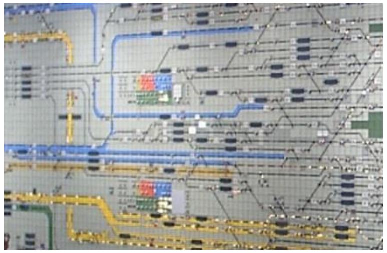
Safety Requirement Specification

An Overview of the Safety Requirement Specification Process in IEC 61508

Standards for Safety-Related Systems

Domain	Certification	Development process	Safety Analysis/ Assessment
Generic		IEEE-12207	IEC-61508
	CMMI		
Process			IEC-61511
Vehicle		ISO-26262	
Aircraft	DO-178C, DO-278A, DO-333		
Railway			IEC-50126
		IEC-50128, IEC-50129	
Space	ECSS		



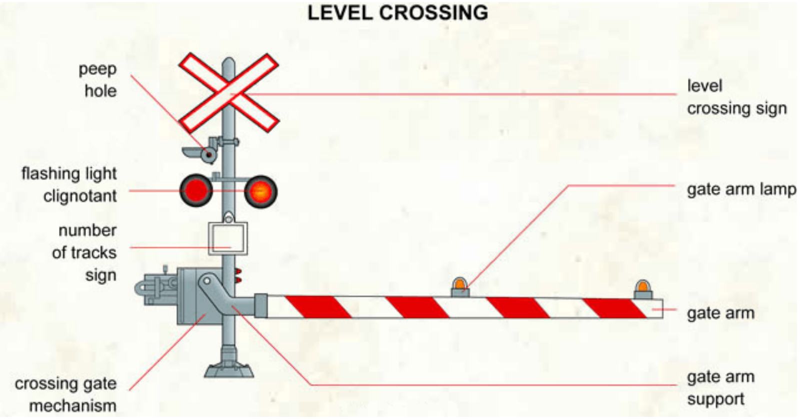
Functional Safety

Consider for example a level crossing:

- typically movable barriers which, when raised, allow road traffic across the rails,
- when lowered, act as a barrier to passage of road vehicles.

IEC 61508 concerns the functional safety aspects of this system.

- Functional safety aspects of this system would concern, e.g., the operation of the barriers and lights:
  - Is it possible for the barriers to remain raised when a train approaches?
  - Do the lights and bells always operate when a train approaches?
  - Are the barriers always visible to road traffic when lowered?
- Non-functional safety aspects might concern, e.g., the toxicity of materials used in the construction.



