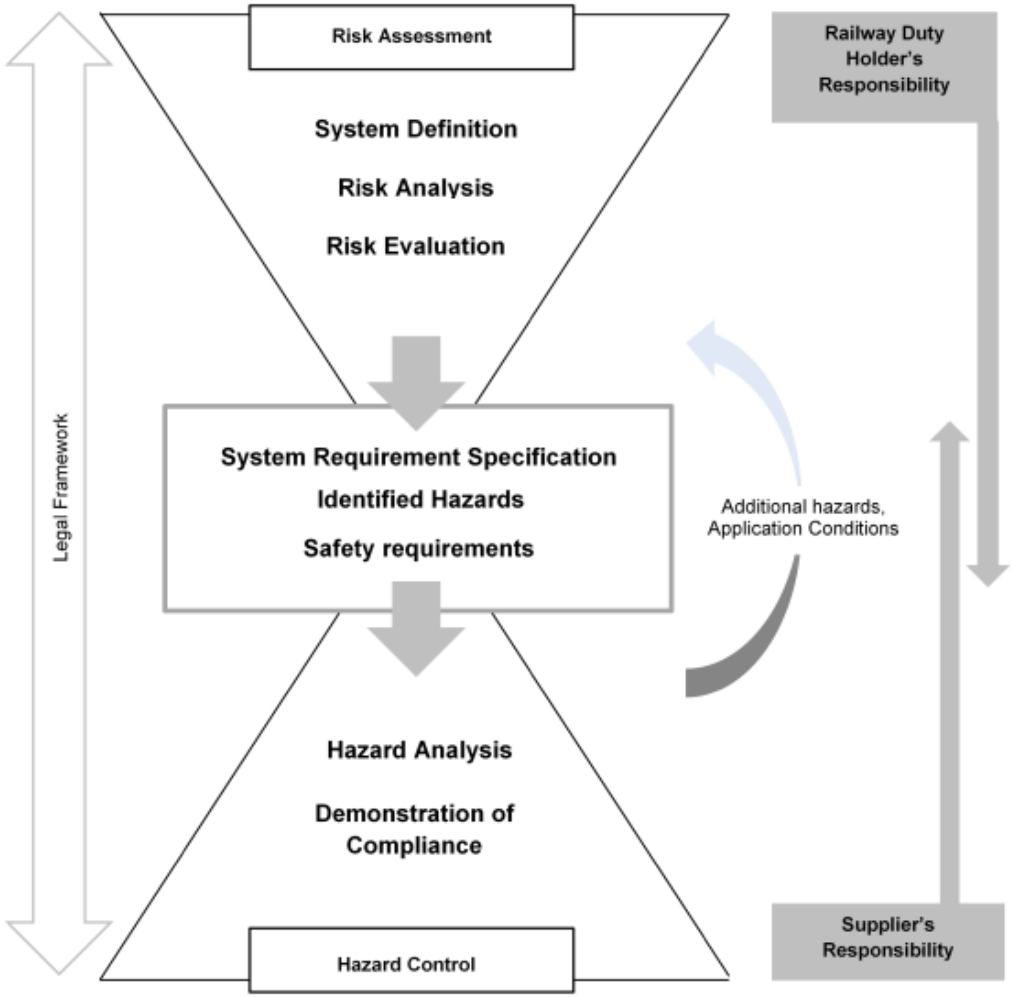
SIEMENS

Definice hazardních stavů

Function	Hazardous Source	Hazardous Events	Hazard
Control doors and MGF	Train outside station and door untimely open	Passengers beside doors and doors are opened or released during train movement	Inadequate intervention to keep doors from opening while train is not at standstill
		Train operated with failure	Inadequate protection of the potential presence of passengers on the track
		Incorrect reaction to failure	Inadequate intervention to keep the train from passing a point

