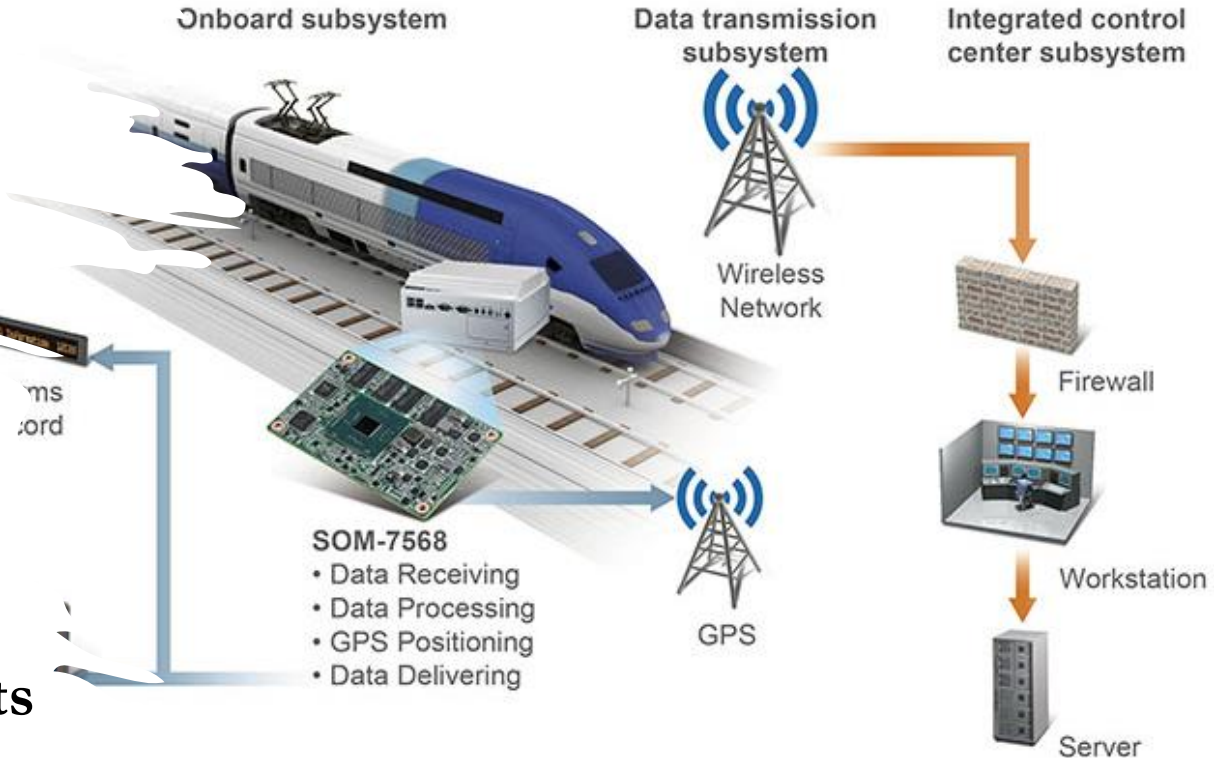
Railway Safety in Design Phase

NAPHAT KETPHAT (PH.D.)

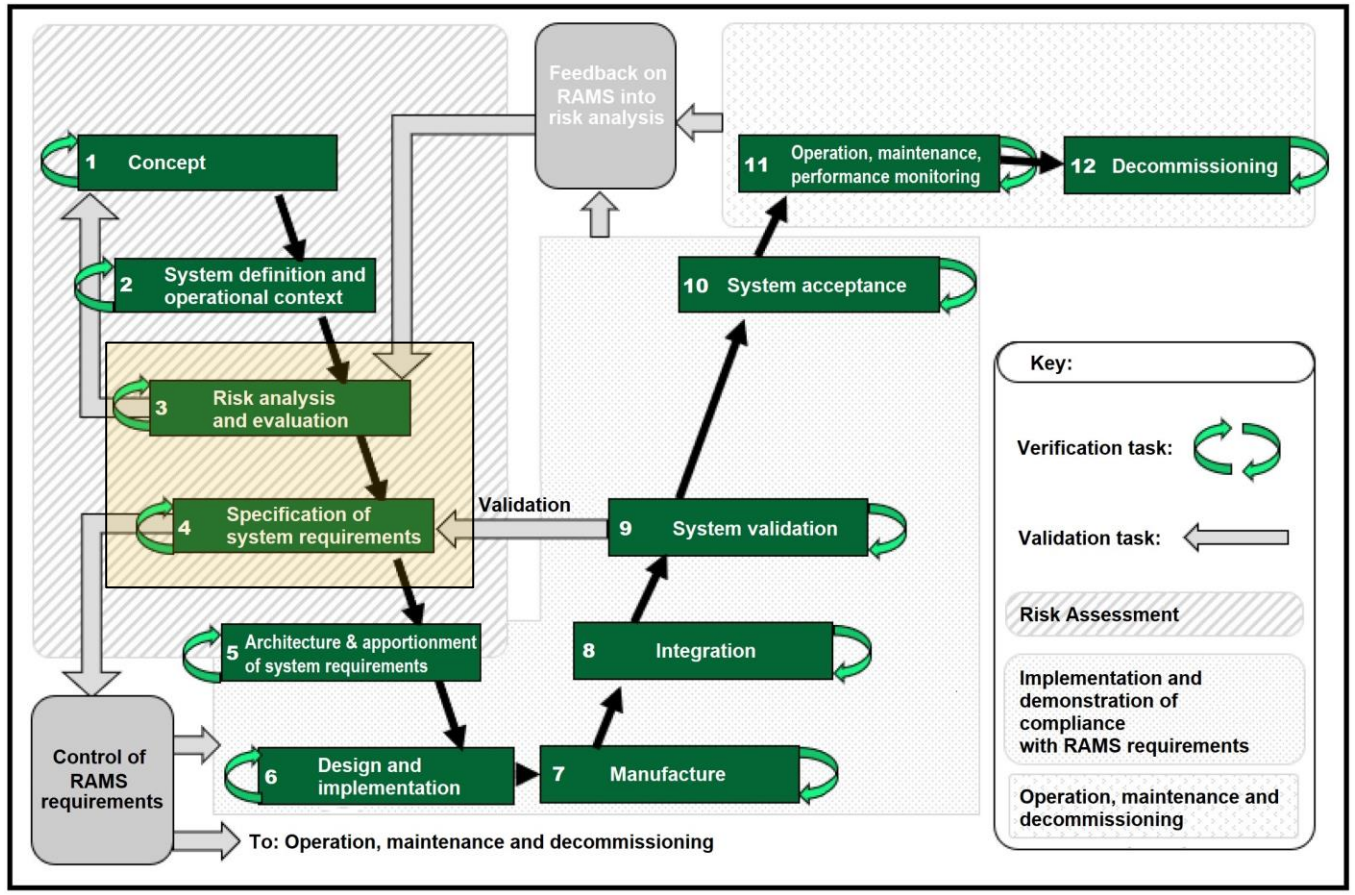
CLUSTER OF LOGISTIC AND RAILWAY ENGINEERING (CLARE)

Content

- **Railway Safety Standard**
- **Phase 3: Risk Analysis and Evaluation**
  - System Hazard Analysis (SHA)
  - Interface Hazard Analysis (IHA)
  - Operating and Support Hazard Analysis (OSHA)
  - Hazard Log
  - SIL Allocation
  - Fault Tree Analysis
- **Phase 4: Specific of System Requirements**



Railway Safety Standard



- **EN 50126 (IEC 62278): Reliability, Availability, Maintainability, and Safety (RAMS)**

To provide a general overview and outline the main **planning activities in safety**-related rail development.