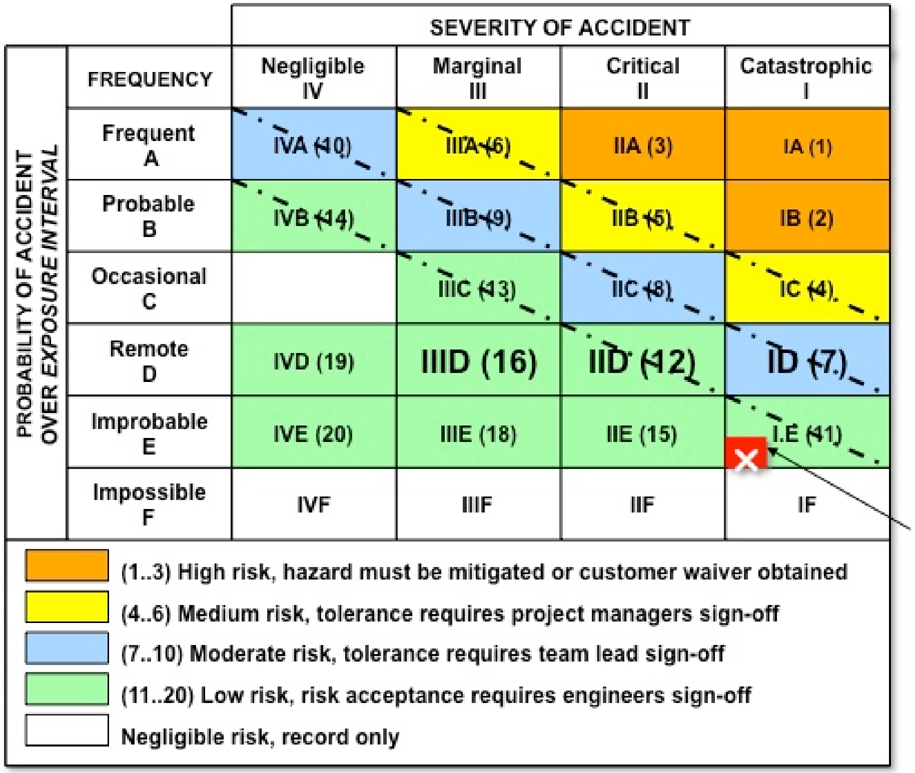
Risk

In 1711 Abraham De Moivre came up with the mathematical definition of risk as:

- The Risk of losing any sum is the reverse of Expectation; and the true measure of it is, the product of the Sum adventured multiplied by the Probability of the Loss.

  Abraham de Moivre, *De Mensura Sortis*, 1711 in the Ph. Trans. of the Royal Society

In a risk matrix each cell notionally represents a point on the iso-risk curve and steps in the matrix define the edges of 'risk zones'. We