Ansaldo STS

A Hitachi Group Company

A Lean approach to CENELEC compliance

ASSC 2018

Dr Andrew Hussey

RAMS and Railway

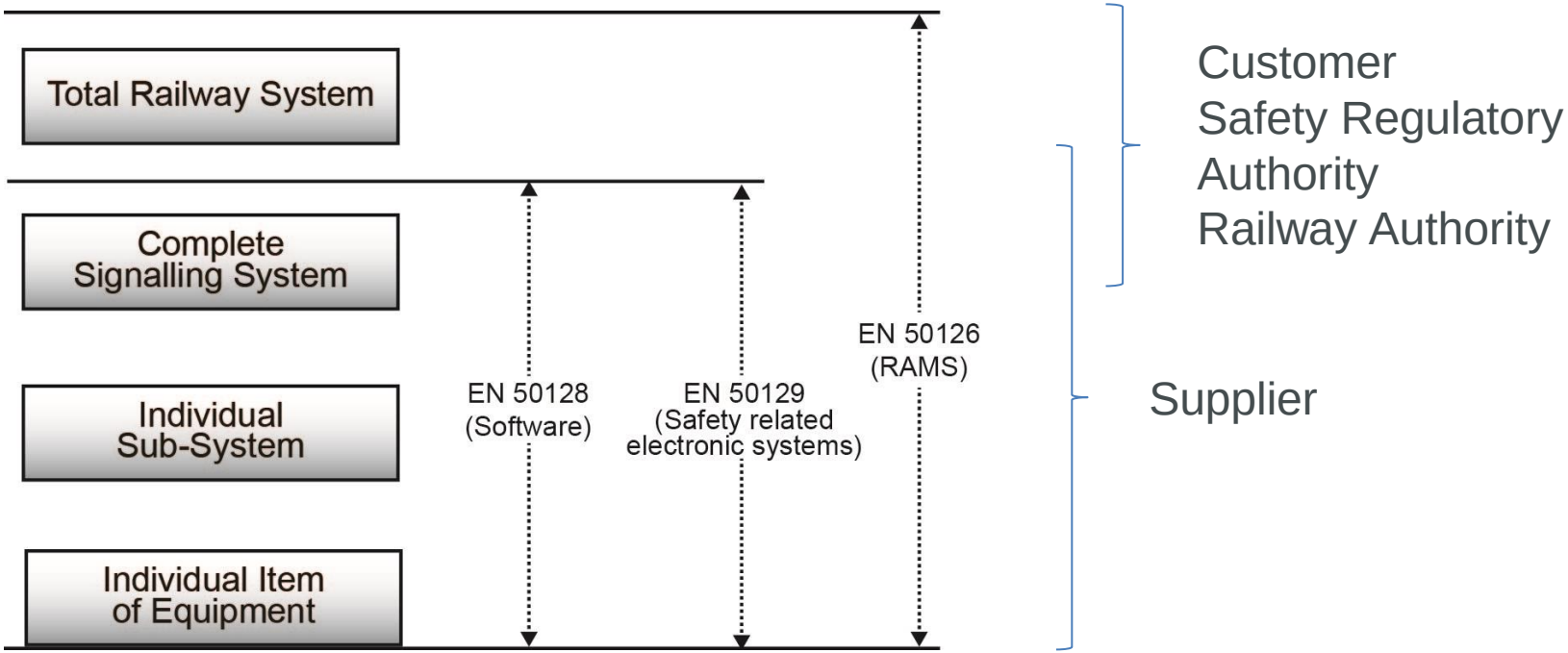
One key goal for a railway system is to safely achieve a defined level of rail traffic in a given time

Railway RAMS is achieved via techniques and process that enable the system to meet this goal

Multiple organisations (operator, integrator, suppliers, developers) must co-ordinate to deliver that outcome

The interface between these organisations gives rise to process inefficiencies and potential waste

CENELEC Standards and Responsibilities



Project phase related tasks are allocated to ASTS/Customer

Lean

Mainly concerned with eliminating process waste

Originated in the Japanese manufacturing industry but abstract concepts broadly applicable

