RAMS and V&V Fundamentals for Railway Applications

Sara STEFANELLI
s.stefanelli@zeta-lab.it

Antonio Scofano
a.scofano@zeta-lab.it

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
Unione europea Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

FOCAL POINTS

1 Why RAMS and V&V activities?

2 What are RAMS and V&V activities?

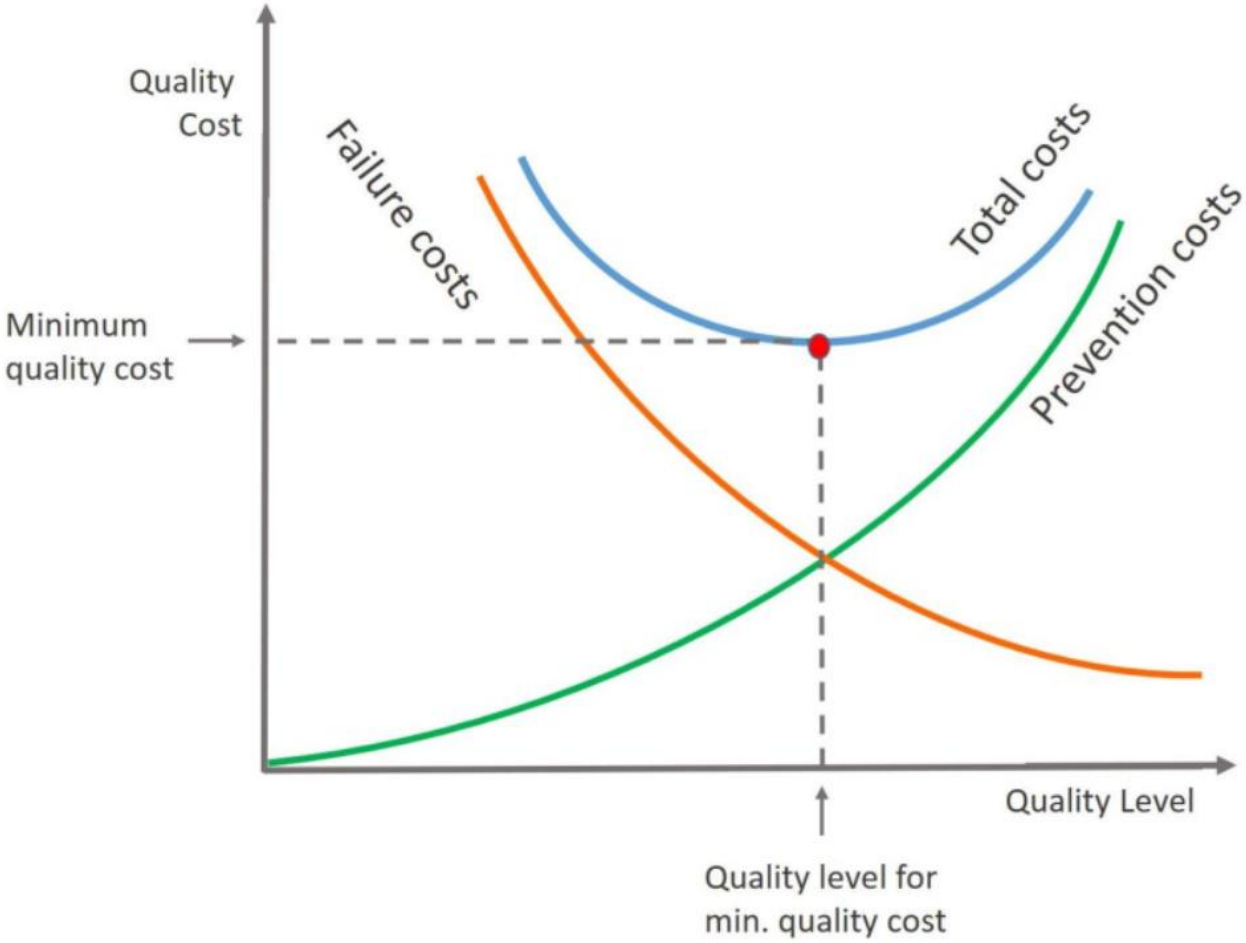
- 2.1 Reliability Prediction
- 2.2 Availability Prediction
- 2.3 Maintainability Analysis
- 2.4 Safety Analysis
- 2.5 V&V activities

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

1. Why RAMS and V&V activities?

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

1. Why RAMS and V&V activities?

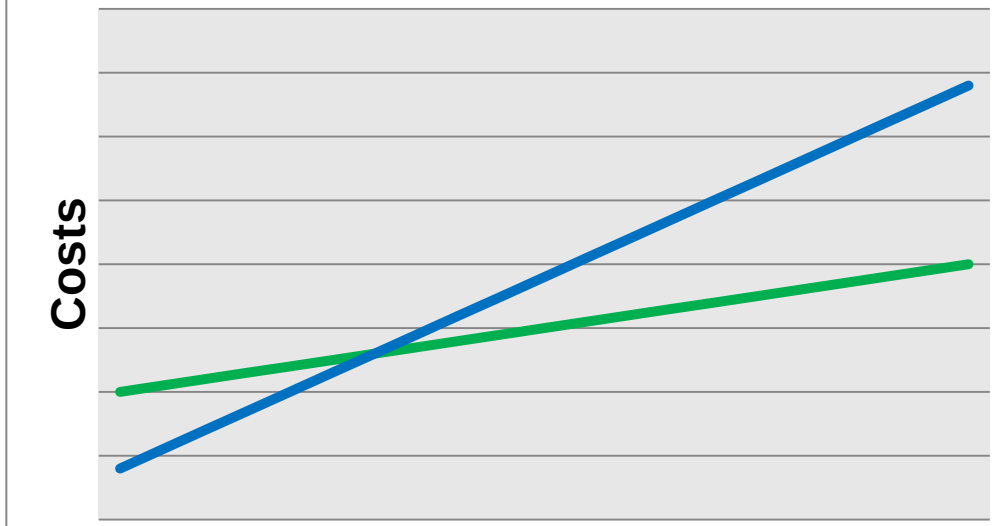


2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

1. Why RAMS and V&V activities?

TRAIN A

TRAIN B



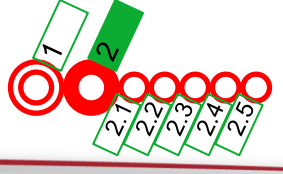
1. Why RAMS and V&V activities?

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

1. Why RAMS and V&V activities?

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2. What are **RAMS** and V&V activities?



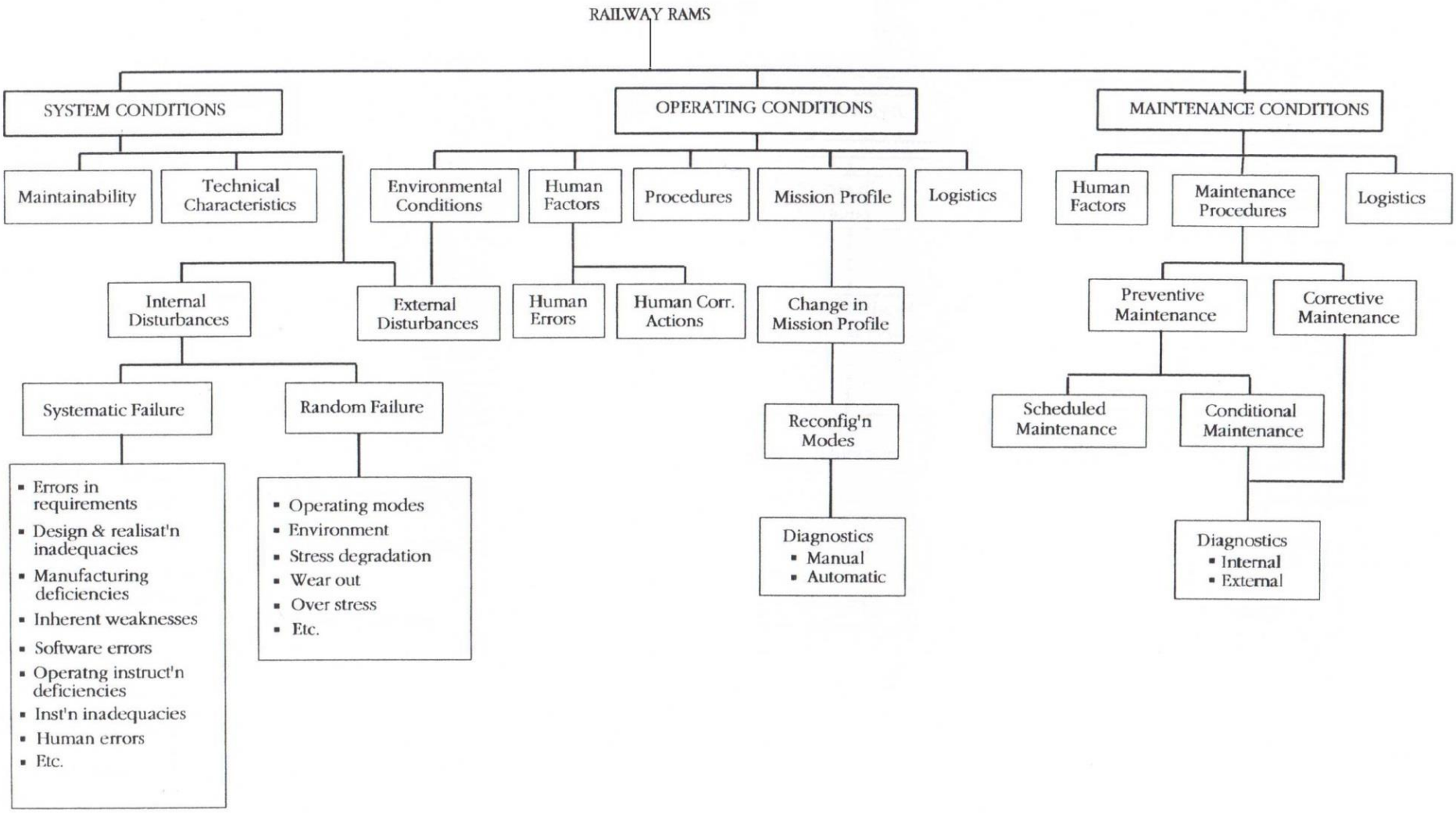
RAMS

Reliability	Confiabilidade
Availability	Disponibilidade
Maintainability	Mantenabilidade
Safety	Segurança