also usually plot the curve using log/log axes which provide straight line contours.



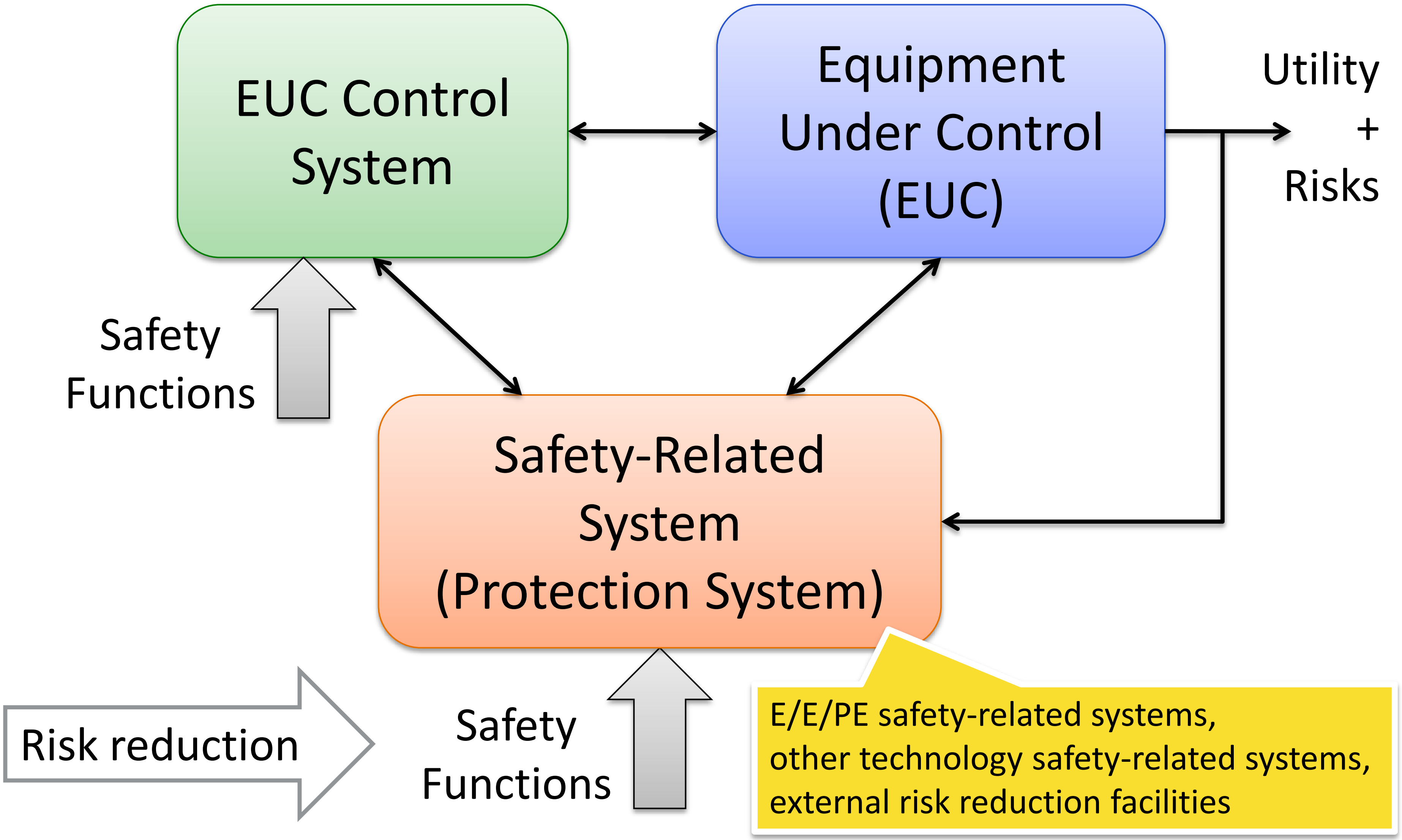
		SEVERITY OF ACCIDENT			
	FREQUENCY	Negligible IV	Marginal III	Critical II	Catastrophic I
PROBABILITY OF ACCIDENT OVER EXPOSURE INTERVAL	Frequent A	IVA (10)	IIIA (6)	IIA (3)	IA (1)
	Probable B	IVB (14)	IIIB (9)	IIB (5)	IB (2)
	Occasional C		IIIC (13)	IIC (8)	IC (4)
	Remote D	IVD (19)	IIID (16)	IID (12)	ID (7)
	Improbable E	IVE (20)	IIIE (18)	IIE (15)	I.E (11)
	Impossible F	IVF	IIIF	IIF	IF