SIEMENS

Definice hazardních stavů



Hazard

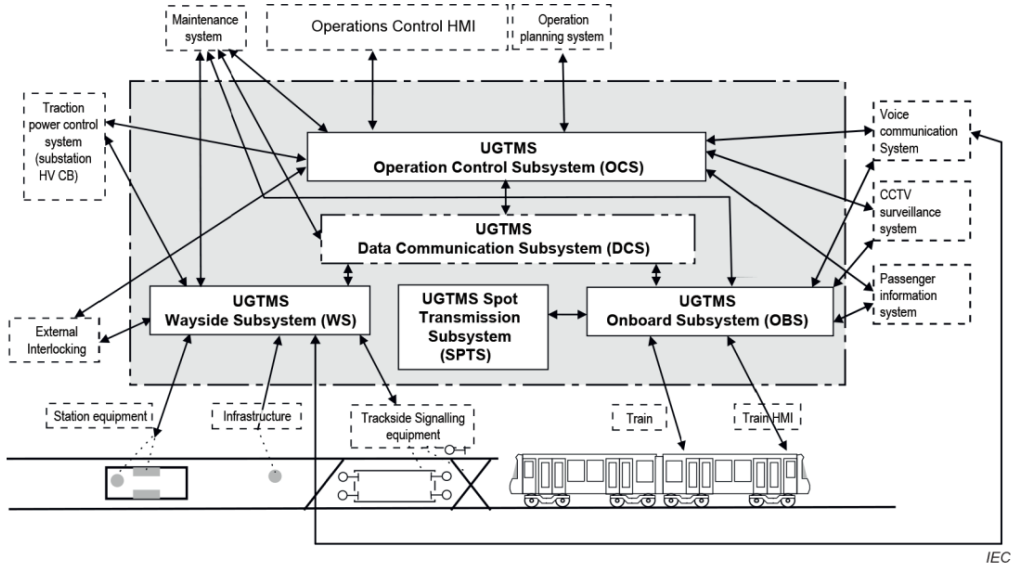
Inadequate intervention to keep doors from opening while train is not at standstill

Inadequate protection of the potential presence of passengers on the track

Inadequate intervention to keep the train from passing a point

SIEMENS

Výhody řešení



Function

Control doors and MGF

New

Hazardous Events

Passengers beside doors and doors are opened or released during train movement

Train operated with failure

Incorrect reaction to failure

New event

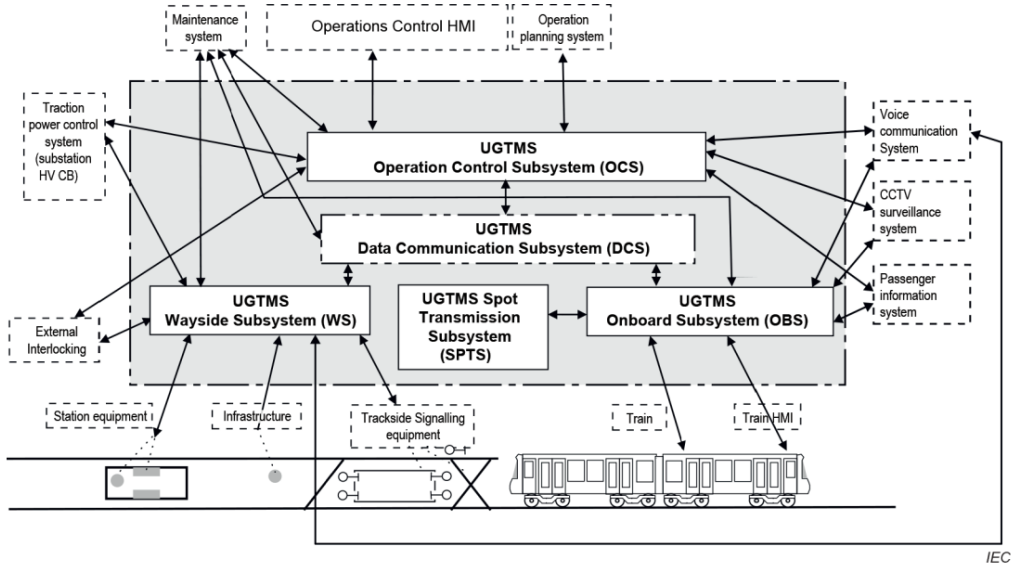
...

Hazard

Inadequate intervention to keep doors from opening while train is not at standstill

SIEMENS

Nevýhody řešení



?