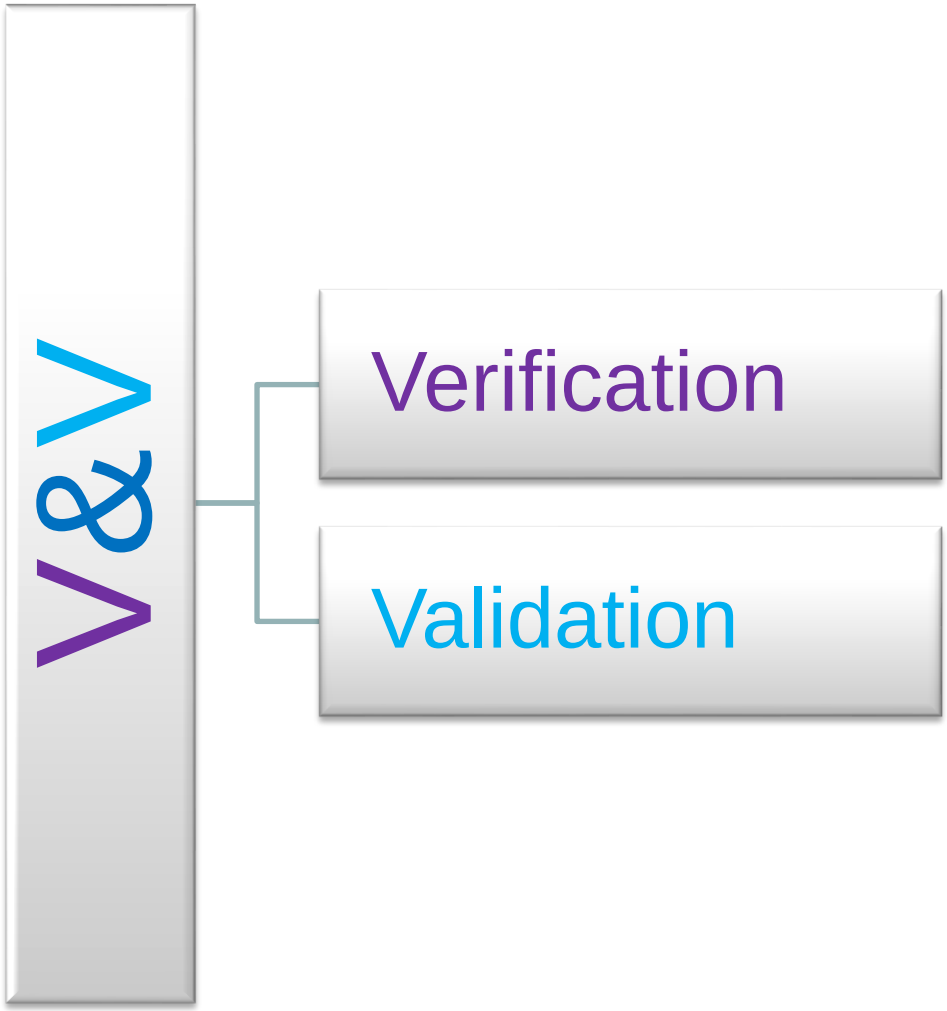
CDMS

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2. What are **RAMS** and V&V activities?

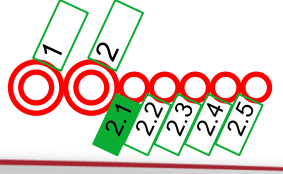


2. What are RAMS and V&V activities?



2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.1 Reliability Prediction



Define the system and all its components parts.

Determine the failure rate of each particular components in the system.

To get the overall system failure rate, add up all the component failure rate.

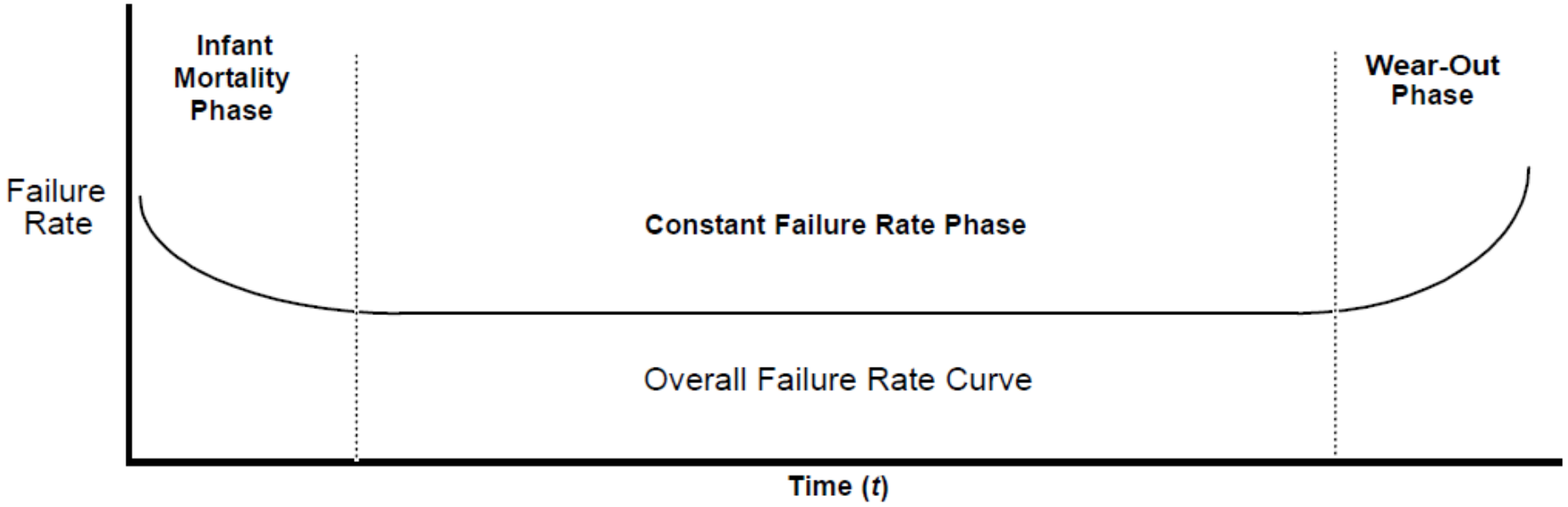
2.1 Reliability Prediction

Failure Rate (λ)

- Number of failure per hour

Mean Time Between Failures

- $MTBF = 1/\lambda$



Bathtub Curve

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.1 Reliability Prediction

Examples of Reliability requirements

5.6 Affidabilità

[illegible] di veicolo deve avere un valore di MTBF reale, misurato sul campo in condizioni di esercizio, di almeno 80.000 ore. Tali valori di MTBF saranno calcolati mediante il rapporto tra il numero delle ore totali di esercizio effettuate dagli impianti/apparati installati su una flotta campione ed il numero di guasti riscontrati nel periodo.

Ai fini del calcolo dell'MTBF deve intendersi per guasto ogni guasto di *tipologia grave* o *maggiore* in conformità alla norma UNI 11565.

MTBF ≥ 80.000 hours.

12 Requisiti affidabilistici

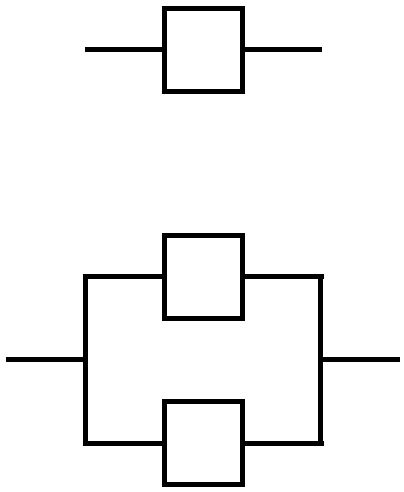
Con "riserva" si intende ogni malfunzionamento, avaria, guasto o inconveniente relativo all'equipaggiamento oggetto di fornitura per cui si determina il mancato svolgimento della funzione richiesta al sistema antincendio o interventi indebiti dell'antincendio o indisponibilità del sistema antincendio.

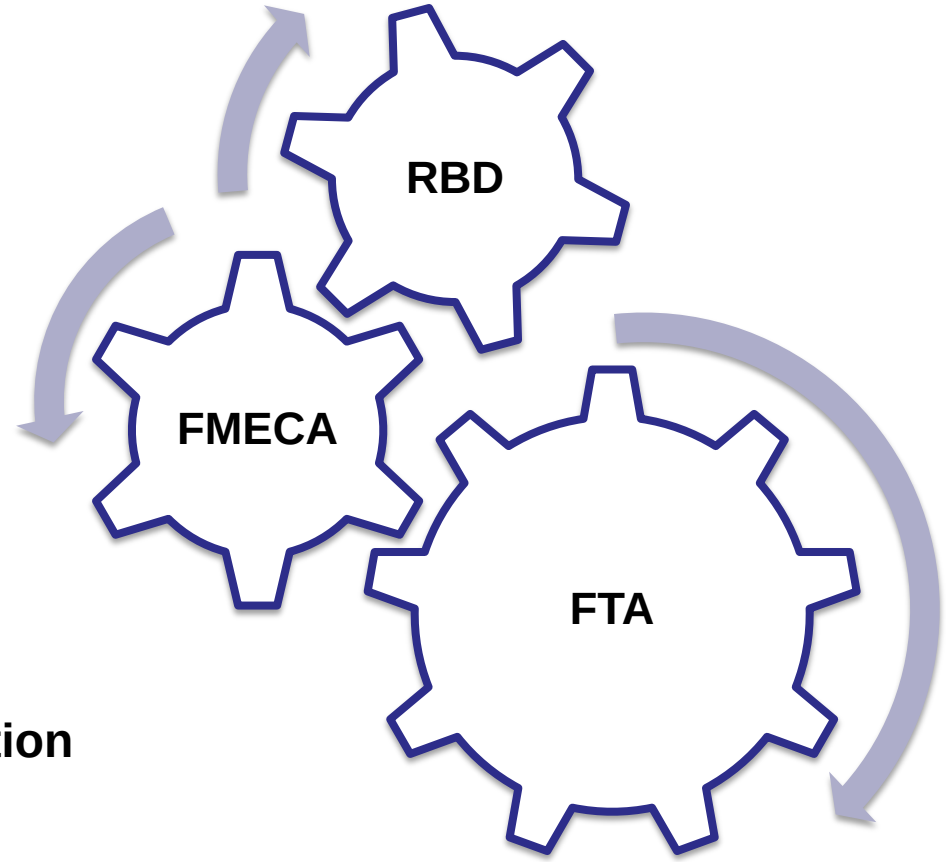
I valori di affidabilità (espressi in: riserve/10^6 km) saranno definiti dal fornitore.