- Overview of European directives and standards in the railway signalling technology and their definitions.
- Elements of **RAMS** and affecting factors
- **Risk / Risk Analysis**
- **Safety Integrity**
- **Life Cycle Model**

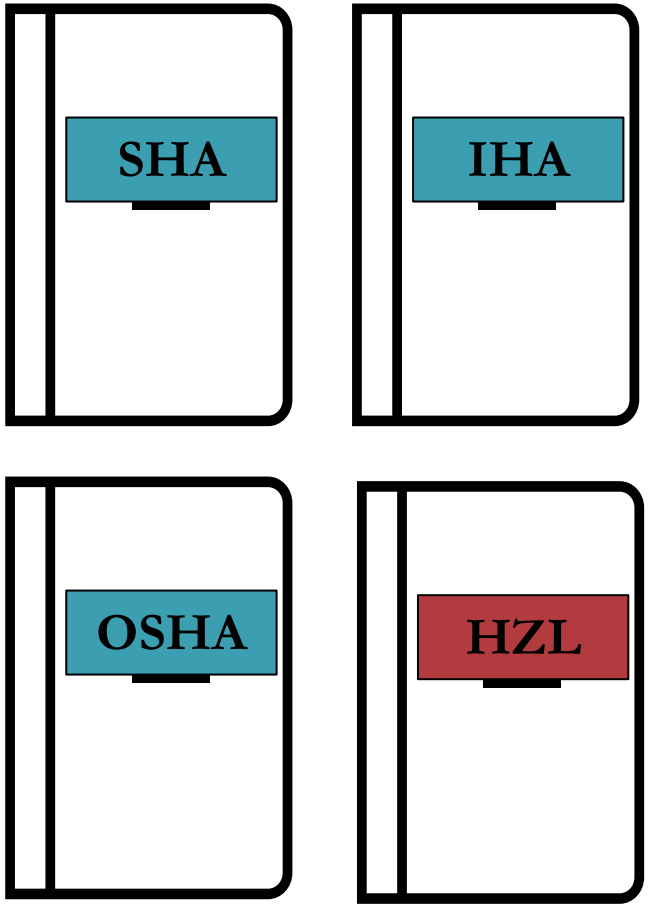
Phase 3: Risk Analysis and Evaluation

Objective:

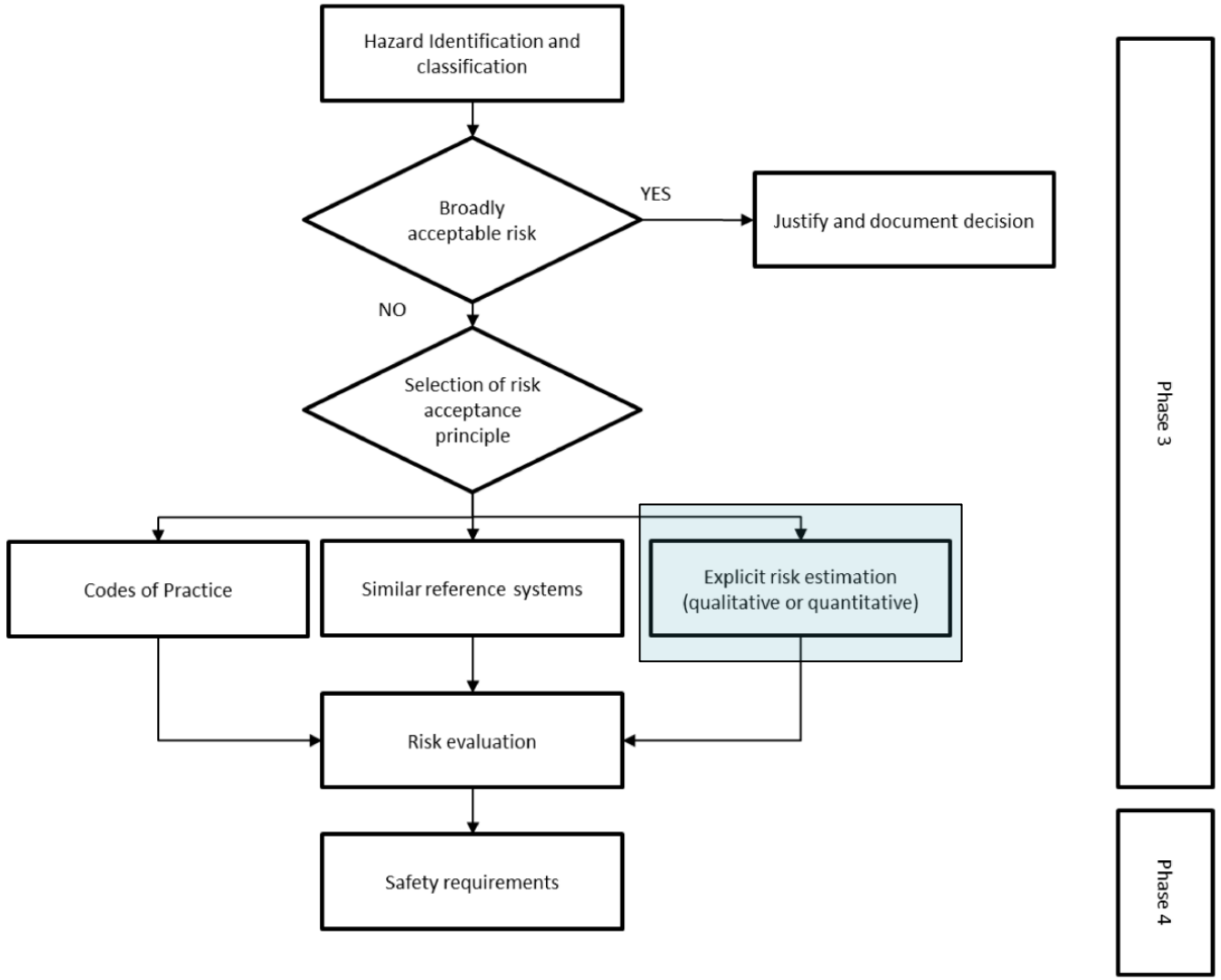
- **Identify and classify hazards** associated with the system
- Select **Risk Acceptance** principle
- Define and apply risk acceptance criteria
- Assess risk
- Establish a process for on-going risk assessment

Safety Activities:

- Perform **Risk analysis**
- Establish **Hazard Log**
- Update safety plan
- Establish **Independent Safety Assessment (ISA) Plan**



Phase 3: Risk Analysis and Evaluation

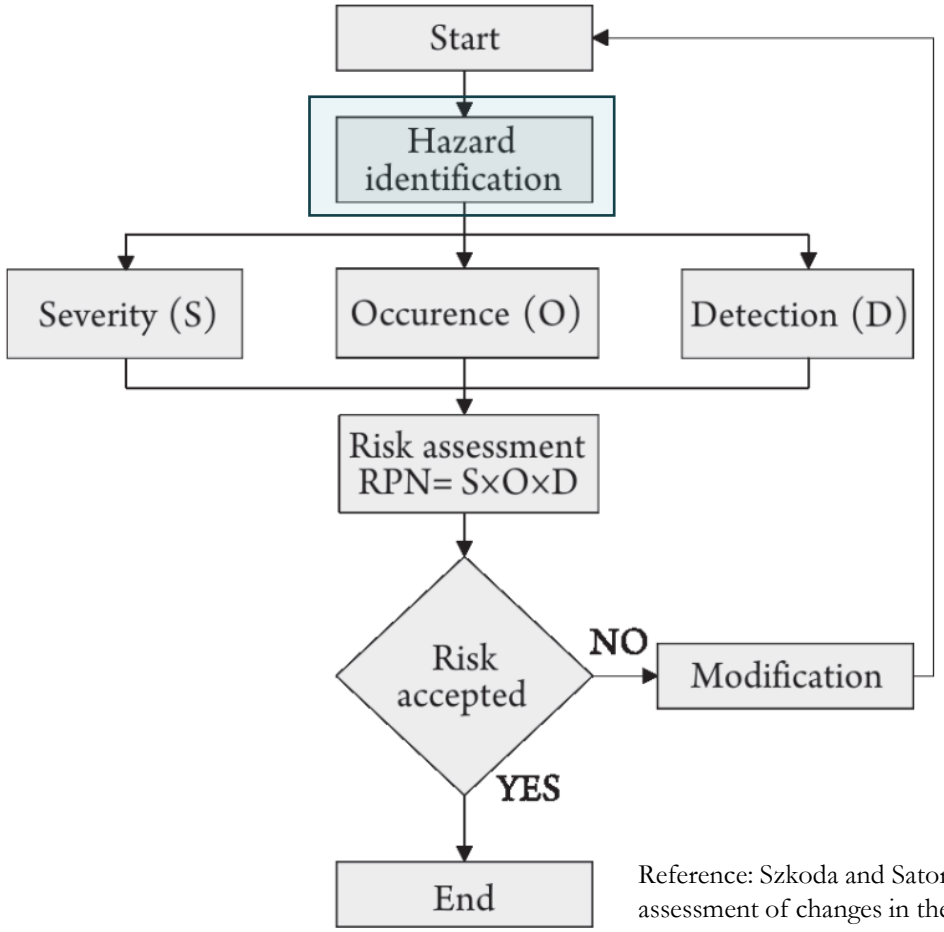


- If the risk analysis identified cases with risk "broadly acceptable", there is no need to specify further requirements for those cases.
- If the risk analysis concluded that a risk is not "broadly acceptable", the risk analysis activity shall be continued by choosing and applying a '**Risk Acceptance Principle**' (RAP), before applying risk evaluation.