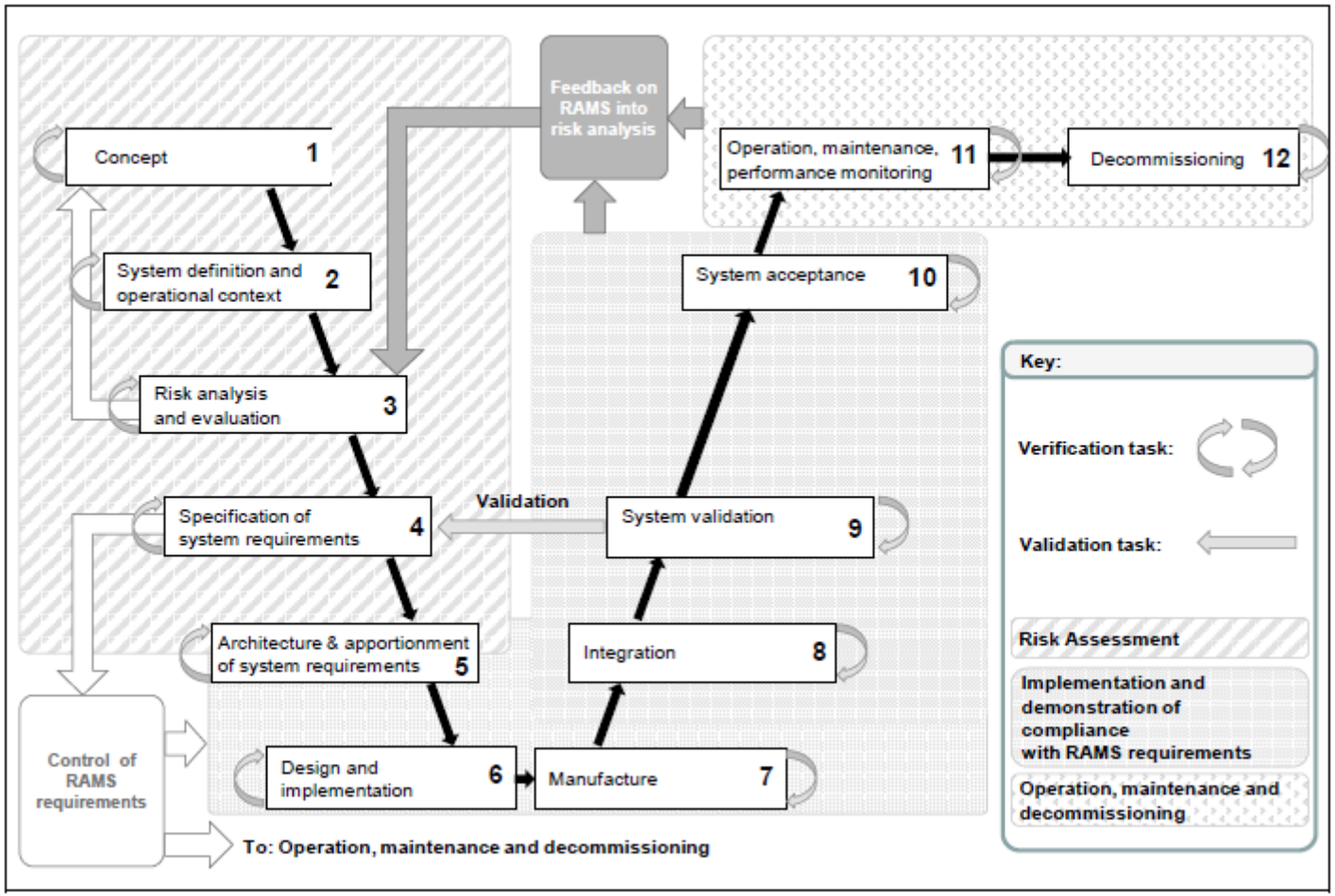
Core premise is that one should act (methods and tools) in a way that is based on overarching organisational values and principles

- Values – the organisational ethics (“right” and “wrong”) e.g. Team Spirit and Integrity, Harmony and Sincerity
- Principles – how the organisation “thinks” in terms of overarching process goals aligned with Values e.g. early lifecycle communication of information between Supplier and Operator
- Methods and Tools – defining how the organisation works and the tools used to perform that work

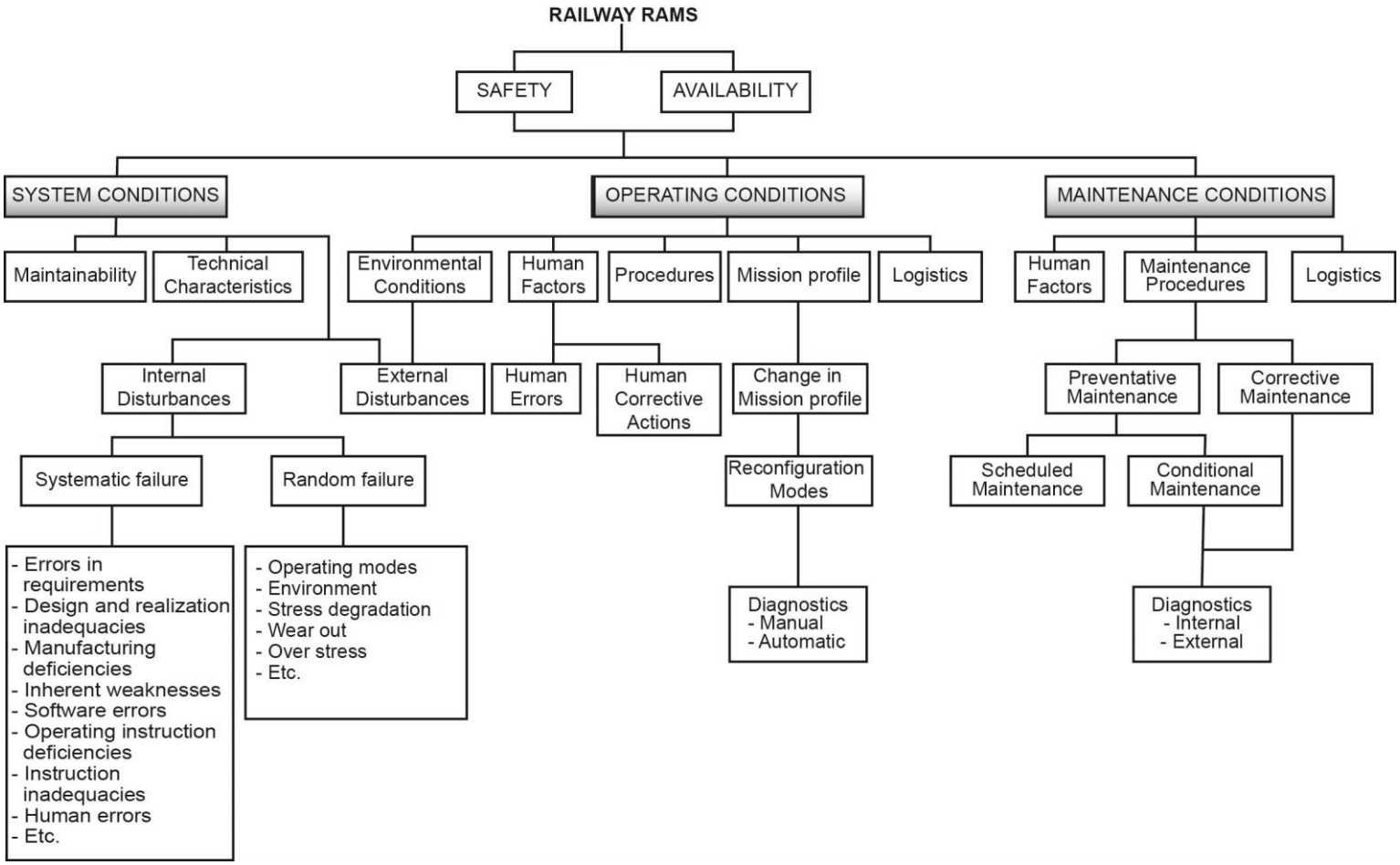
Values, principles, methods and tools are oriented towards process effectiveness (“flow” of a product through the development lifecycle – reducing process variation, downtime and rework)