Il fornitore a seguito di analisi FMECA, FTA e quanto altro necessario deve specificare ed individuare in dettaglio tutti gli specifici eventi che possono generare "riserva".

Tutte le avarie e tutte cause di generazione di una riserva devono essere tracciate in diagnostica in modo specifico e puntuale.

2.1 Reliability Prediction





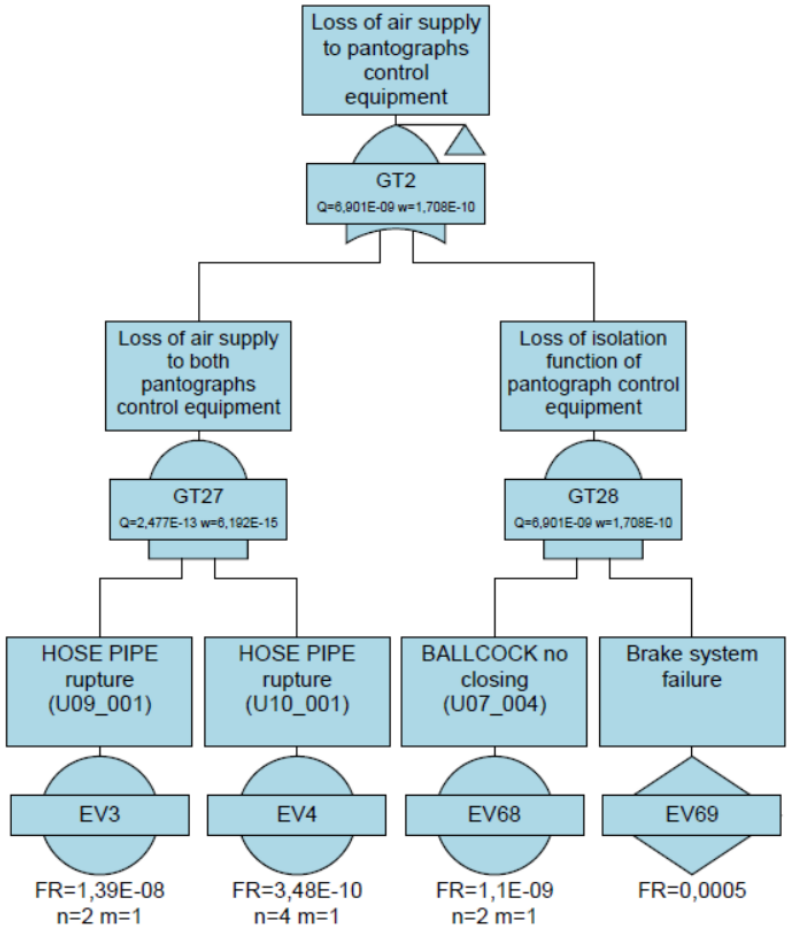
Mission Reliability Prediction

2.1 Reliability Prediction

Example of FMECA

Foglio di lavoro
di Microsoft Excel

Example of FTA



2.1 Reliability Prediction

Examples of Mission Reliability requirements

The following reliability performances shall be reached:

SEC	ALFA [events/10e6 km]
Brake & Pneumatic	**< 0,34**
N.B.: *being the result of multiple events, the "Mission Reliability" (**ALFA**) figure is calculated at "Vehicle level"*	

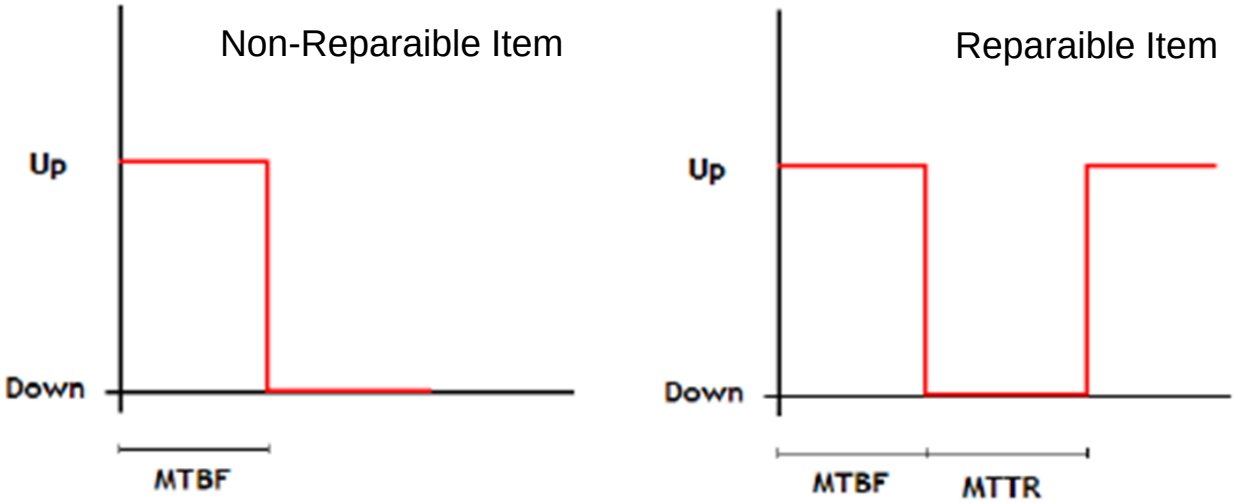
The events to be considered as **Mission Failure** for the SEC are those that lead to a maximum speed reduction greater than 20%; at least (but not limited to these) the following events are to be evaluated by the Supplier :

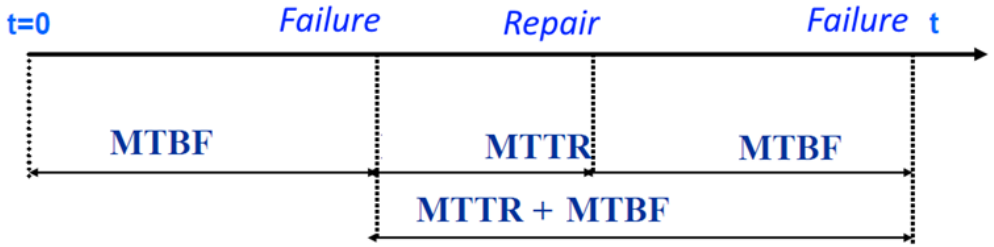
- brake caliper stuck on one bogie or more;
- more than two Bogies Brake isolation;
- more than one car brake isolation;
- Complete loss of compressed air.

During the project phase it is also required to perform the FMECA to analyze failure modes causing both Safety and Mission Reliability issues. The following is the table to be adopted (when producing the FMECA) in ranking the effects over the Mission reliability (revenue service):

EFFECTS ON "MISSION"	RANKING
No effects on revenue service	N
Vehicle withdrawal and/or a service delay ≥ 15 minutes.	A

2.2 Availabilty Prediction





$$Availability = \frac{MTBF}{MTBF + MTTR}$$

2.2 Availabilty Prediction

Example of Failure categories to define the Reliability and Availability performances:

- **Significant:** Each anomaly, fault or trouble causing a service delay ≥ x minutes
- **Major:** Each anomaly, fault or trouble causing a functional degradation and/ or a service delay ≤ x.

- **Minor:** Any failure occurring on the System, that is not classified as significant or major, leading to a maintenance task, even if this failure has no impact on service

2.2 Availabilty Prediction

Examples of Availability requirements

4.2. Disponibilità

Il parametro è definito come il rapporto tra i minuti di servizio effettuati ed i minuti di servizio programmati.

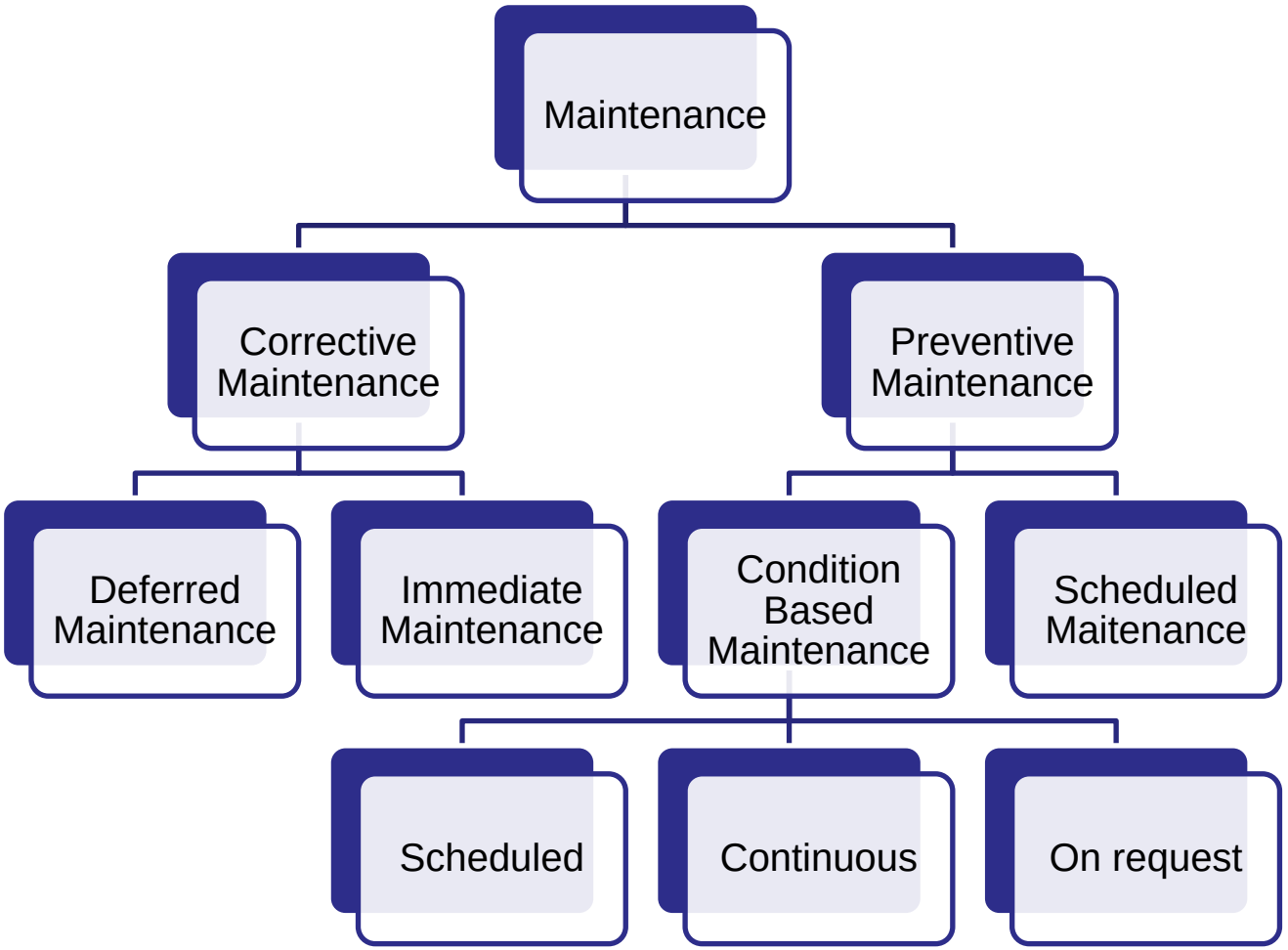
$$Disponibilità = \frac{\min uti.di.servizio.effettuati}{\min uti.di.servizio.programmati} * 100$$