The three risk acceptance principles are:

- use of Code of Practice (CoP);
- comparison with a similar system as a reference;
- Explicit risk estimation (ERE) (qualitative or quantitative).

Risk Analysis: Hazard Identification



- Hazard and Operability Study (HAZOP) is often used as a technique for **identifying potential hazards** in a system and identifying operability problems likely to lead to nonconforming products.

HAZOP is based on a theory assuming risk events are caused by deviations from design or operating intentions.

Reference: Szkoda and Satora (2019), The application of failure mode and effect analysis (FMEA) doe the risk assessment of changes in the maintenance system of railway vehicles

Risk Analysis: Hazard Identification

No.	Parameter	Description
1	Interface	. Data interface between wayside equipment and on-board equipment . Communication interface between the wayside operator and vehicle driver . Data interface between sub-systems . Data interface between related systems . Communication interface between the wayside operator(system) and maintainer
2	Time	. Train operation time based on the train schedule . Operation time of the on-site facilities . Software data processing time . Generally defined time
3	Action	. Operation of operator, driver, maintainer . Action of on-site facilities . Action of on-board equipment
4	Limit	. Limit to the train speed . Limit to the line capacity . Limit to the software data processing . Limit to the human labor . Limit to the availability and reliability of facility
5	Procedure	. Operation, driving, maintenance procedure . Countermeasure procedure at emergency
6	Outside	. Natural phenomena (earthquake, storm, snow, rain, wind, etc.) . passenger behavior . Prerequisite to the intentional external obstacle
7	Data	. Control command (train control, on-site facility control, etc.) . On-site information . Database information

Guidewords

- No, Late, Incorrect
- Longer, Shorter
- Higher, Lower
- Etc.

Factor	Guideword	Possible Hazard	Hazard Description
Leading train Position	No	Collision between trains	The minimum safe distance and the actual distance between trains cannot be calculated (No MA).

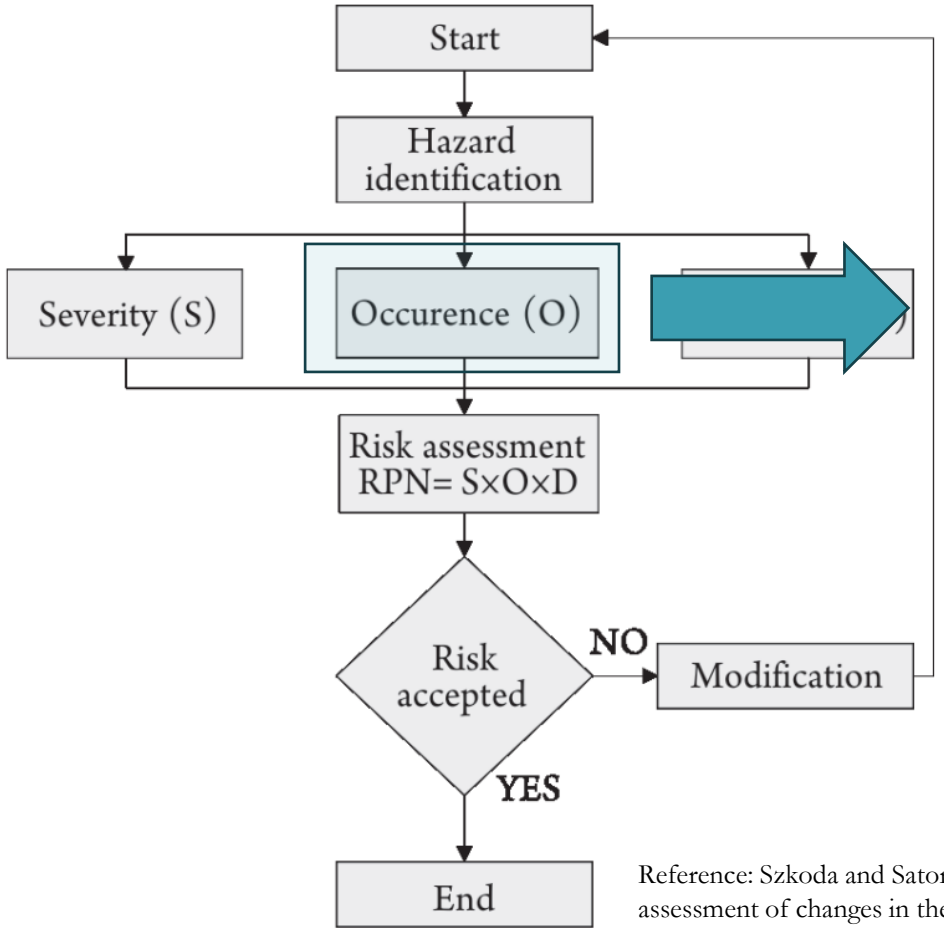
Risk Analysis: Hazard Identification

Interface Label	Detailed Interface	Failure Mode	Failure Cause	Local effect	Operations effect	IS	IF	IHR	Mitigation Measure	FS	FF	FHR
RATO – ATS Control Centre	To receive the instructions from the ATS and then send the status and alarms. To send/receive information to/from ATS including command, supervision, alarms, hold station status, driving profiles to the trains.	**No** transmitted data	DTS failure	1) Loss of status information on the ATS display. 2) Unable to send commands to the onboard and wayside subsystems.	Trains will continue to operate upto there limit of movement authoity then stop. Operational Impact. No Safety Impact	IV	C	IVC	The DTS is configured in a redundant (fault tolerant) configuration.	IV	E	IVE
		Late transmitted data	Latency in the DTS network	1) Delay in the update of status information on the ATS display. 2) Delay in the reciept of commands to the onboard and wayside subsystems.	System will continue to operate normally. No Safety Impact.	IV	C	IVC	Compliance with EN50159:2010, Category 2 – Open transmission systems Message time out is used to mitigate the threat of delay.	IV	E	IVE
		Wrong data	HW/SW faults (Transmittion system)	Incorrect status information causing lossing of alarm data	Collision as a train may operate unsafely due to incorrect information received. Operational Impact. Safety Impact	I	D	ID	Compliance with EN50159:2010, Category 2 – Open transmission systems Corruption threats are addressed by safety codes (CRCs). These CRCs include all data bytes in the messages, including header, serial number and data. The CRC protects against random and systematic bit errors. A message with bad CRC will be rejected by the subsystem CPU.	I	E	IE

Risk Analysis: Hazard Identification

Interface Label	Detailed Interface	Failure Mode	Failure Cause	Local effect	Operations effect	IS	IF	IHR	Mitigation Measure	FS	FF	FHR
VATP – Tachometers	This interface allows detection of wheel rotation by onboard CBTC system (VATP). This information is used to calculate train speed, acceleration, travelling direction as well as travelled distance. In addition, it will provide information of potential slip/slide events in case of axle blocking, braking capabilities and vital zero speed detection.	**No** transmitted data	Tachometer failure VATP failure	Collision. There is no train's position data	Train position error/ fail to determine exact location of a train possibly cuasing collision with consecutive trains on the sane line	I	D	ID	When the VATP cannot determine the train speed, then the VATP shall shut itself down.	I	E	IE
		Late transmitted data	HW/SW faults	Delayed trains' speed/trevelling direction sent from tachometers	Train may be forced to stop. Operational Impact No Safety Impact	IV	D	IVD	1) Redundant tachometers are required. 2) Each tachometer input is read by a different Vital IO channel. The vital input signal is active only when both channels report activity within a bounded tolerance.	IV	E	IVE
		Wrong data	HW/SW faults	Incorrect train speed (speed might be lower than actual) Incorrect trevelling direction.	Collision or derailment due to exceeding speed (driving speed is higher than speed limit)	I	D	ID	1) Redundant tachometers are required. 2) Each tachometer input is read by a different Vital IO channel. The vital input signal is active only when both channels report activity within a bounded tolerance.	I	E	IE