e.g. Womack, Jones, Roos (1990s); Modig, Ålström (2010s)

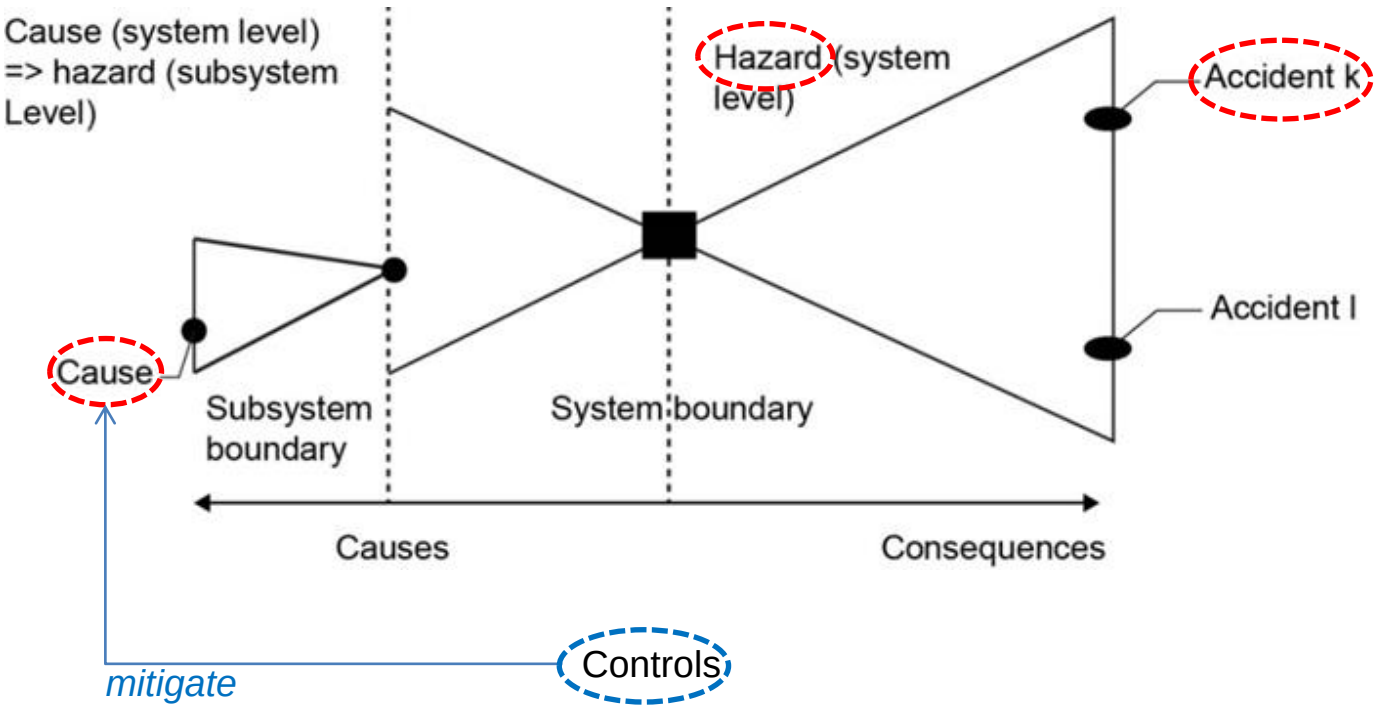
‘V’ System Life Cycle as per EN 50126-1



Generic Factors Influencing Railway RAMS

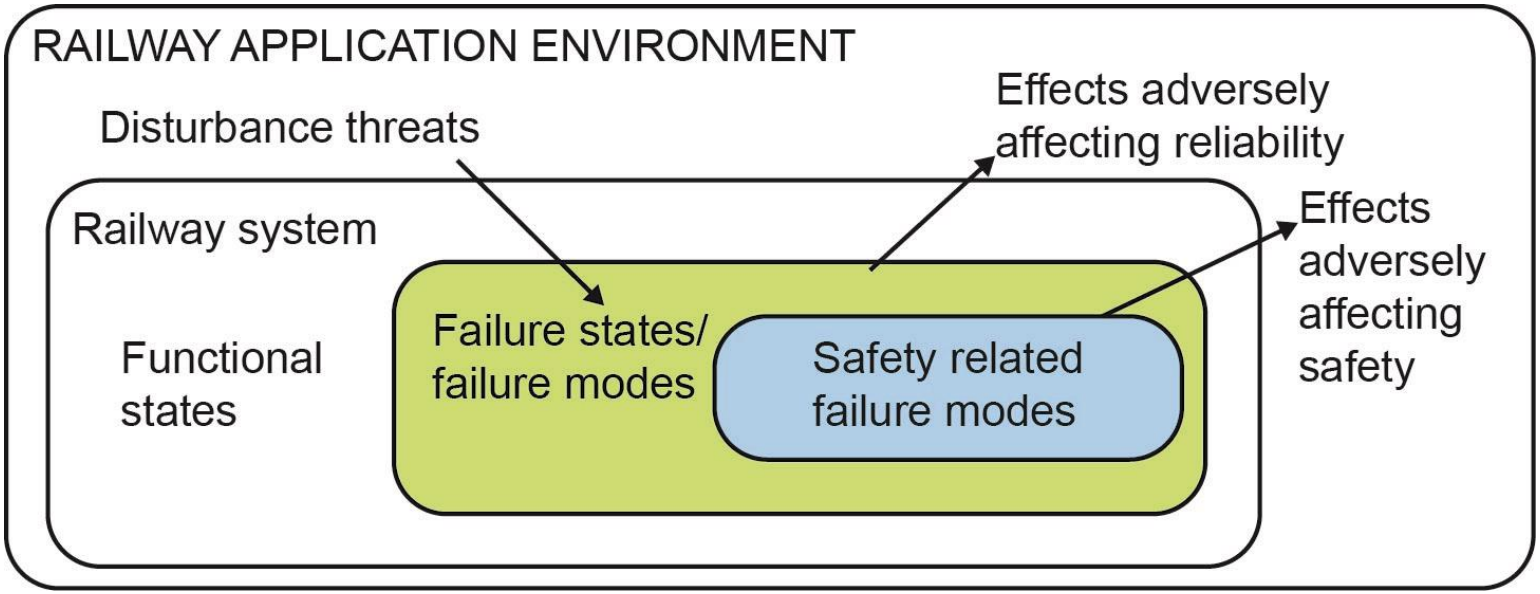


Elements of Railway RAMS



Railway System / System Context

Risk is a product of the system failure and the environment in which the system is operated and maintained



Risk

Risk is the combination of