I minuti di servizio effettuati sono valutati in rapporto al numero di stazioni servite, allo scopo di considerare nella valutazione del parametro i periodi in cui il servizio offerto non è completo (non tutte le stazioni sono servite). In pratica, per ogni periodo di servizio non completo, il valore dei minuti di servizio effettuati sono calcolati come segue:

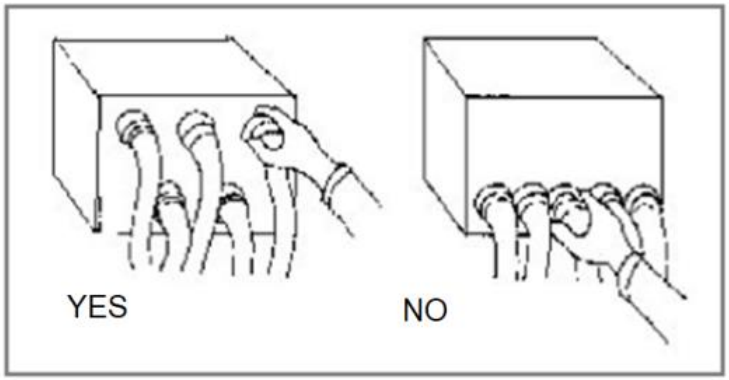
$$\min uti.di.servizio.effettuati = \min uti.di.servizio.non.completo \times \frac{numero.stazioni.servite}{numero.stazioni.totali}$$

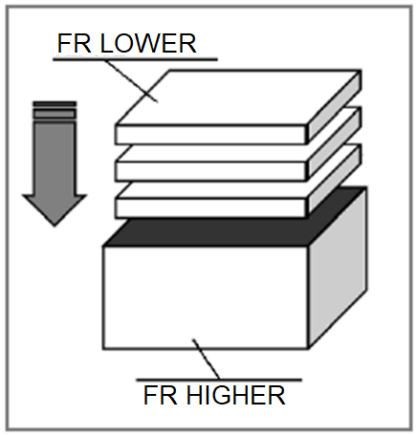
Il valore target indicato dalle Specifiche di contratto [2] per questo parametro è pari a **98,55%.**

2.3 Maintainability Analysis



Design for Maintainability





2.3 Maintainability Analysis

Examples of Maintainability requirements

[R-DMS-1779] The maximum corrective maintenance time (MCMT) and the maximum mean time to repair (Max MTTR) shall have the values given in:

[R-DMS-1780]

MTTR [hr]	MCMT at 90th percentile [hr]
24	48

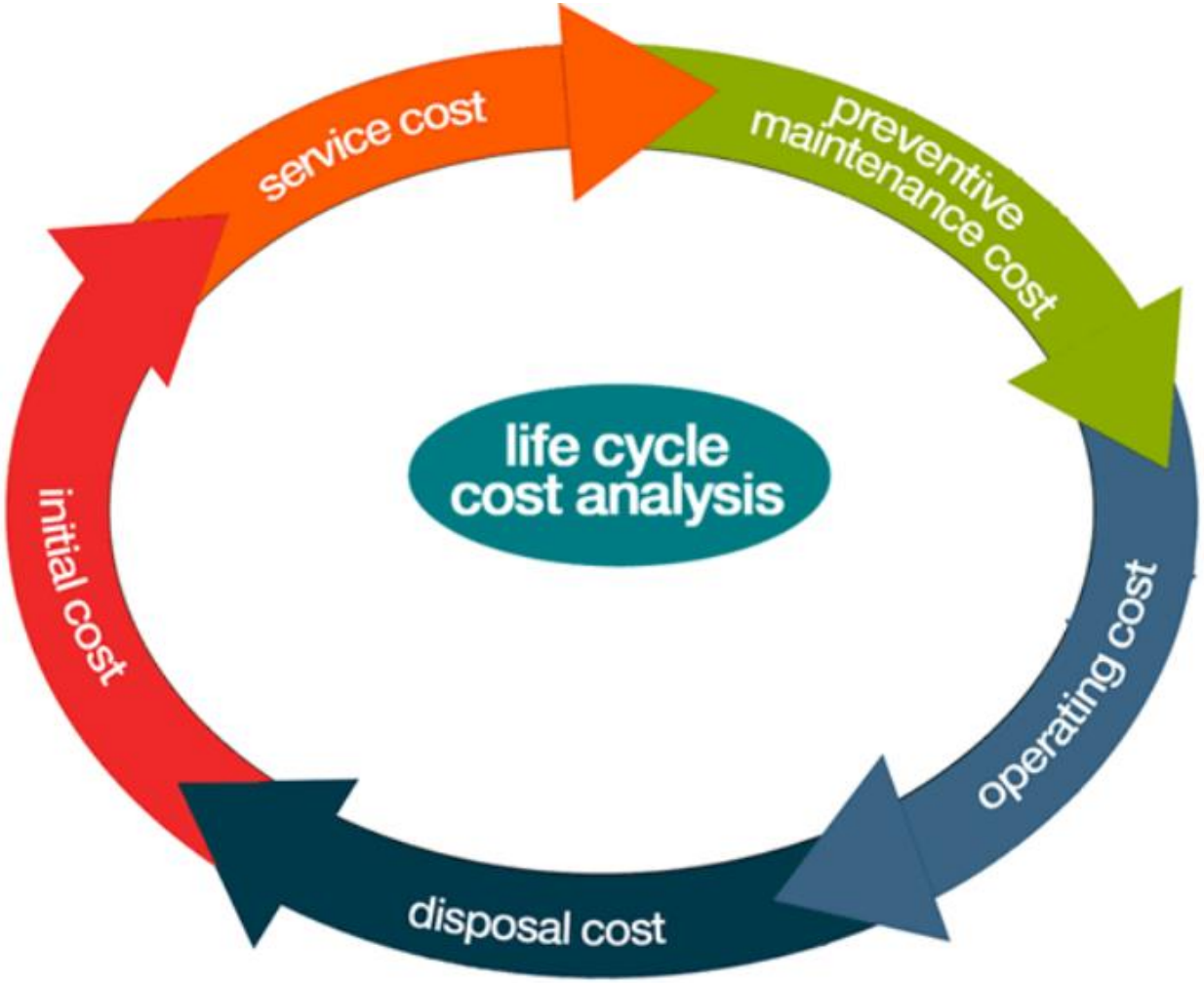
Table 9.3.2-1: Summary Table for max MTTR and MCMT for Corrective Maintenance

[R-DMS-1781] The time specified in requirements Table 9.3.2-1 shall be considered to be the clock time.

[R-DMS-1782] Any corrective maintenance action shall be performed with a maximum of 3 qualified maintenance technicians, using standard tools and/or special tools specific to the Dome and Main Structure design.

[R-DMS-1783] The time to repair (TR) shall be considered as the elapsed time between the event of communicating the occurrence of a failure (e.g. reporting the occurrence in a software tracking system) and the event of communicating the restoration of the System (reporting the failure resolution in a software tracking system) and assuming that the spares and necessary manpower are readily available where applicable (no logistic delay and administrative delay time shall be considered).