Risk Evaluation

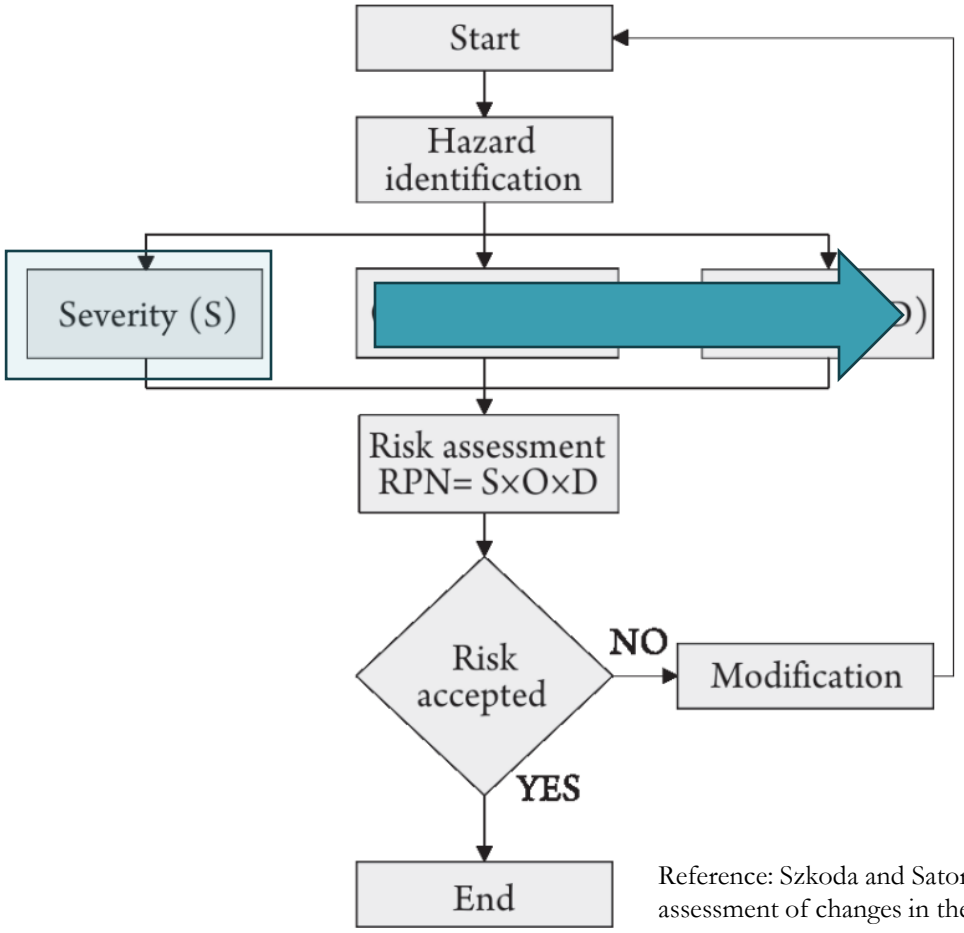


Categories of the probability Hazard Frequency (O)

Frequency of Occurrence		Description	Mean Time Between Hazard Events (MTBHE)	Failure Rate
5	Frequent	Likely to occur frequently. The hazard will be continually experienced.	MTBHE $< 1 \times 10^{3}$	$\lambda > 1 \times 10^{-3}$
4	Probable	Will occur several times. The hazard can be expected to occur often	$1 \times 10^{3} \leq$ MTBHE $< 1 \times 10^{5}$	$1 \times 10^{-3} \geq \lambda > 1 \times 10^{-5}$
3	Occasional	Likely to occur several times. The hazard may be expected to occur several times	$1 \times 10^{5} \leq$ MTBHE $< 1 \times 10^{6}$	$1 \times 10^{-5} \geq \lambda > 1 \times 10^{-6}$
2	Remote	Likely to occur sometime in the system life cycle. The hazard may reasonably be expected to occur	$1 \times 10^{6} \leq$ MTBHE $< 1 \times 10^{8}$	$1 \times 10^{-6} \geq \lambda > 1 \times 10^{-8}$
1	Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur	MTBHE $\geq 1 \times 10^{8}$	$\lambda \leq 1 \times 10^{-8}$

Reference: Szkoda and Satora (2019), The application of failure mode and effect analysis (FMEA) doe the risk assessment of changes in the maintenance system of railway vehicles

Risk Evaluation

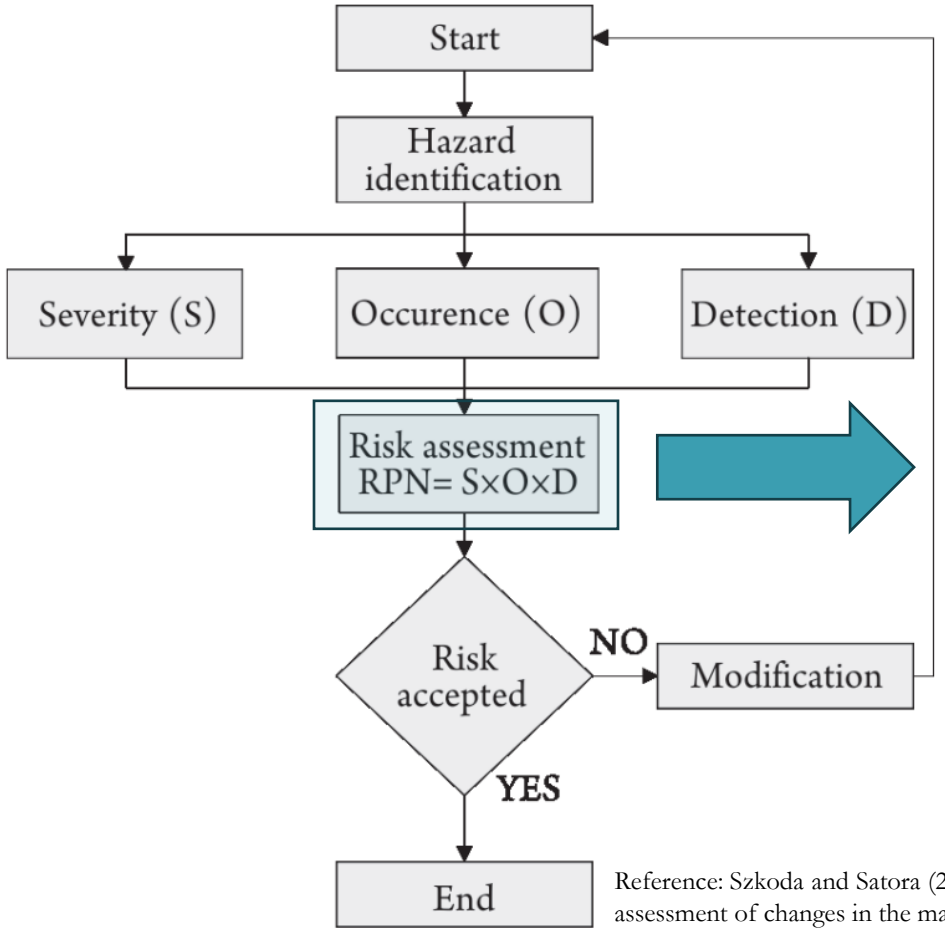


Categories of Hazard Severity (S)

Category	Severity Level	Consequence to person or environment	Consequence to service
4	Catastrophic	Death, system loss, or severe environmental damage	Loss of train service
3	Critical	Severe injury, severe occupational illness, or major system or environmental damage	Loss of major system
2	Marginal	Minor injury, minor occupational illness, or minor system or environmental damage	Severe system(s) damage
1	Negligible	Less than minor injury, occupational illness, or less than minor system or environmental damage	Minor system(s) damage

Reference: Szkoda and Satora (2019), The application of failure mode and effect analysis (FMEA) doe the risk assessment of changes in the maintenance system of railway vehicles