🟧	(1..3) High risk, hazard must be mitigated or customer waiver obtained
🟨	(4..6) Medium risk, tolerance requires project managers sign-off
🟦	(7..10) Moderate risk, tolerance requires team lead sign-off
🟩	(11..20) Low risk, risk acceptance requires engineers sign-off
⬜	Negligible risk, record only

Functional Safety Concept: Risk

- Risk based approach for determining the target failure measure
  - Risk is a measure of the probability and consequence of a specified hazardous event occurring
  - There is no such thing as „Zero Risk“
- A safety-related system both
  - implements the required safety functions necessary to
    - achieve a safe state for the EUC or
    - to maintain a safe state for the EUC
  - is intended to achieve the necessary safety integrity for the required safety functions

Model of Risk Reduction



EUC Control System

Equipment Under Control (EUC)

Utility + Risks

Safety Functions

Safety-Related System (Protection System)

Risk reduction

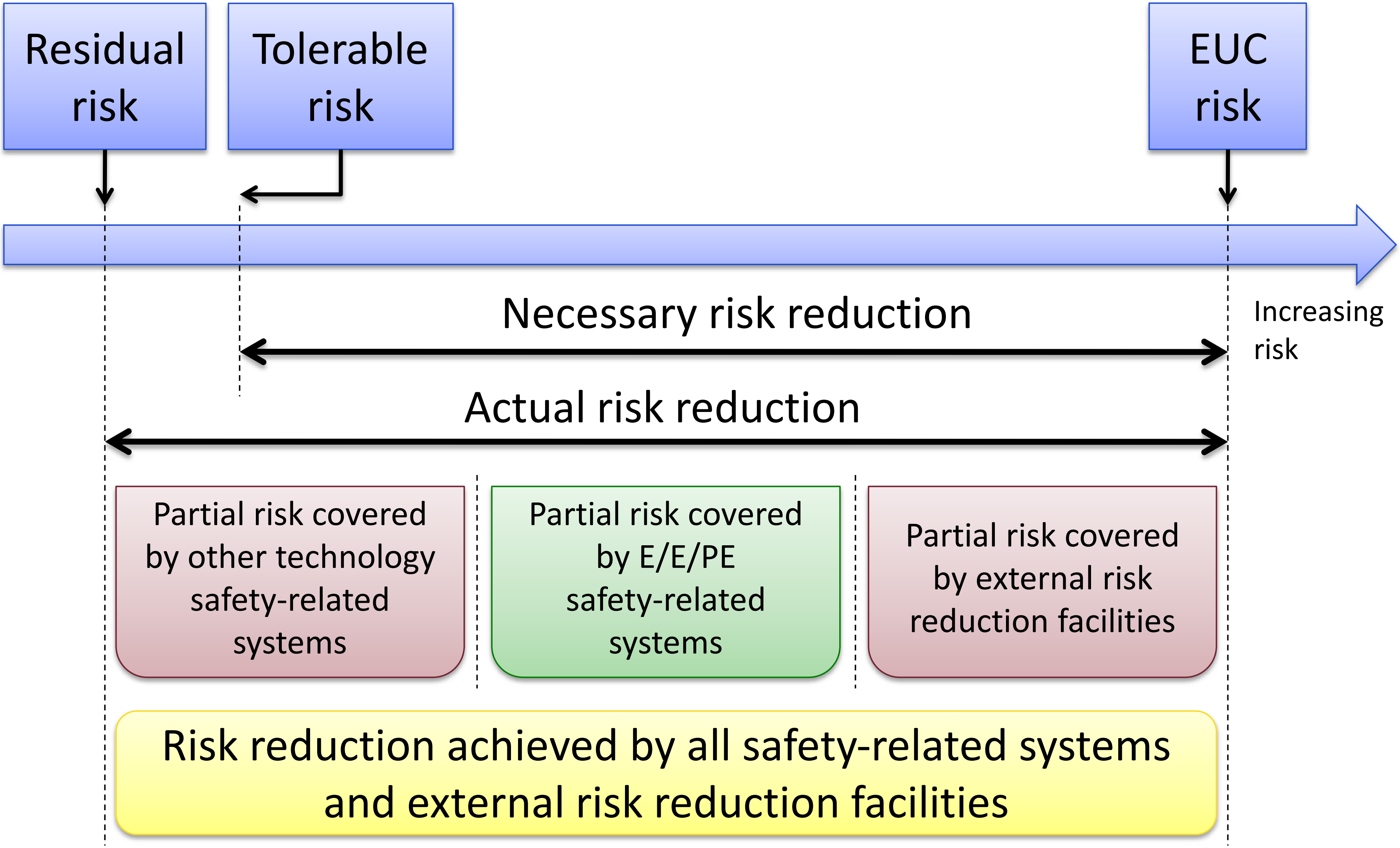
Safety Functions

E/E/PE safety-related systems,
other technology safety-related systems,
external risk reduction facilities

Functional Safety Concept: Risk Reduction

- The Safety Functions (SF) are concerned with risk reduction
  - There is EUC risk: risk arising from the EUC or its interaction with the EUC control system [EUCCS]
  - There is a tolerable risk (socially derived)
  - There is a residual risk: risk remaining after protective measures have been taken
- Developers must assess
  - the EUC risk and the tolerable risk to calculate the required safety integrity level (SIL)
  - the residual risk, which must be as low as reasonably practicable (ALARP)

Determining the Necessary Risk Reduction


Residual risk
Tolerable risk
EUC risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other technology safety-related systems
Partial risk covered by E/E/PE safety-related systems
Partial risk covered by external risk reduction facilities
Risk reduction achieved by all safety-related systems and external risk reduction facilities

Is Airbag Deployment a Safety Function?

- Safety function:
  - is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event
  - is concerned with risk reduction
- Airbag deployment
  - Does not return the EUC to a safe state
  - But reduces harm → reduces risk
  - Risk reduction properties:
    - does not reduce the likelihood (frequency) of any hazardous events that are collisions
    - but reduces the severity (consequences) of those events