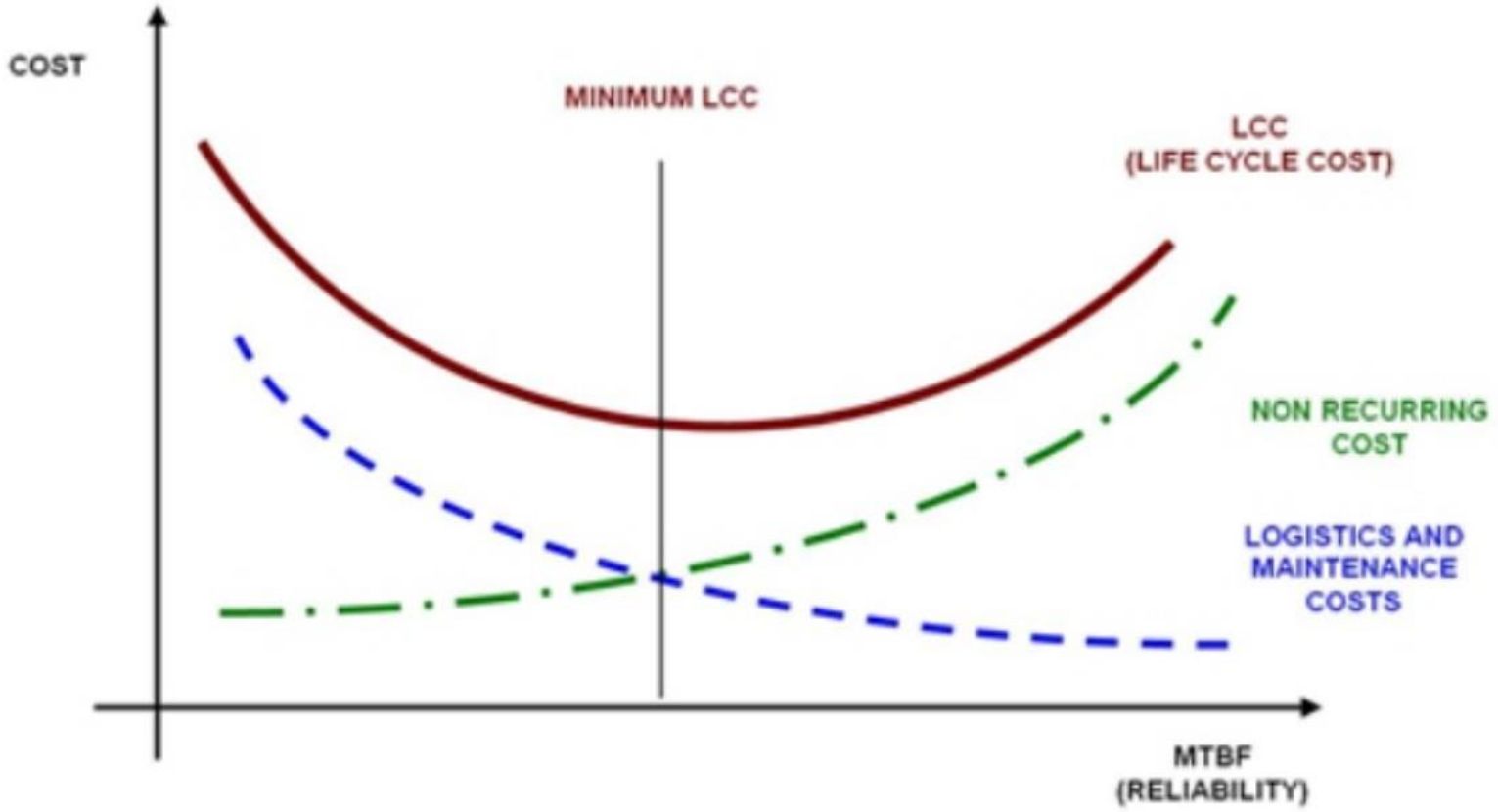
2.3 Maintainability Analysis



2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.3 Maintainability Analysis

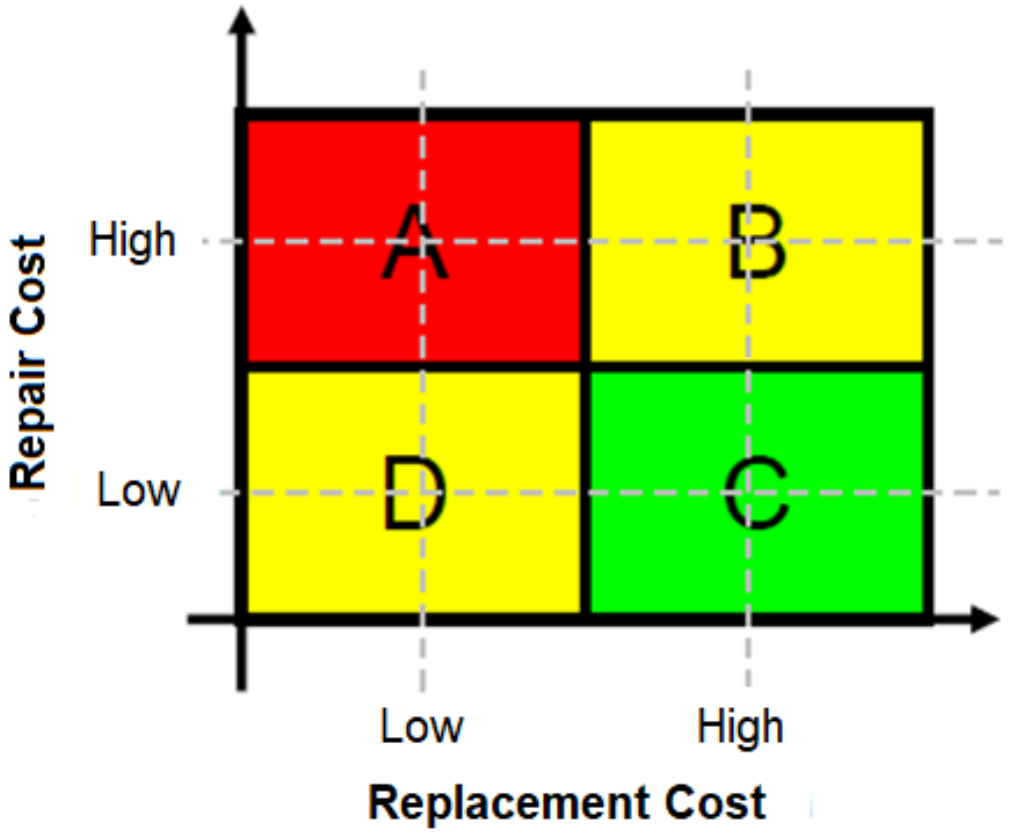
Cost vs Reliability Trade Off



2014 2020 POR CreO
PROGRAMMA OPERATIVO REGIONALE
CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.3 Maintainability Analysis

Maitenance Strategy



2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.3 Maintainability Analysis

Examples of LCC Requirements

SEC	MATPM [EUR/10e3 km]	MHRPM [EUR/10e3 km]
Brake & Pneumatic *(Vehicle level – 5 cars)*	**< 147,126 (Note)**	**< 21,205**
N.B.: *the preventive maintenance costs are to be calculated over the whole Vehicle life (25 years) taking into consideration the actual numbers of basic operations to be performed – eg.: the "1 year" interval operation will be performed 24 times only (at the end of the 25 years the Vehicle will be definitely out of service).* *Note: the cost of brake pads is excluded.*		

SEC	MATCM [EUR/10e3 km]	MHRCM [EUR/10e3 km]
Brake & Pneumatic *(Vehicle level – 5 cars)*	**< 15,5 (Note)**	**< 1,4**
N.B.: *the corrective maintenance costs are to be calculated taking into account the supposed occurrence frequency (failure rate) of the SEC parts.* *Note: the cost of brake pads is excluded.*		

Examples of LCC

LCC Example

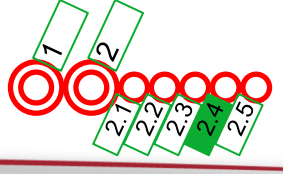
2.4 Safety Analysis

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

Risk = Severity x Frequency

SEVERITY	CONSEQUENCES TO PERSONS OR ENVIRONMENT
Catastrophic	Fatalities and/or multiple injuries and/or major damage to the environment
Critical	Single fatality and/or severe injury and/or significant damage to the environment
Marginal	Minor injury and/or significant threat to the environment
Insignificant	Possible minor injury

2.4 Safety Analysis



Frequency of occurrence	Severity Levels of Hazardous Consequences			
	INSIGNIFICANT	MARGINAL	CRITICAL	CATASTROPHIC
FREQUENT	Undesirable	Intolerable	Intolerable	Intolerable
PROBABLE	Tolerable	Undesirable	Intolerable	Intolerable
OCCASIONAL	Tolerable	Undesirable	Undesirable	Intolerable
REMOTE	Negligible	Tolerable	Undesirable	Undesirable
IMPROBABLE	Negligible	Negligible	Tolerable	Tolerable
INCREDIBLE	Negligible	Negligible	Negligible	Negligible

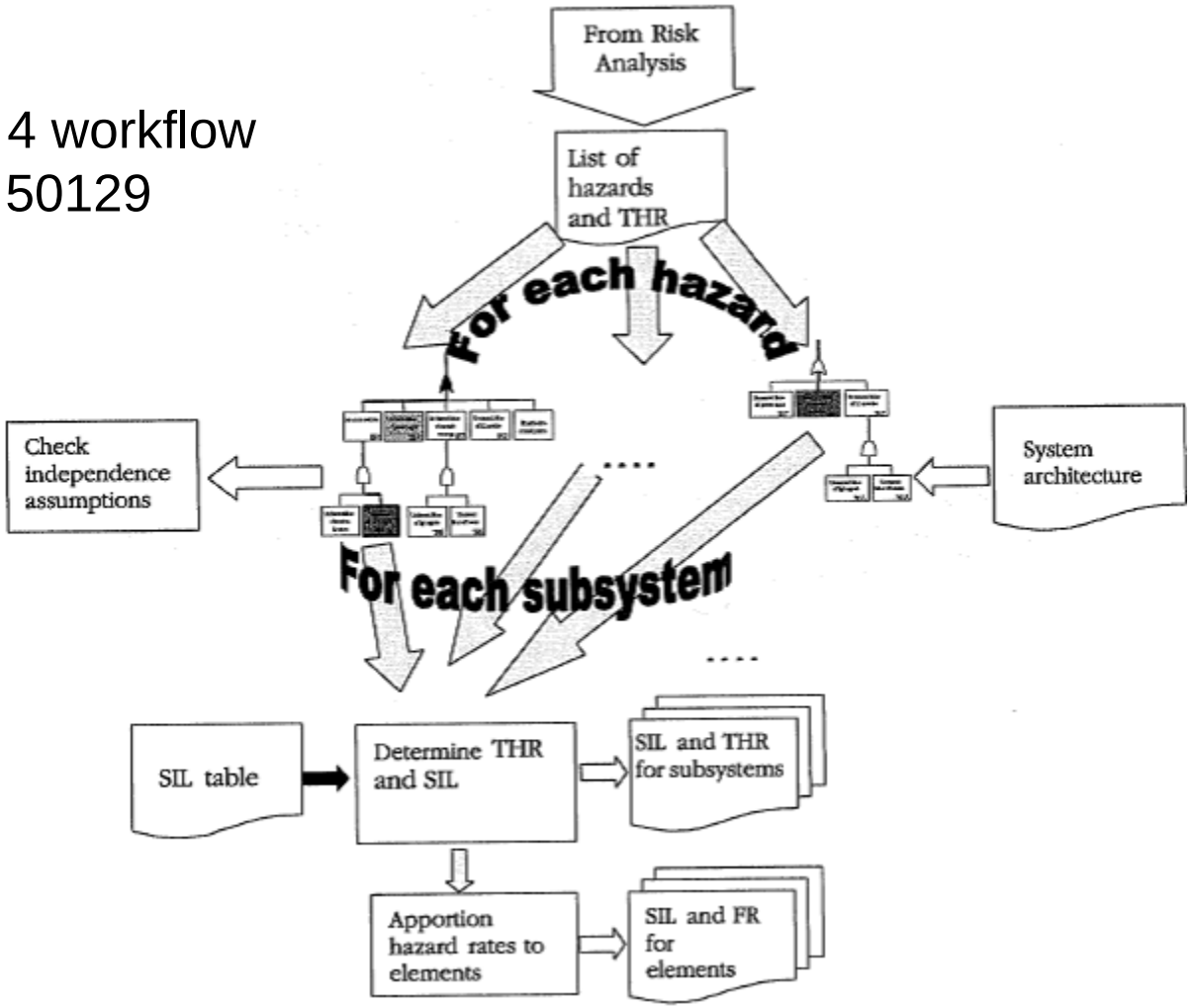
RISK EVALUATION	RISK REDUCTION/CONTROL
INTOLERABLE	Shall be eliminated
UNDESIRABLE	Shall only be accepted when risk reduction is impracticable and with agreement of Railway autority
TOLERABLE	Acceptable with agreement of Railway autority
NEGLIGIBLE	Accepted without any agreement