Risk Evaluation

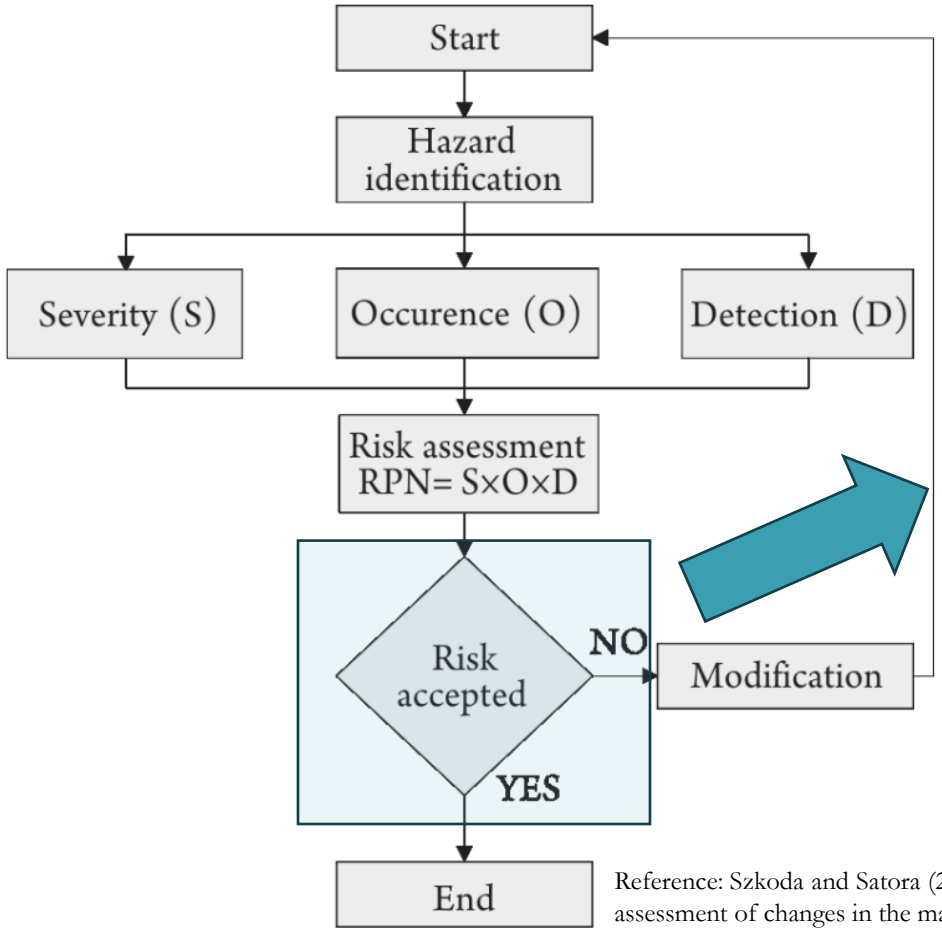


Risk Assessment

		Hazard Severity			
		Catastrophic 4	Critical 3	Marginal 2	Negligible 1
Frequency of Occurrence	Frequent 5	Intolerable (20)	Intolerable (15)	Intolerable (10)	Tolerable (5)
	Probable 4	Intolerable (16)	Intolerable (12)	Undesirable (8)	Tolerable (4)
	Occasional 3	Intolerable (12)	Undesirable (9)	Tolerable (6)	Negligible (3)
	Remote 2	Undesirable (8)	Tolerable (6)	Tolerable (4)	Negligible (2)
	Improbable 1	Tolerable (4)	Tolerable (3)	Negligible (2)	Negligible (1)

Reference: Szkoda and Satora (2019), The application of failure mode and effect analysis (FMEA) doe the risk assessment of changes in the maintenance system of railway vehicles

Risk Evaluation



Risk Acceptance Matrix

Risk Category	Risk Level	Action to be applied against each category
Intolerable	10 – 20 (10, 12, 15, 16 and 20)	Unacceptable (Hazard must be eliminated)
Undesirable	8 – 9 (8 and 9)	Undesirable (Shall only be accepted when risk reduction is impracticable and with the agreement of the Operator.).
Tolerable	3 – 7 (3, 4, 5, and 6)	Acceptable with adequate control measures
Negligible	1 – 2 (1 and 2)	Acceptable (No action required)

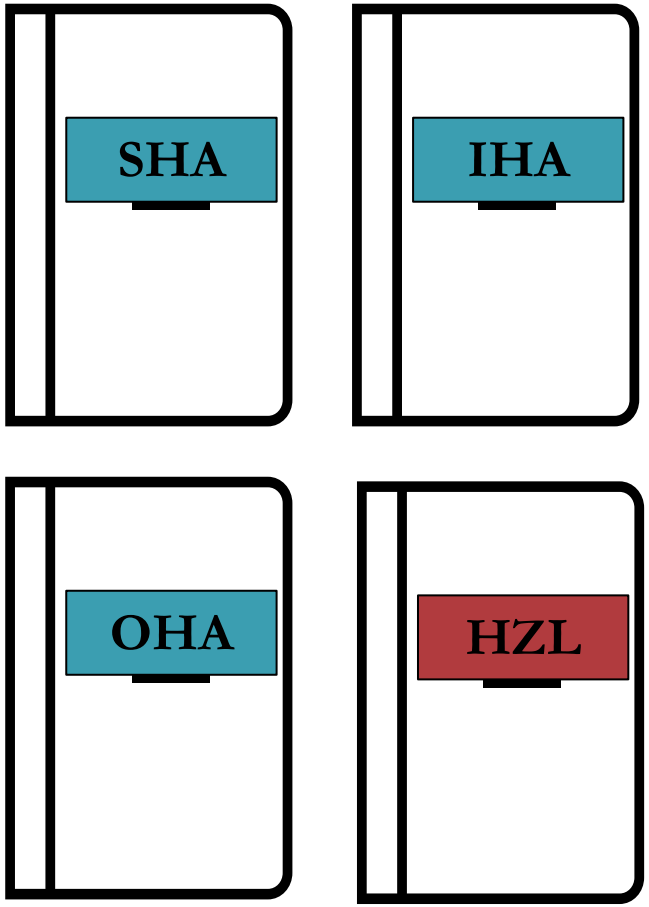
Reference: Szkoda and Satora (2019), The application of failure mode and effect analysis (FMEA) doe the risk assessment of changes in the maintenance system of railway vehicles

Phase 3: Risk Analysis and Evaluation

To identify hazards:

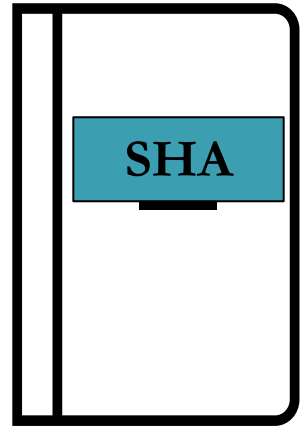
- System Hazard Analysis (SHA)
- Interface Hazard Analysis (IHA)
- Operational Hazard Analysis (OHA)

These hazard analysis including PHA will be included in **Hazard Log** for managing risks of the project



Phase 3: Risk Analysis and Evaluation

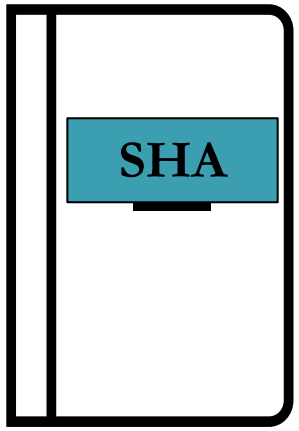
System Hazard Analysis (SHA)



- The System Hazard Analysis (SHA) report is required for the design phase of V life cycle of the project.
- The purpose of the SHA is to record hazards identified during the design phase that are relevant to the full system.
- Identify the hazards associated with the correct and incorrect operation and non-operation of the system.
- Considering the individual subsystems.
- The SHA scope will cover **all the functions of the signalling system**. The results of the assessment will be used for the identification and allocation of SILs to the function of the subsystems.
- The SHA covers Normal mode, Manual mode with ATP, Manual mode.
- **HAZOP** is used to identify hazards