Inadequate intervention to keep the train from passing a point

Specific application Function:

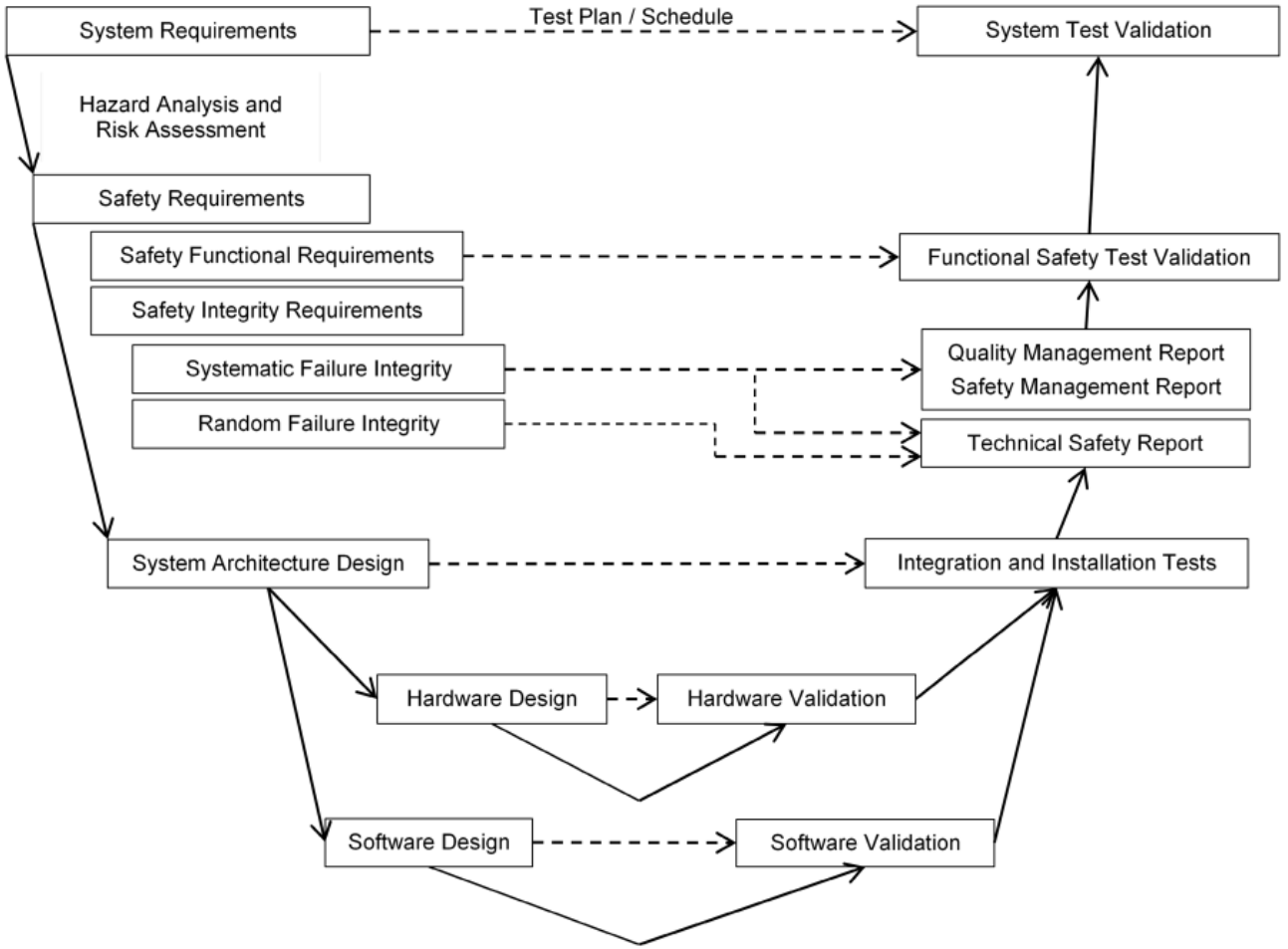
Train Location Supervision
Train Speed Supervision
Train Movement Protection
…

Specific application Hazards:

Incorrect train location of trains
Incorrect determination of train location
Signaling system does not consider occupation
…

SIEMENS

Demonstrace bezpečnosti podle EN 50129:2018



SIEMENS

Kontakt

Luboš Janhuba, Ph.D.

RAMS Manager

Siemens Mobility, s.r.o.
SMO RI LCE CZ HW RAMS
Siemensova 1
155 00 Prague 13
Czech Republic

E-mail lubos.janhuba@siemens.cz

SIEMENS