- **The probability of occurrence** of an event or combination of events (hazard) leading to an accident, or the **frequency** of such occurrences
- The **consequence of the accident**

EN 50126 (Annex C) specifies

- *Typical* categories of probability/frequency of occurrence
- *Typical* hazard severity levels

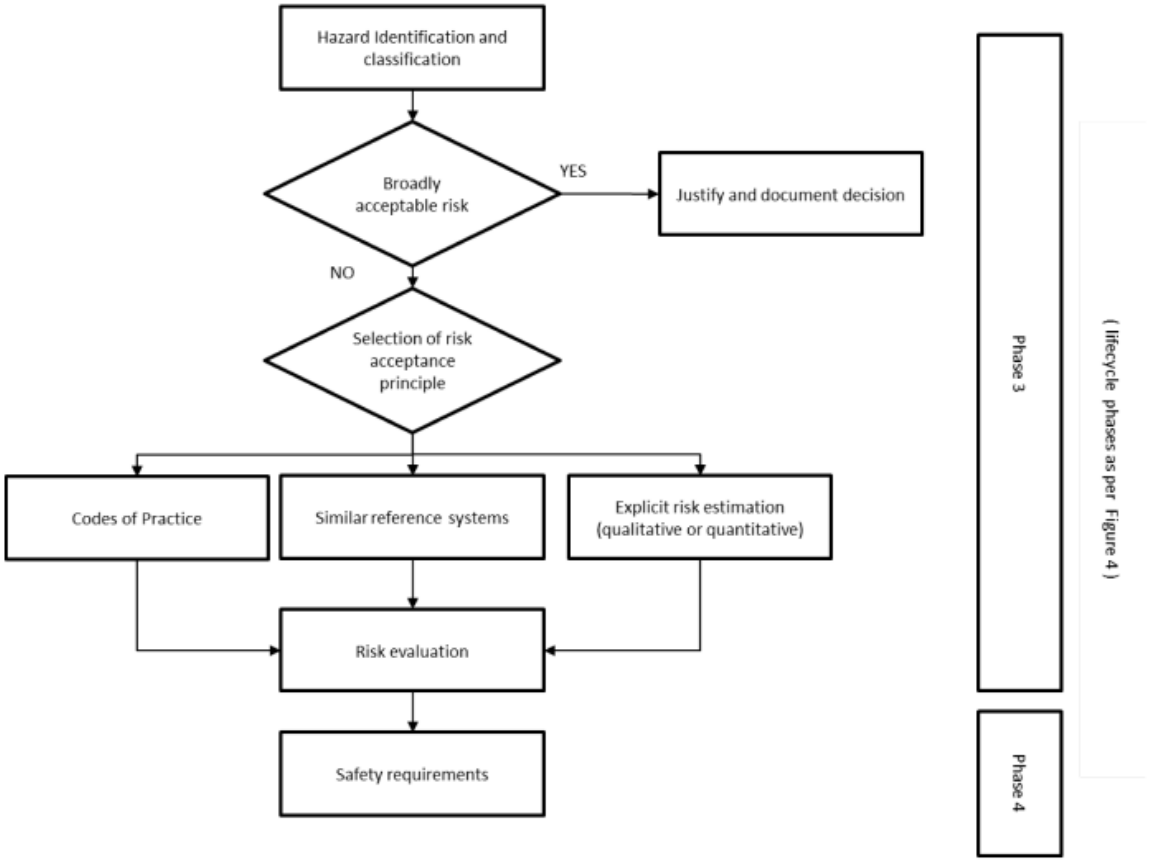
Definitions used are application dependent and defined by the Railway Authority