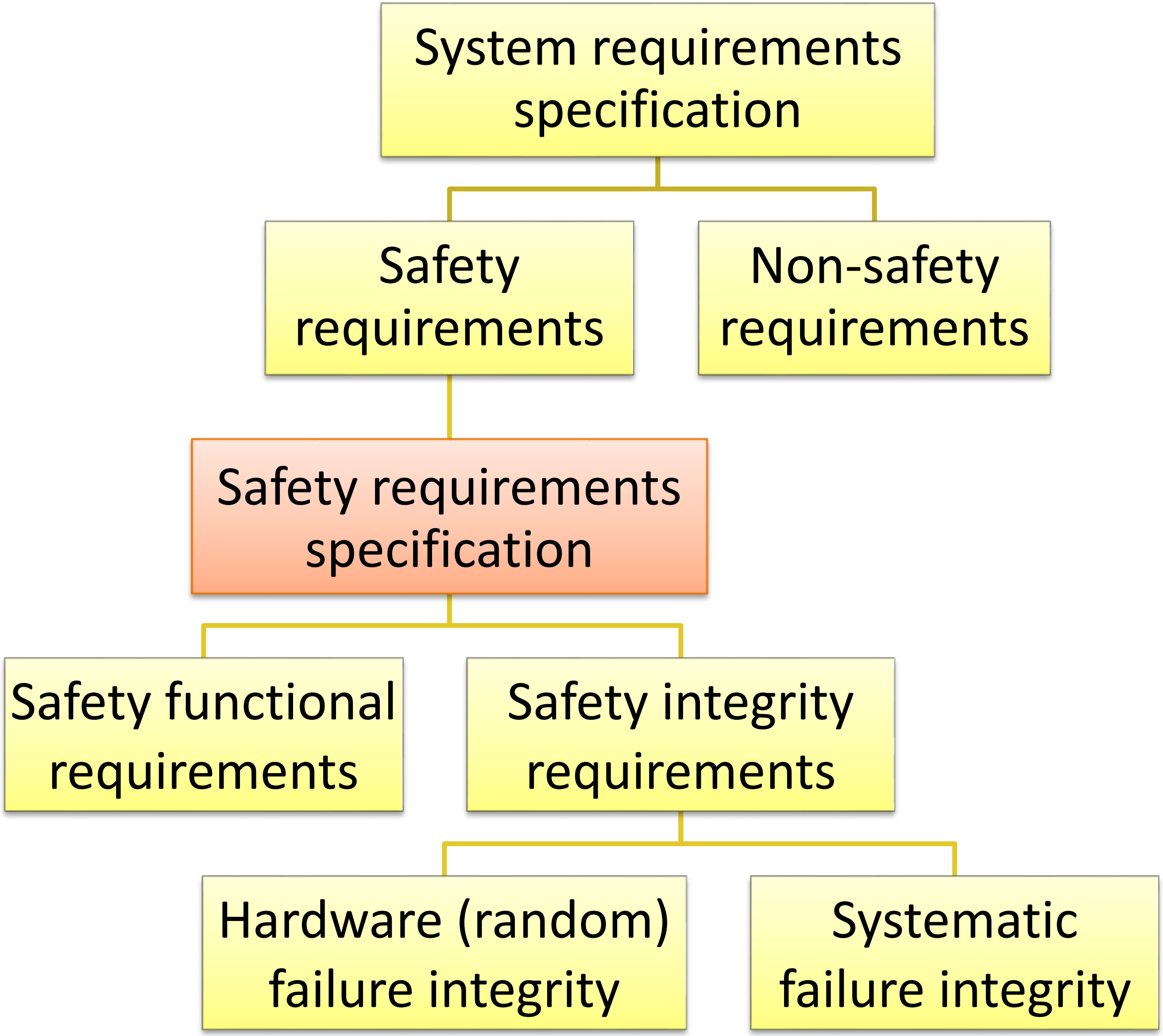
Is the ABS a Safety-Related System?

- Consider an anti-lock braking system, an ABS
  - the EUC is the brakes
  - the EUCCS is the brake activation mechanism, from pedal to brake pads
  - ~~the SRS is the wheel-rotation sensors and the responsive brake-release-and-reapply mechanism~~
- Functional safety assessment:
  - the EUC risk is known, similarly the tolerable risk
  - the required risk reduction can be calculated
  - this requirement can be transformed into a SIL
- Then it can be demonstrated that the ABS fulfils the SIL
- But the ABS is not designated as an SRS (which must always be active) but rather as a functional enhancement which is not formally safety-related

Safety Requirements

- Requirements for a safety-related system:
  - Safety function requirements
    - Derived from hazard identification
  - Safety integrity requirements
    - Relates to the target failure measure of the safety function
    - Derived from risk assessment
- The required safety integrity of the safety-related systems, must be of such a level so as to ensure that
  - the failure frequency of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk, and/or
  - the safety-related systems modify the consequences of failure to the extent required to meet the tolerable risk