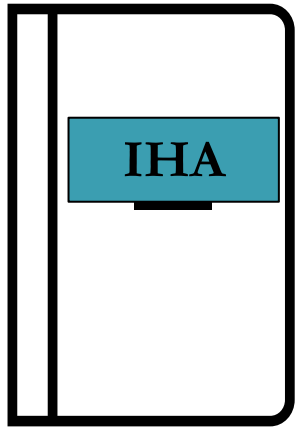
Phase 3: Risk Analysis and Evaluation

Top Level Hazard	Hazard Description	Potential Cause	Hazard Consequences	Initial Risk			Mitigating Actions	Final Risk		
				Frequency	Severity	Initial Hazard Risk		Final Frequency	Fina severity	Final Hazard Risk
Train exceeds allowed speed.	VATC fails to determine safe speed (leading to vehicle overspeed condition).	The most restrictive active speed limit is not used by VATP.	Collision or loss of guidance.	C	I	IC	VATP shall determine the maximum authorized speed of the train based on the most restrictive active speed limiting condition. VATP shall limit train speed to the most restrictive active speed limiting condition of the approaching section of track upon the train entering that section of track.	E	I	IE
Train exceeds allowed speed.	VATC speed calculation failure leading to vehicle overspeed condition.	Tachometer failure (one or both) leading to either crosscheck failure of speed sensor input signals to VATC or loss of speed sensor input signals to VATC.	Collision or loss of guidance.	C	I	IC	VATP shall calculate speed using multiple independent speed sensor inputs and perform cross-checking to confirm speed sensor inputs and speed calculations derived from those inputs are within a required error tolerance. Speed sensor input crosscheck failures or loss of speed sensor input signals shall result in VATP commanding emergency braking and disabling of propulsion. VATP shall distinguish between odometer failure and actual zero speed. VATP shall command braking upon odometer failure.	E	I	IE



Phase 3: Risk Analysis and Evaluation

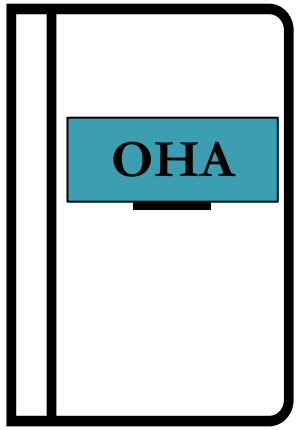
Interface Hazard Analysis (IHA)



- Identify hazards associated with **system/subsystem interfaces**.
- The IHA allows the identification of the hazards related to the interface (Internal and External Interfaces between subsystems).
- The hazards will be classified into three categories including
  - Safety Critical (SC),
  - Safety Related (SR), and
  - Non-Safety (NR).
- The analysis will identify components and equipment whose behaviour could result in an interface hazard.
- **HAZOP** is used to identify hazards.

Phase 3: Risk Analysis and Evaluation

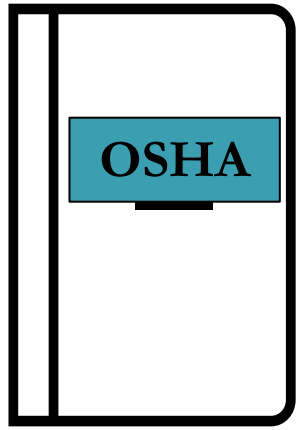
Operational Hazard Analysis (OHA)



- Identify those hazards associated with any task that may be undertaken by operation and support personnel.
- The analysis will be based on **Operational and Maintenance procedures.**
- The analysis will also identify the specific nature and duration of actions that occur under hazardous conditions during the various stages of in-service usage such as testing, installation, migration, modifications, maintenance, support, transportation, servicing, storage operation and training.
- Identify necessary actions or countermeasures to eliminate or to adequately reduce risk to an acceptable level.
- HAZOP or FMEA are used to determine risks

Phase 3: Risk Analysis and Evaluation

Hazard ID.	Operation phase	Hazard Description	Location	Hazard Cause	Potential Accident	System operation mode	S (BF)	F (BF)	Risk (BF)	Mitigation /Recommendation	S (AF)	F (AF)	Risk (AF)	Action Category
7 Normal Operation														
7.1 Train movement														
7.1.1 Operating Train in UTO mode														
HL 01	Operating train in UTO mode	Incorrect movement authority	All CBTC area	ATS failure/ Operator error	Collision/ Derailment	UTO	I	C	IC	Train operating in UTO mode ensures safe train movement by supervising safe train separation and safe speed protection based on allowed distance to go. Incorrect route request do not lead to accident as it will be protected by RATP.	I	E	IE	Signaling System
HL 02	Operating train in UTO mode	Incorrect switch position	All CBTC area	ATS failure/ Operator error	Collision/ Derailment	UTO	I	C	IC	RATP will lock the route and will provide MA to the train only when switch is set at the correct position.	I	E	IE	Signaling System
7.1.2 Accurate stopping in UTO mode														
HL 03	Operating train in UTO mode	Incorrect stopping position Train is not berth at station with pre-defined station's stop location	All CBTC area	RATP failure/ VATC failure	Delay/ Operational impact/ No safety impact	UTO	IV	C	IVC	If the train has stopped within tolerable location, the doors will be enabled and door opening will commence. If the train stopped out of the tolerable area, it may attempt to berth	IV	E	IVE	Traffic Controller



Phase 3: Risk Analysis and Evaluation

Hazard Analysis

- Preliminary Hazard Analysis (PHA)
- System Hazard Analysis (SHA)
- Interface Hazard Analysis (IHA)
- Operational Hazard Analysis (OHA)

Hazard Log

- Hazard situations
- Hazard causes
- Hazard effects
- Initial risk level (pre-mitigated)
- Mitigation measures
- Final risk level (post-mitigated)

Symbol	Interface Label	Detailed Interface	IHA ID.	Failure Mode	Failure Cause	Local effect	Operations effect	S	F	R	Mitigation Measure	S	F	R
A	RATO – ATS Control Centre	The object of this interface is to receive the instructions from the ATS and send the indications of status and alarms regarding the field objects to both. Send/reception of info to/from ATS: command, supervision and alarms, such as train alarms, or as Hold station, driving profiles to be transmitted to the trains, etc.	KLIA-APM-IHA-001	No transmitted data	DTS failure RATO failure ATS failure	Loss of status information on the ATS display. Unable to send commands to the onboard and wayside subsystems.	Trains will contiune to operate upto there limit of movement authoity then stop. Operational impact.	II	C	IIC	The DTS is configure in a redundant (fault tolerant) configuration.	II	E	IIE
			KLIA-APM-IHA-002	Late transmitted data	Latency in the DTS network	Delay in the update of status information on the ATS display. Delay in the reciept of of commends to the onboard and wayside subsystems.	System will continue to operate normally. No safety impact.	IV	C	IVC	Compliance with EN50159:2010, Category 2 – Open transmission systems Message time out is used to mitigate the threat of delay.	IV	E	IVE
			KLIA-APM-IHA-003	Untimely data	Latency in the DTS network	Untimely in the update of status information on the ATS display. Untimely in the reciept of of commends to the onboard and wayside subsystems.	System will continue to operate normally. No safety impact.	IV	C	IVC	Compliance with EN50159:2010, Category 2 – Open transmission systems Message time out is used to mitigate the threat of delay.	IV	E	IVE
			KLIA-APM-IHA-004	Corrupted data	HW/SW faults	Incorrect status information Loss of alarm data	Train may operate unsafely due to incorrect information. Operational Impact.	II	C	IIC	Compliance with EN50159:2010, Category 2 – Open transmission systems Corruption threats are addressed by safety codes (CRCs). These CRCs include all data bytes in the messages, including header, serial number and data. The CRC protects against random and systematic bit errors. A message with bad CRC will be rejected by the subsystem CPU.	II	E	IIE