Hazard
A physical situation with a *potential* for human injury.

Risk
The probable rate of occurrence of a *hazard* causing harm and the degree of severity of the harm.

Choice of Risk Assessment Principle

Unless risk is broadly acceptable, the Risk Acceptance Principle shall be selected – based on Common Safety Method approach



SFAIRP

The SFAIRP principle ensures, *So Far As Is Reasonably Practicable*, that a System is safe if it is used for a purpose for which it was designed, commissioned, manufactured, supplied, installed or erected

Some of the general approaches used to demonstrate SFAIRP:

- Using a risk matrix to help identify acceptable risks, in terms of reference systems and/or codes of practice
- Using quantified risk estimates and SIL/THR to show that further risk reduction efforts will have no impact
- Considering the available further risk reduction options in terms of impact on risk and cost
- Showing that cost is grossly disproportionate to the achieved risk reduction (e.g. by reference to Value of Statistical Life)
- A cost benefit analysis is normally only used where margins are small

Tolerable Safety Risk of a Railway System

The tolerable safety risk of a railway system for any Railway Authority is dependent upon the safety criteria set by:

- the national Safety Regulatory Authority, or
- the Railway Authority itself in agreement with the Safety Regulatory Authority.

The primary responsibility for assessing, controlling and minimising risk rests with the Railway Authority.

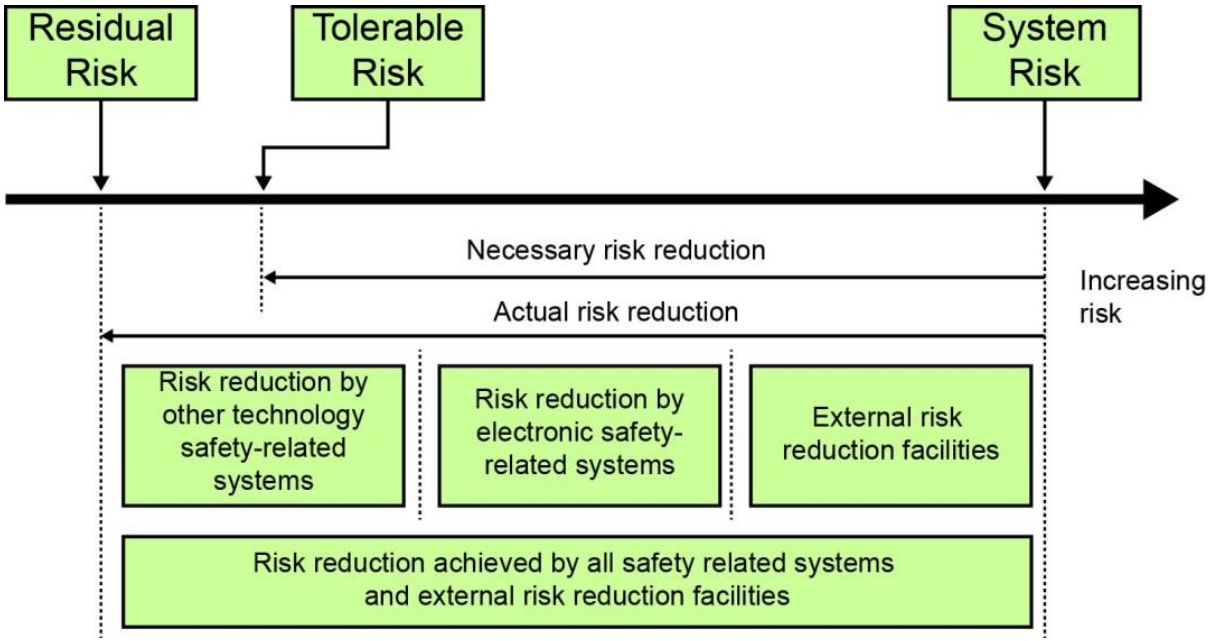
In some cases, legislation requires the formal presentation of evidence to demonstrate the adequacy of system safety

Risk acceptance should be based on a generally accepted principle

- E.g. Code of Practice, Reference System, SFAIRP etc

ONRSR guidelines for Major Projects suggests that major projects shall document the upper limit for individual or collective risks of equivalent fatality