SIL Requierements

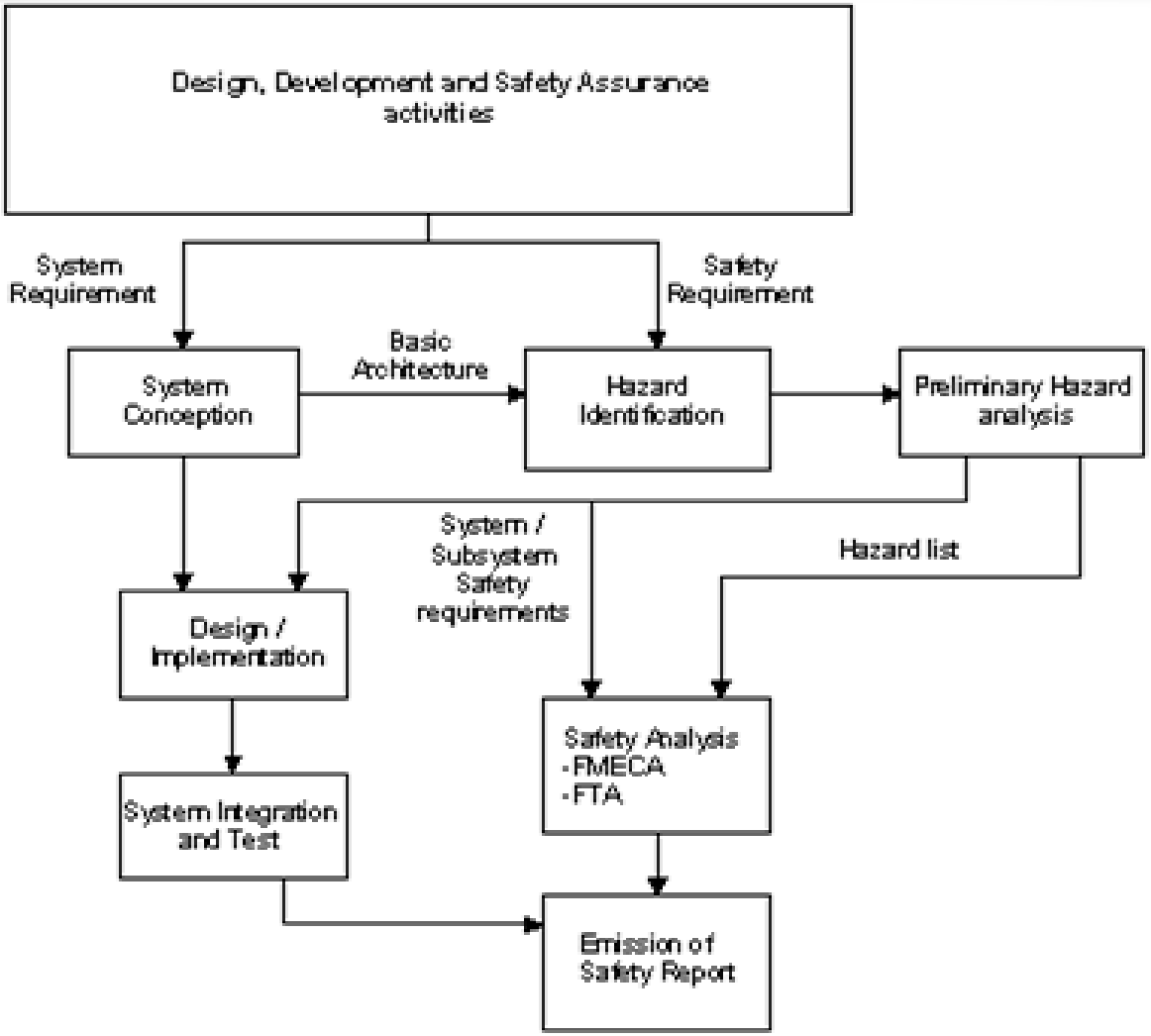
Torelable Hazard Rate (THR) per hour and function	Safety integrity level
$10^{-9} \leq THR \leq 10^{-8}$	4
$10^{-8} \leq THR \leq 10^{-7}$	3
$10^{-7} \leq THR \leq 10^{-6}$	2
$10^{-6} \leq THR \leq 10^{-5}$	1

2.4 Safety Analysis

HW SIL 4 workflow
EN 50129



2.4 Safety Analysis

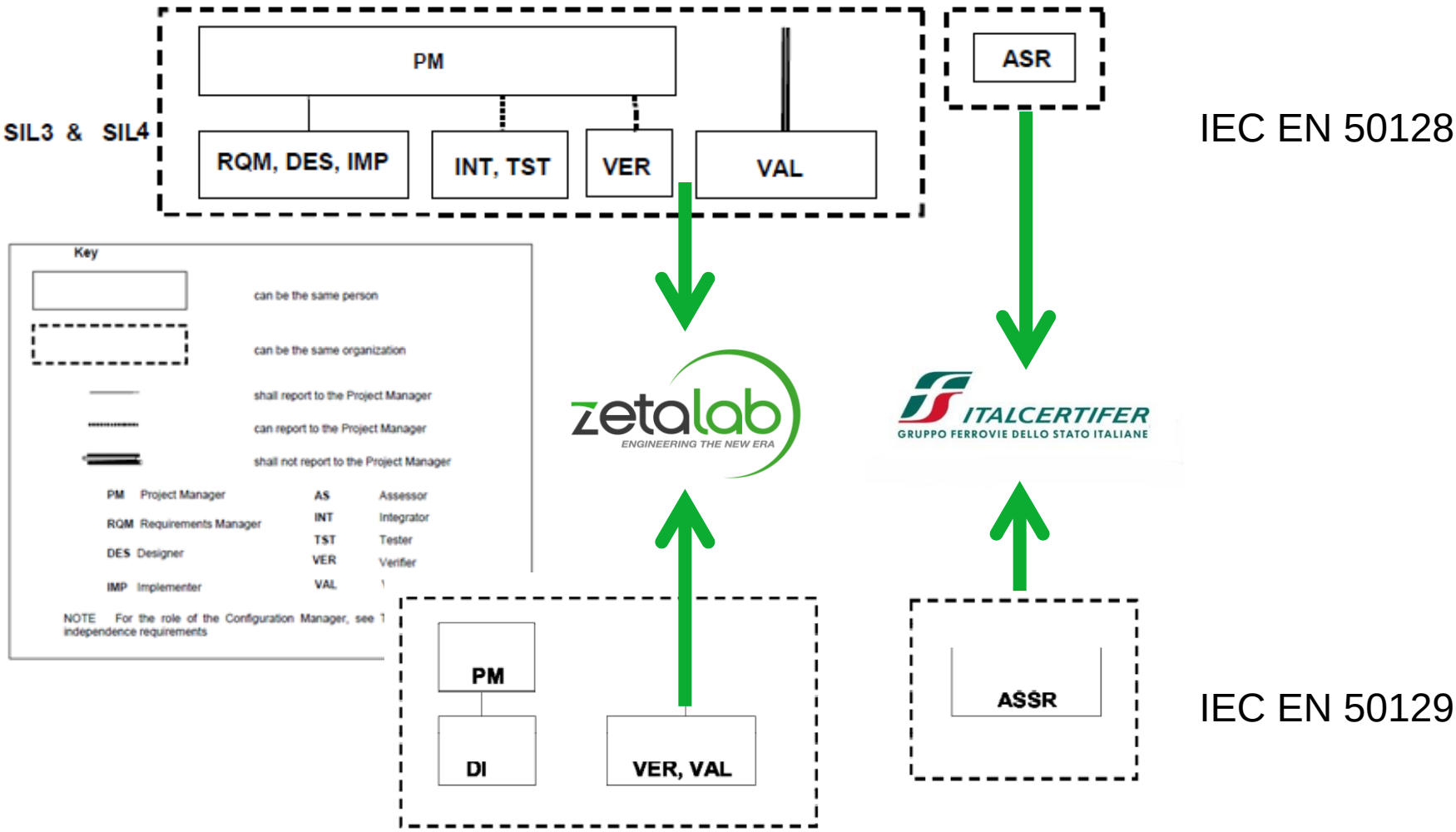


2.4 Safety Analysis

Hazard Analysis												
Project: AFTC **Supplier: HISTACO**									**Issue: 00** **Date: 12/07/2017** **edited by:**			
ID	**Mission Phase**	**Hazard**	**Cause**	**Consequence**	**Frequency**	**Severity**	**Risk**	**Proposed Controls**	**Frequency**	**Severity**	**Risk**	**Note**

ID	Identification Number for each Hazard
Mission Phase	Operating phase in which the hazard could be occur
Hazard	Description of hazard
Cause	Description of cause
Consequence	Description of consequence associated to each hazard (it's been considered the worst case for the environment)
Frequency	Frequency of occurrence according to EN 50126
Severity	Severity Levels of Hazardous Consequences according to EN50126
Risk	The risk associated (as product between Frequency and Severity)
Proposed Control	The control which is proposed as mitigation for risk calculated and associated to each hazard
Frequency	Frequency of occurrence according to EN 50126 and associated to new proposed control
Severity	Severity Levels of Hazardous Consequences according to EN50126 and associated to new proposed control
Risk	The risk associated (as product between Frequency and Severity) and associated to new proposed control
Remarks	Remarks if necessary.