Example of Hazard Log

Hazard Description						Mitigation Measure(s)
Potential Accident	Hazard Situation	Hazard Cause	Risk Assessment			
			Sev.	Freq.	Risk Level	
Rear-end collision	Stopping distance is longer than minimum safe distance	Signalling system not giving the braking order despite it is required	I	E	IE	The signalling system shall be developed ensuring that speed supervision does not allow train to exceed the maximum authorized speed and the safe stopping distance, under fail-safe principles. The signalling system shall be developed ensuring that functions related to emergency brake application are designed taking into account fail-safe principles.
Rear-end collision	Stopping distance is longer than minimum safe distance	Incorrect speed measure (Incorrect speed detemination) (odometer failure...)	I	E	IE	The signalling system shall be developed ensuring that train real speed detection and determination are designed taking into account fail-safe principles.
Rear-end collision	Stopping distance is longer than minimum safe distance	Failure of overspeed protection (ATP (Automatic Train Protection), EB (Emergency Brake) command...)	I	E	IE	1) The signalling system shall be developed ensuring that speed supervision does not allow train to exceed the maximum authorized speed and the safe stopping distance, under fail-safe principles. 2) The signalling system shall be developed ensuring that train real speed detection and determination are designed taking into account fail-safe principles.
Rear-end collision	Stopping distance is longer than minimum safe distance	Non application of a permanent / temporary speed restriction	I	E	IE	1) The signalling system shall be developed ensuring that speed supervision does not allow train to exceed the maximum authorized speed and the safe stopping distance, under fail-safe principles. 2) The signalling system shall be developed ensuring that train real speed detection and determination are designed taking into account fail-safe principles. 3) The signalling system responsible for speed control shall have a speed restriction safety function by regions which can be triggered in maintenance or degraded situations, allowing trains to only move in a given region with a speed below a design predefined value.
Rear-end collision	Stopping distance is longer than minimum safe distance	Unexpected speed restriction cancellation TSR	I	E	IE	Separated cancellation command and confirmation of cancellation are required for the TSR.
Rear-end collision	Stopping distance is longer than minimum safe distance	Train driver error (distance with downstream train, trackside signalling not respected)	I	E	IE	When the train is operating in a degraded operating mode, without control of onboard signalling system, it is responsibility of the train driver to operate the train safely, following an operational procedure established by line operator.
Rear-end collision	Stopping distance is longer than minimum safe distance	RATC calculates incorrect MA	I	E	IE	RATP shall calculate MA by including conflict point, and speed of each segment.

Phase 3: Risk Analysis and Evaluation

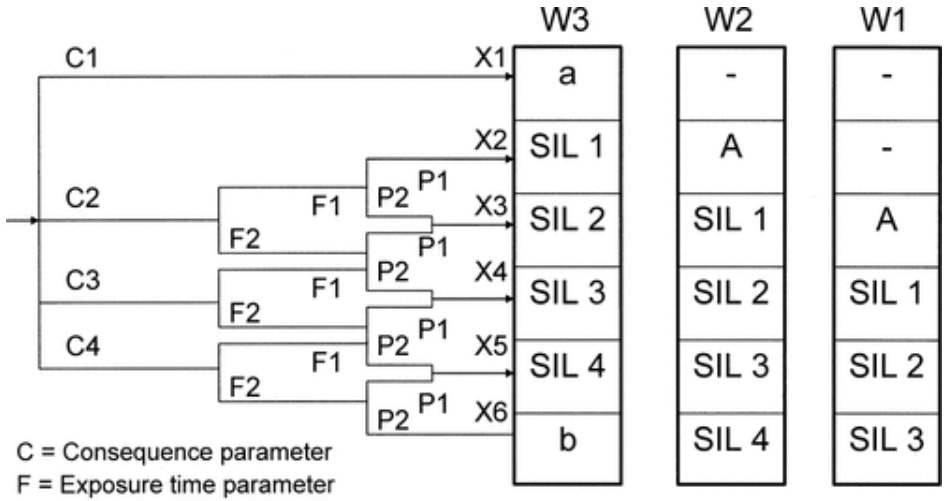
Example: Hazard Log

Stopping distance is shorter than minimum safe distance

Phase 3: Risk Analysis and Evaluation

SIL allocation report (SILA)

The Objective of this report is to demonstrate systematic approaches to confirm the SIL Allocation to the subsystems

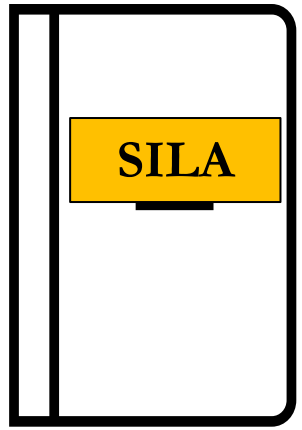


C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = Probability of the failure/occurrence (without SIS in place)
X = Frequency/probability-adjusted consequence

-	No safety requirement
a	No special safety requirements
b	A single SIF is not sufficient

Safety integrity is principally a function attribution and not physical one. A creditable system approach and process for the determination of the safety integrity requirements and associated evidence for its achievement by a product, process, sub-system or system is necessary to ensure expectations are managed and delivered by objective analysis. IEC 61508 proposed a risk-graph approach to determine SIL level for a function based on the analysis of

- Consequence (C)
- Frequency (F) exposure time risk parameter,
- Possibility (P) of failing to avoid hazard risk Parameter
- Probability of the unwanted occurrence (W).



Phase 3: Risk Analysis and Evaluation

Allocating SIL to Safety Function:

- When the failure of the function occurs (i.e., the corresponding safety requirement is not fulfilled) and it

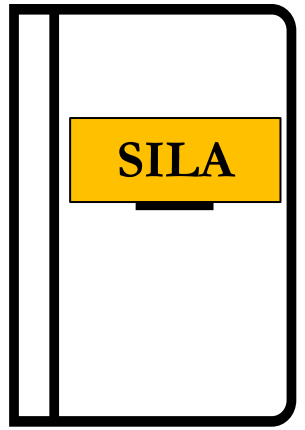
potentially leads directly to a severity "**Catastrophic**" accident, the corresponding function is **SIL4**.

- When the failure of the function occurs and it potentially leads directly to a severity "**Critical" accident**,

the corresponding function is **SIL3**.

- Can lead to **Undesirable** Risk, the function is **SIL2**.
- Can lead to **Acceptable Risk**, the function is **SIL1**.
- When the failure of the function occurs and it **does not lead to an accident**, even combined with other

independent function failure, the corresponding function is **SIL0** (no safety related function).

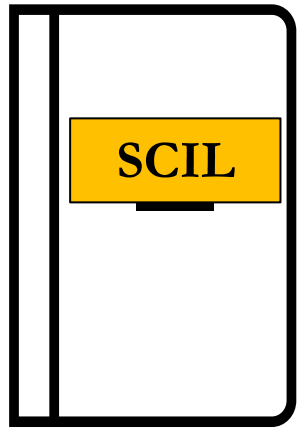


Phase 3: Risk Analysis and Evaluation

Safety Critical Item List (SCIL)

- Identifying the safety critical items in the respective subsystem design

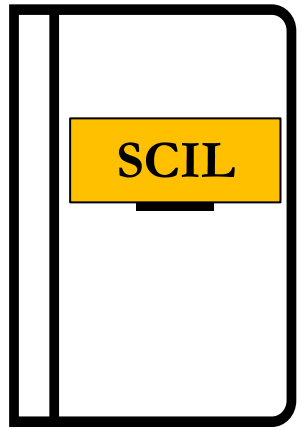
Safety Classification		Meaning	Inclusion within the SRIL
Safety	Safety Critical (SC)	Item or activity on which failure or error leads to a direct impact with potentially Catastrophic or Critical severity. Function (or part supporting function) rated as SIL4/SIL3.	Mandatory
	Safety Related (SR)	Item or activity on which failure or error can have an impact on safety that is not critical. Function (or part supporting function) rated as SIL2/SIL1.	Optional
Not safety	Insignificant/Not safety	Item or activity on which failure or error has an insignificant or no impact on safety. Function (or part supporting function) rated as Non safety/SIL0.	Not applicable



Phase 3: Risk Analysis and Evaluation

Safety Critical Item List (SCIL)