Risk Reduction

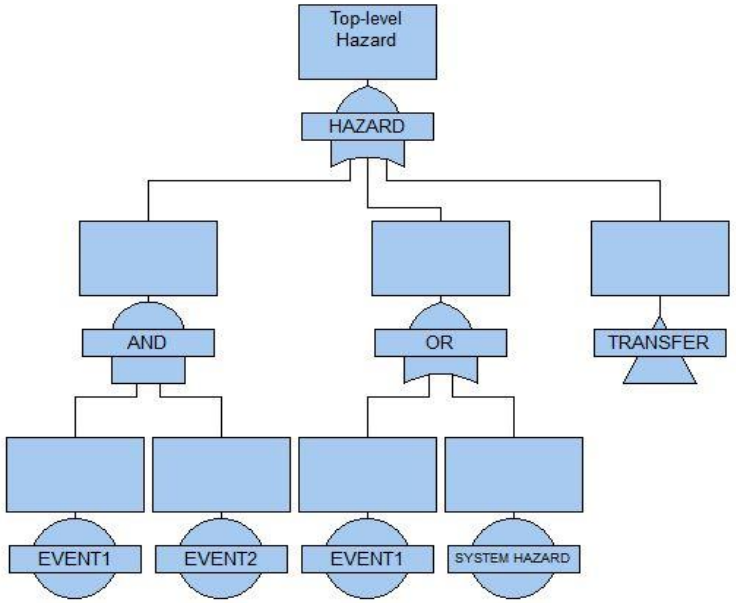


Assigning Safety Targets

Can be modelled using Fault Trees

Based on tolerability criteria

May assign Safety Integrity requirements (quantitative THR targets and/or qualitative SIL targets)



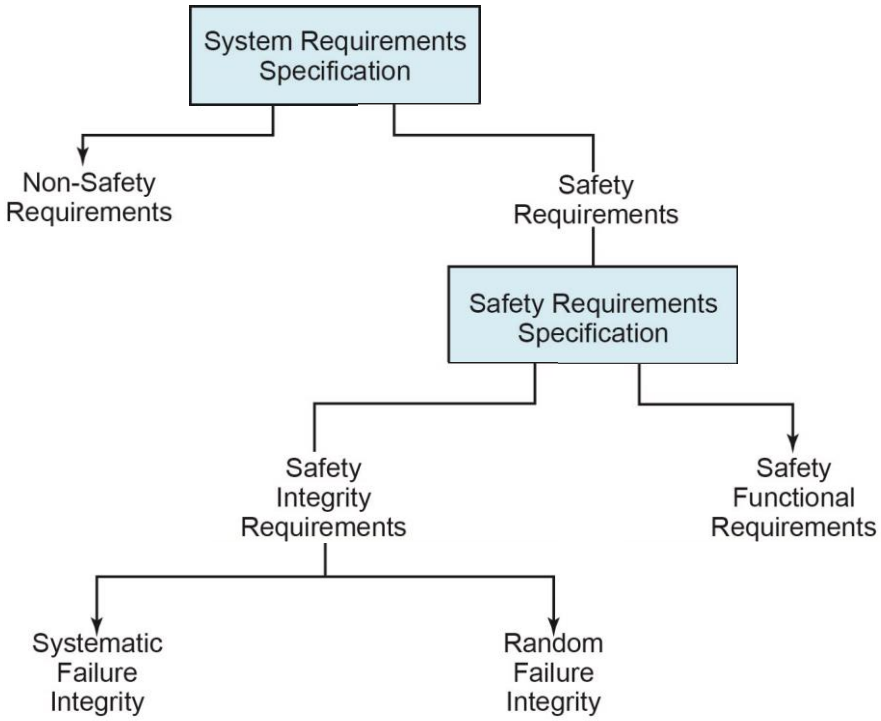
Safety Integrity

Safety integrity relates to the ability of a safety-related system to reliably achieve its required safety functions

The higher the safety integrity, the higher the likelihood that it will carry out the required safety functions.

Safety integrity consists of two parts:

- Systematic failure integrity
- Random failure integrity



Determining SIL Requirements – Process Overview

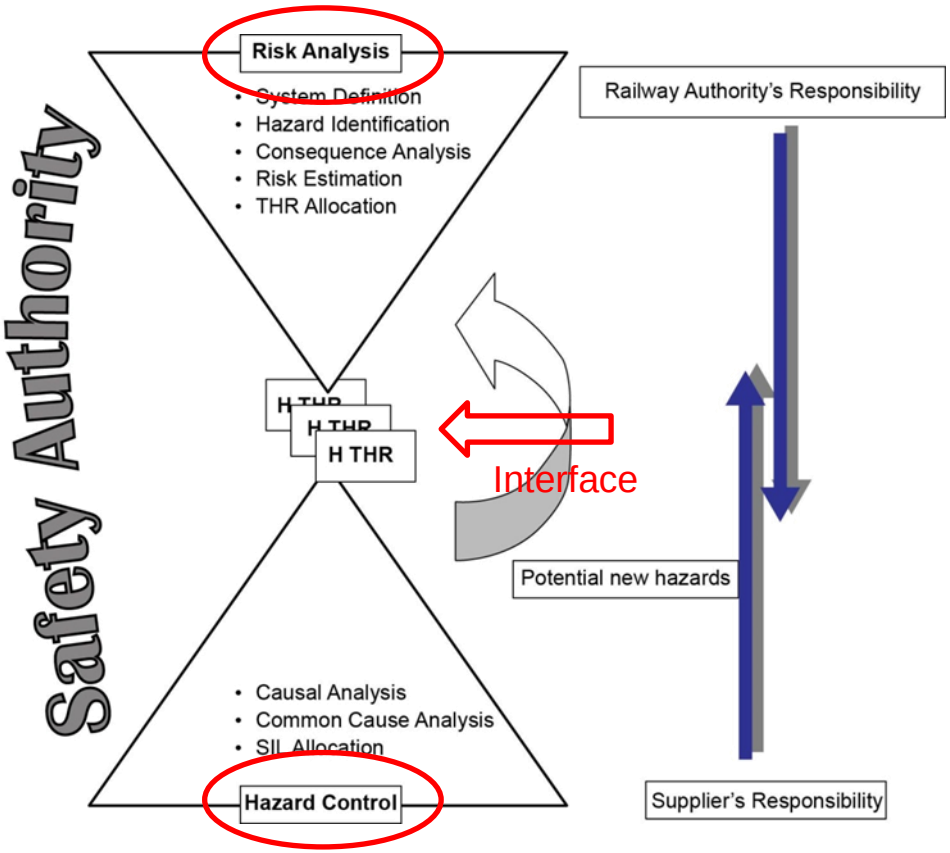
Requires a well defined interface between the operational environment and the system:

- list of hazards
- associated tolerable hazard rates

The Risk Analysis produces tolerable hazard rates which are the input to Hazard Controls

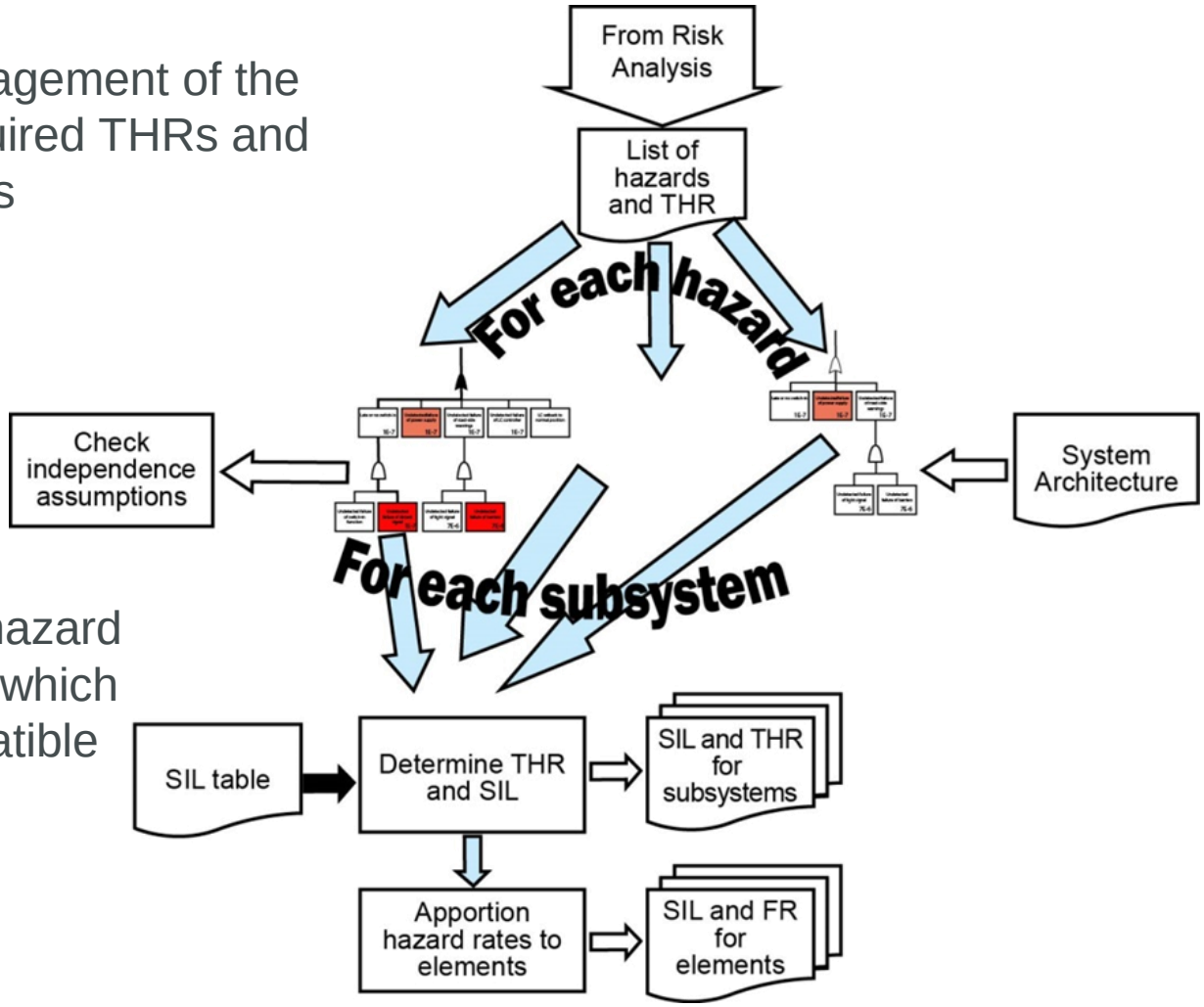
Analysis proceeds

- **bottom-up** - identification of possible consequences of failures and related risks; and
- **top-down** identification of the causes of the hazards.