2.5 Verification and Validation

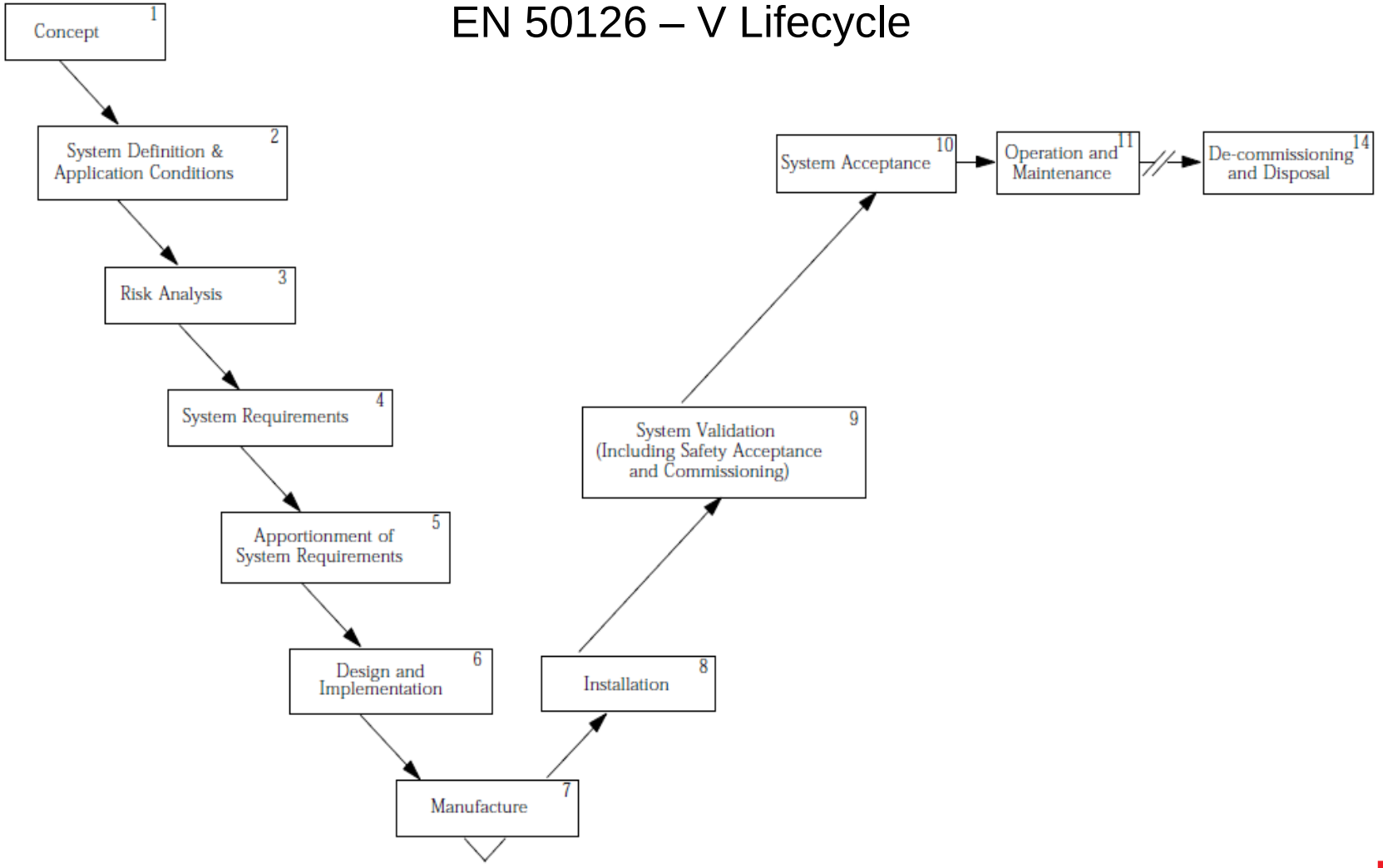


IEC EN 50128

IEC EN 50129

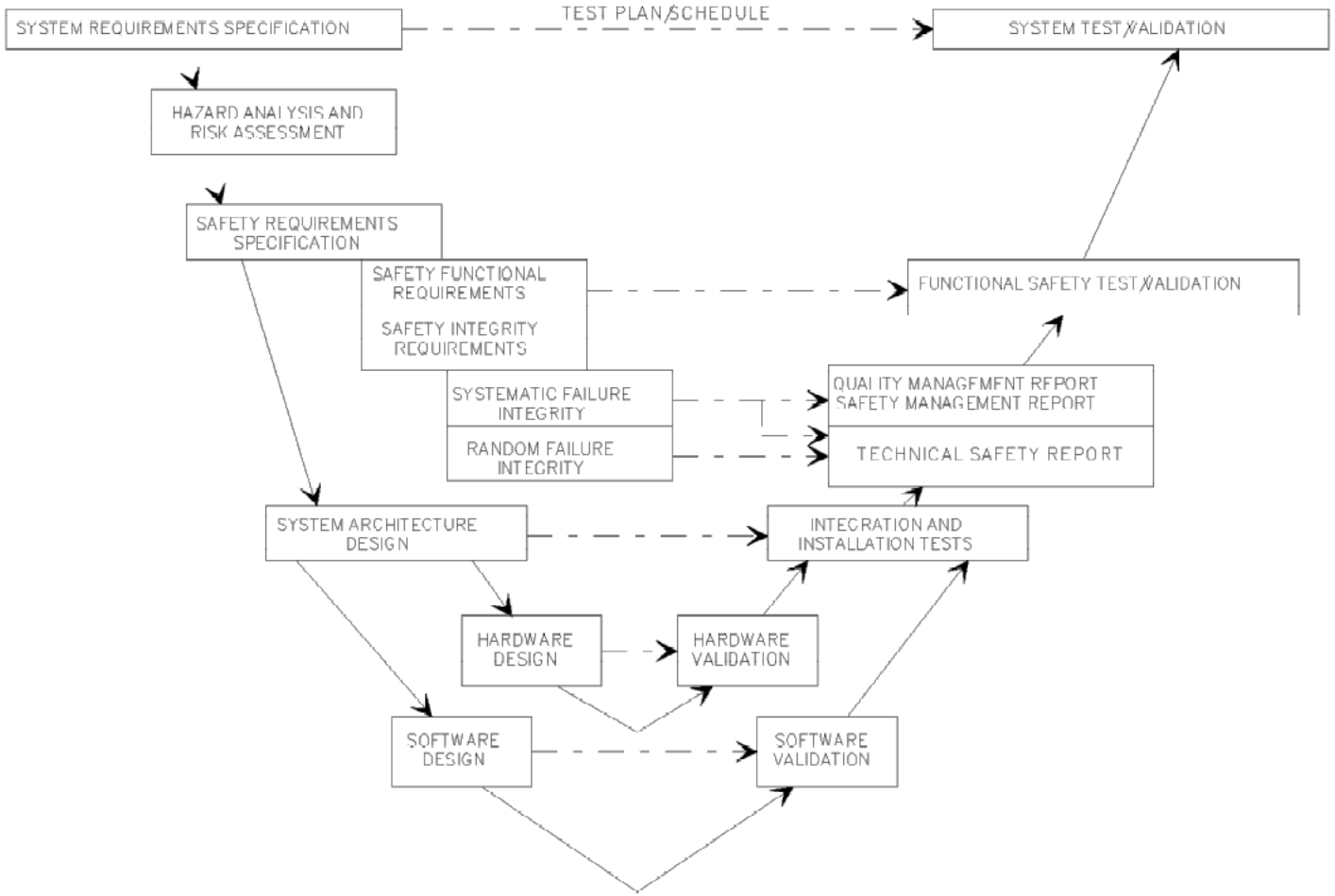
2.5 Verification and Validation

EN 50126 – V Lifecycle



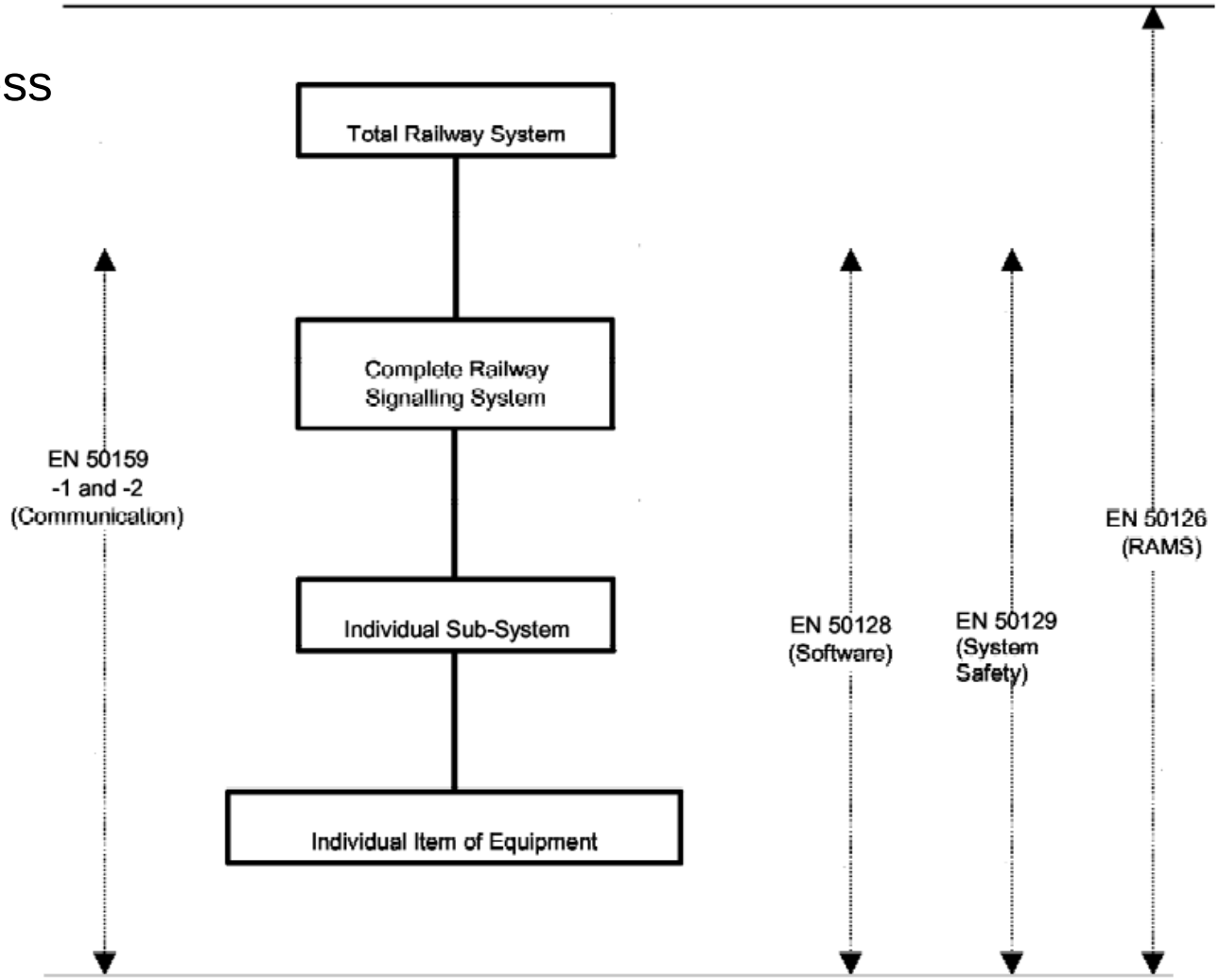
2.5 Verification and Validation

V&V Process



2.5 Verification and Validation

V&V Process



Reference Standards

- **EN 50126-1: 2017** Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process
- **EN 50126-2:2007** Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety
- **EN 50126-3:2006** Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the application of EN 50126-1 for Rolling Stock
- **EN 50128:2011** Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems
- **EN 50129:2003** Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling
- **EN ISO 9001** Quality management systems – Requirements (ISO 9001:2008)
- **EN 50155:2002** Railway applications – Electronic equipment used on rolling stock
- **EN 50121:2007** Railway applications – Electromagnetic compatibility
- **EN 50124-1:2005** Railway applications – Insulation coordination Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment
- **EN 50125-1:2000** Railway applications – Environmental conditions for equipment . Part 1: Equipment on board rolling stock
- **EN 50153:2003** Railway applications – Rolling stock - Protection measures against electrical hazards
- **EN 50159-1:2002** Railway applications – Communication, signaling and processing systems - Part 1: Safety-relevant communications in a closed transmission network

2.5 Verification and Validation

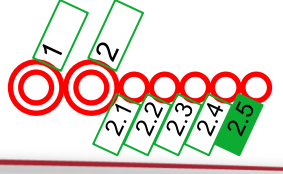
Software architecture - EN 50128

Technique/Measure	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
Fully Defined Interface	HR	HR	HR	M	M
Modular Approach	HR	M	M	M	M
Design and Coding Std	HR	HR	HR	M	M

Verification and testing - EN 50128

Technique/Measure	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
Traceability	R	HR	HR	M	M
Functional/Black-box Testing	HR	HR	HR	M	M
Performance Testing	-	HR	HR	M	M
Functional and Black-box Testing	HR	HR	HR	M	M
Compliant with EN ISO 9001	M	M	M	M	M
Complianti with ISO/IEC 90003	R	R	R	R	R
Company Quality System	M	M	M	M	M
Software Configuration Management	M	M	M	M	M
Checklists	R	HR	HR	HR	HR
Data Recording Analysis	HR	HR	HR	M	M

2.5 Verification and Validation



- Receiving complete documentation as reported in Documentation Plan
- Reference of laboratory in which type test, functional test and series tests are executed
- Name, Curriculum Vitae and Role of each component team;