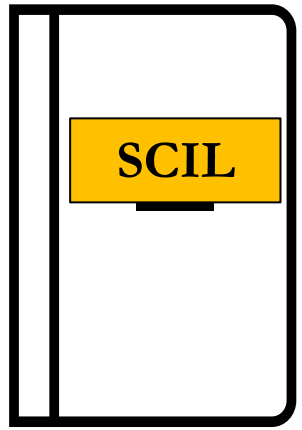
Safety Critical Item	Safety Critical Factor	Hazard Effects	Initial Risk			Mitigation Measures	Item Type
			IS	IF	Risk Level		
Central Emergency Stop Button (CESB)	Central Emergency Stop Button is not activated when required	Train will not stop in case of platform / guideway incident, i.e., PSD incident, intrusion on to the guideway. It will lead to the safety impact. The trains within the emergency area still operate (trains continue moving) leading to an accident	II	E	IIE	When the button is activated, RATP will command all communicating trains in the region to SB and prohibit all the switched in the region to move. The train service can continue after the button is released. Before release the button, the ATS operator needs to ensure that the incident is resolved by using CCTV at the stations/trains or contact with the station/site staff.	SR



Phase 3: Risk Analysis and Evaluation

Safety Critical Item List (SCIL)

Safety Critical Item	Safety Critical Factor	Hazard Effects	Initial Risk			Mitigation Measures	Item Type
			IS	IF	Risk Level		
Vehicle Automatic Train Protection (VATP)	Potential hazard causes include hardware failures of processor and I/O boards, interface failures, and software errors.	Failure to safely perform VATP functions could lead to various hazards that could result in a wide range of effects such as collision, derailment, passengers falling from the platform to the guideway, passengers falling from the train (door open while a train is departing), and passengers trapped in the train.	I	D	ID	Preventive Action / Risk Reduction measures include several safety requirements to ensure that the VATP functions are implemented in a manner that reduces risk to Tolerable risk level	SC



Phase 3: Risk Analysis and Evaluation

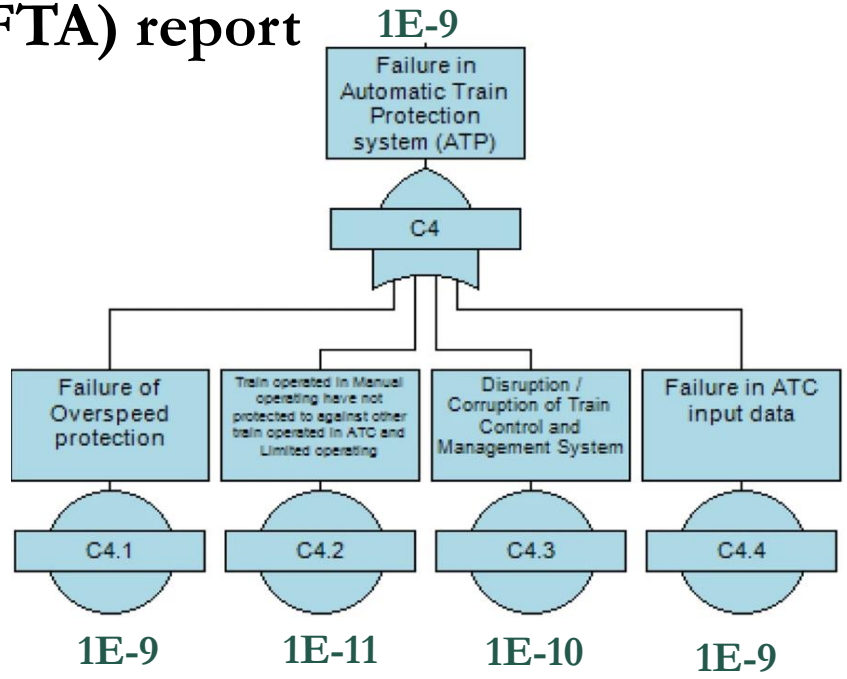
Fault Tree Analysis (FTA) report

- The purpose of this report is to demonstrate that the system reaches the contractual safety target.
- This analysis aims to gather and link the causes leading to each hazard identified at the boundary of the system (identifying the complete list of multiple faults scenarios leading to a hazard).
- It is also used to quantify the achieved safety target for the project.
- The Safety target for the Signalling and Train Control System as the probability of wrong side failure shall be less than 10-9 per train operating hour (SIL4).

Parameter	Description	Unit
Q	Unavailability: Probability that the component or system is not opening at time t, given that it was operating at time zero.	-
W	Failure rate of an intermediate event.	h^{-1}
FR	Failure rate: the probability per time unit that the component or system experiences a failure at time t, given that it was operating at time zero and has survived to time t.	h^{-1}
MTTR	Repair time.	h
Tau	Test interval.	h

Phase 3: Risk Analysis and Evaluation

Fault Tree Analysis (FTA) report



Rate of dangerous failures per hour (Example from ENV 50129 [4]	Tolerable Hazard Rate (THR) per hour and per function (Example from prEN50129 [6])	Safety Integrity Level
$< 10^{-10}$	$10^{-9} \leq THR < 10^{-8}$	4
$\geq 10^{-10}$ to $0.3\ 10^{-8}$	$10^{-8} \leq THR < 10^{-7}$	3
$\geq 0.3\ 10^{-8}$ to $<10^{-7}$	$10^{-7} \leq THR < 10^{-6}$	2
$\geq 10^{-7}$ to $0.3\ 10^{-5}$	$10^{-6} \leq THR < 10^{-5}$	1

Subsystem	SIL
VATP	4
RATP	4
OCS	4
VATO	0
RATO	0
PDCU	4
ATS	0
TWS	0
DTS	0

Fault Tree Analysis: Calculation

Failure rate of an equipment/item

$$FR_i = 1/MTBF_i$$

Note: MTBF is the Mean Time Between Failure of an item
Mean Time To Failure (MTTF) is used for Non-repairable item

Unavailability rate of an equipment/item

$$Q_i = [(Tau_i \times FR_i)/2] + (FR_i \times MTTR_i)$$

Failure rate of an event/situation

For **AND** Gate: $W = Q_A W_B + Q_B W_A$
For **Or** Gate: $W = W_A + W_B$

Unavailability rate of an event/situation

For **AND** Gate: $Q = Q_A \times Q_B$
For **Or** Gate: $Q = Q_A + Q_B$

Phase 4: Specific of System Requirements

Objective:

- Specify the overall **Safety Requirement** of the system.
- Specify the overall demonstration process and criteria for acceptance of safety of the system

Safety Activities:

- Establish **Safety Requirement Specification**
- Establish **Safety Related Application Condition (SRAC)**
- Update hazard log
- Update safety plan
- Establish **validation plan** for safety requirements

Phase 4: Specific of System Requirements

IEC 62290 – 3 Railway applications – Urban guided transport management and command/control systems – Part 3: System requirements specification

{ GOA1: O; GOA2: O; GOA3: O; GOA4: O }

UGTMS shall provide two possibilities for automatic emergency brake release (O):

- during deceleration if actual determined train speed returns below the train protection profile provided there are no other conditions for triggerring the emergency brake
- and/or only if actual train speed is determined as zero and there is no more triggering condition.

{ GOA1: M; GOA2: M; GOA3: M; GOA4: M }

UGTMS shall lock all route elements in a route to be set if they are confirmed in the required position.

{ GOA1: n/a; GOA2: M; GOA3: M; GOA4: M }

UGTMS shall stop the train in station according to the stopping point determined in the train operating profile.

Grade of Automation	Type of train operation	Setting train in motion	Stopping train	Door closure	Operation in event of disruption
GoA1	ATP* with driver	Driver	Driver	Driver	Driver
GoA2	ATP and ATO* with driver	Automatic	Automatic	Driver	Driver
GoA3	Driverless	Automatic	Automatic	Train attendant	Train attendant
GoA4	UTO	Automatic	Automatic	Automatic	Automatic

ATP - Automatic Train Protection; ATO - Automatic Train Operation

Phase 4: Specific of System Requirements

Example Communication Failure (VATP – RATP)

Safety Related Requirement

Requirement 1

When the RATP has declared the train **communication failed**, then the RATP shall **send a service brake command** to the VATP.

Requirement 2

When the VATP receives a service brake request from RATP, then the **VATP shall enforce a service brake** stop by imposing a conflict point at Service Brake distance plus a configurable margin.

Non- Safety Related Requirement

Requirement 1

If the RATP stops receiving valid location updates from a train for a specified period, then the RATP shall declare the train "communication failed".

Requirement 2

When the RATP has declared the train communication failed, then the RATP shall maintain the protection of the communication failed train within the VO assigned to the train at communication failure.

Requirement 3

When the RATP has declared the train communication failed, then the RATP shall maintain route locking within the VO of a communication failed train.

Q&A

Thank you