Process of Hazard Control

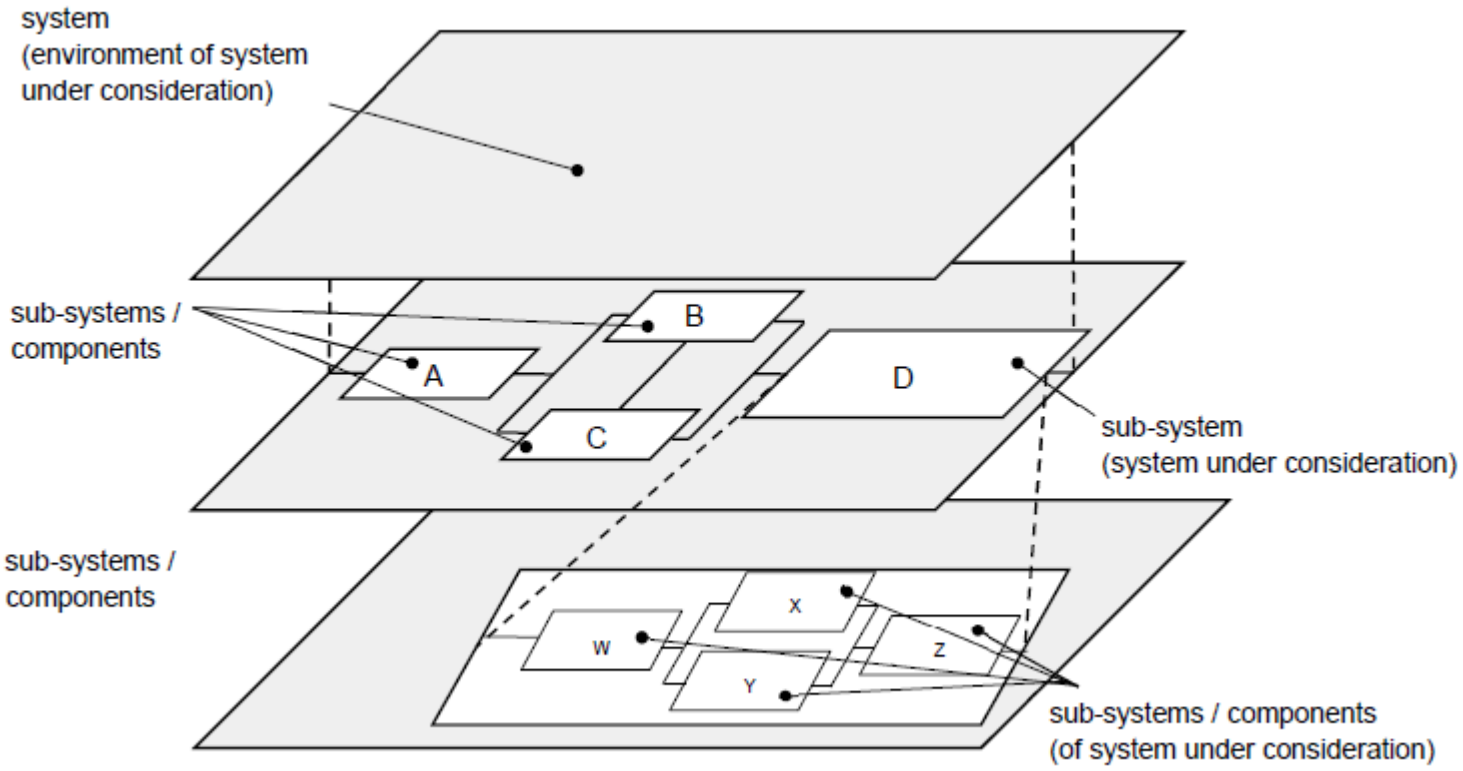
Hazard control is the management of the implementation of the required THRs and associated safety functions



The supplier controls the hazard so that the frequency with which they may present is compatible with agreed THR

Railway System / System Context

The System is defined hierarchically, at overall System level in terms of the context in which it operates, and then at subsequent levels of decomposition



Lean CENELEC

Bring the operator-supplier discussion on Safety Targets into the foreground

Raise potential disconnects regarding targets early

- Operator assumptions regarding process
- Supplier capability to mitigate hazards and/or to manage the required Safety Integrity
- Potential Supplier application conditions

Early identification of issues reduces deviation from supplier product and later rework of System function

Conclusions

Four key contributions:

- The customer is active in the translation of railway-level targets to focus on the system that is being developed by the supplier;
- The customer is involved early in the development lifecycle, to begin analysis of the operational impact of the system;
- The supplier engages with the customer to ensure that the system that is built will meet the provided targets;
- The delineation of abstraction levels for customer and supplier helps to ensure that each party remains focused on the problems that are most pertinent to their tasks in the development of the system.

From a Lean perspective:

Mismatches between Operator objectives and supplier activities are identified early in the lifecycle

Collaboration between the Operator and Supplier for definition of the System Hazards enables efficient utilisation of both teams, with minimal rework