- Organization chart to demonstrate the independence of roles;
- Project deadline

Which documents ?

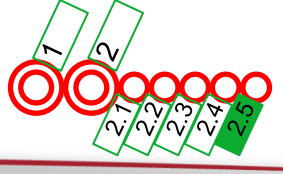
Depends on Safety Integrity Level (SIL)

2.5 Verification and Validation

SIL 4 system documents list

1. Safety Plan
2. Verification and Validation Plan
3. Verification and Validation Report
4. System Functional Hazard Analysis
5. System Requirements Specification
6. System Architecture Specification
7. Hazard Log
8. Functional Test Specification
9. Funzional Test Report
10. Requirements Traceability Matrix
11. SW Requirements Verification Report
12. SW Architecture Requirement and Component Design Verification
13. SW Source Code Verification Report
14. HW/SW Integration Test Specification
15. HW/SW Integration Test Report
16. SW Integration Test Specification
17. SW Integration Test Report
18. SW Verification and Validation Plan
19. SW Verification and Validation Report
20. SW Component Test Specification
21. SW Component Test Report
22. SW – Static and Quality Analysis
23. SW – Non regression Analysis
24. SW – Validation Test Plan
25. SW – Validation Test Report
26. Type Test Plan
27. Type Test Procedure
28. Type Test Report
29. Product RAM analysis
30. MTBHE Evaluation
31. Subsystems FMEA
32. Configuration Management Plan
33. Software Configuration Management Plan
34. Software Requirements Specification
35. Hardware Design Specification
36. Installation User and Maintenance Manual
37. Quality Plan
38. Software Quality Assurance Plan
39. System Safety Report
40. **Generic Product Safety Case**

2.5 Verification and Validation



SAFETY CASE

Part 1 Definition of System

Part 2 Quality Management Report

Part 3 Safety Management Report

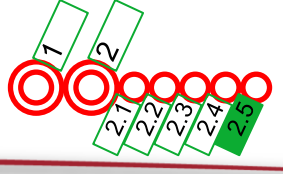
Part 4 Technical Safety Report

Part 5 Related Safety Cases

Part 6 Conclusion

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

2.5 Verification and Validation



SAFETY CASE

Part 1 Definition of System

Part 2 Quality Management Report

Part 3 Safety Management Report

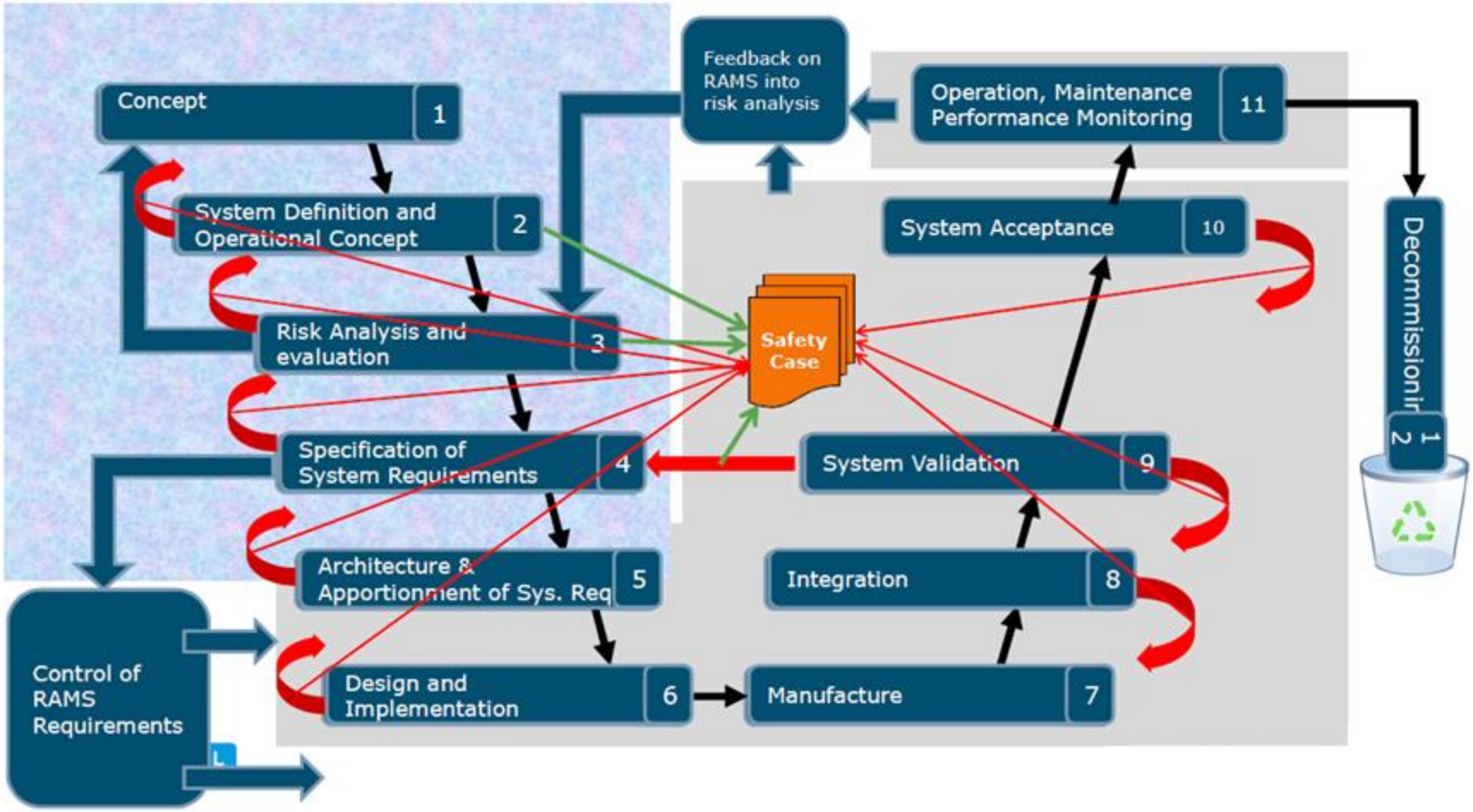
Part 4 Technical Safety Report

- Introduction
- Assurance of correct operation
- Effects of faults
- Operation with external influences
- Safety-related application conditions
- Safey qualification tests

Part 5 Related Safety Cases

Part 6 Conclusion

Conclusion: Safety Case



2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana

Thanks for the attention

2014 2020 POR CreO PROGRAMMA OPERATIVO REGIONALE CRESCITA e OCCUPAZIONE
zetalab BRASIL
TECNAU
Unione europea
Fondo Europeo di Sviluppo Regionale
REPUBBLICA ITALIANA
Regione Toscana