Structure of Requirements



System requirements specification

Safety requirements

Non-safety requirements

Safety requirements specification

Safety functional requirements

Safety integrity requirements

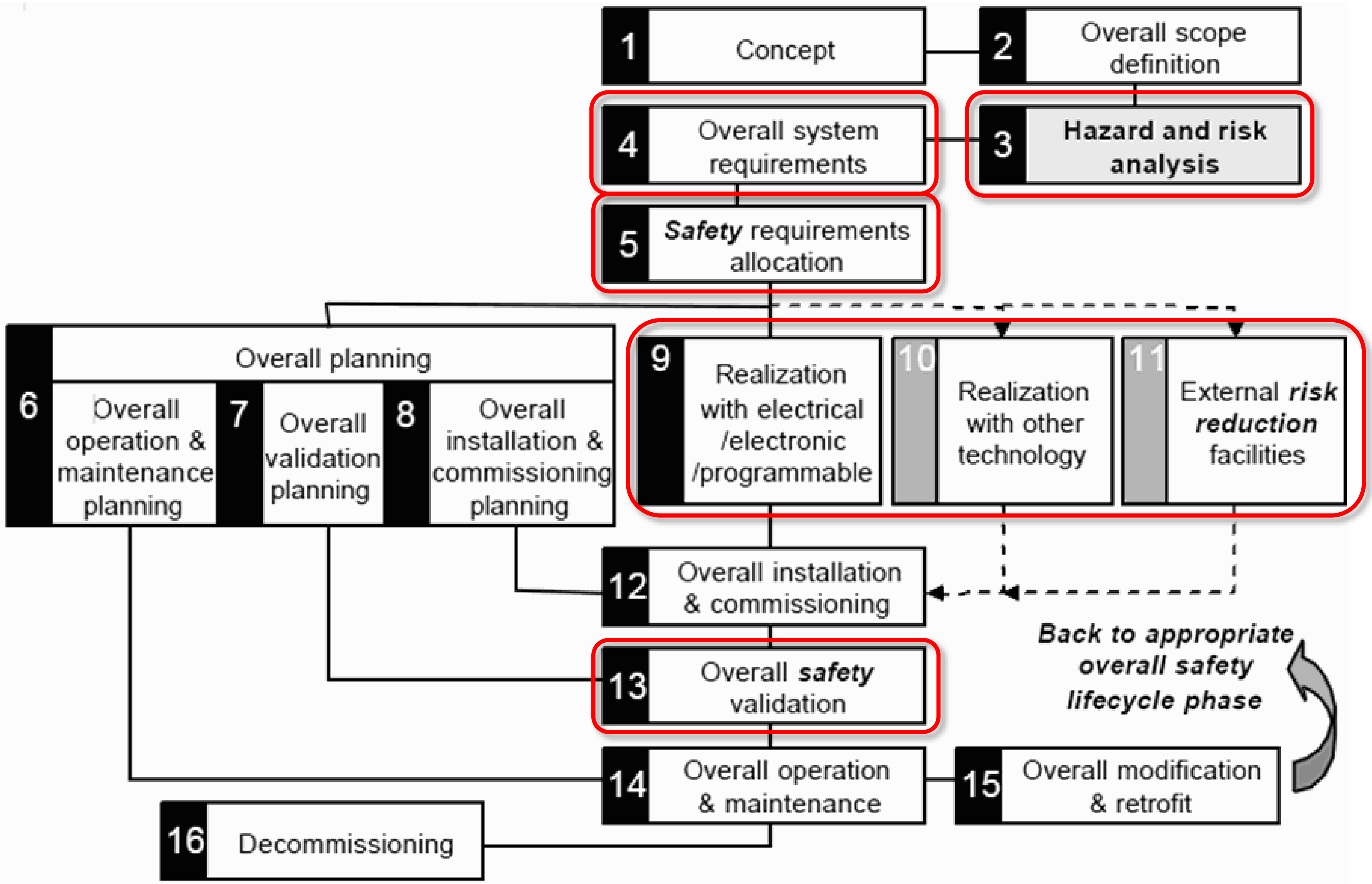
Hardware (random) failure integrity

Systematic failure integrity

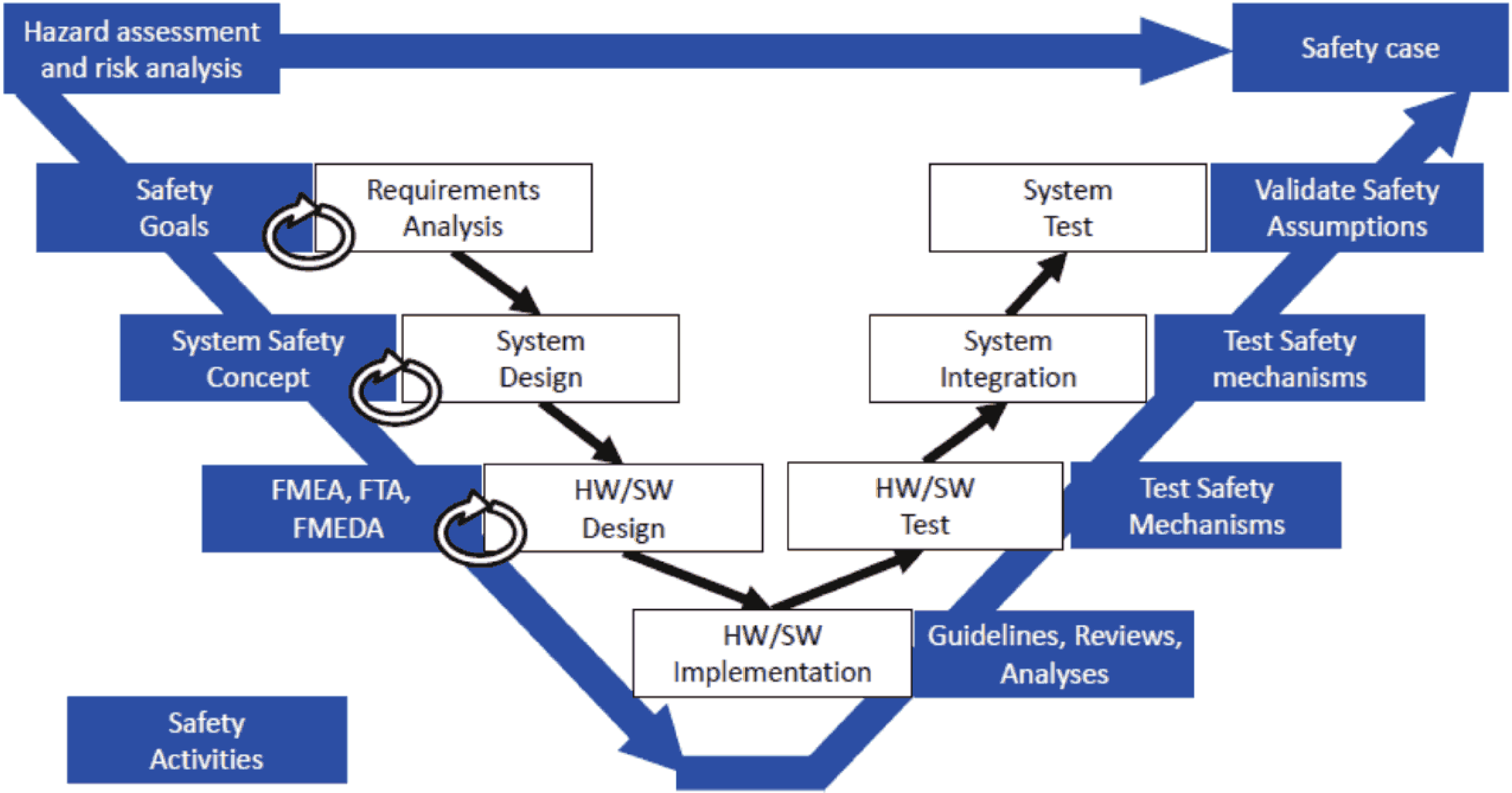
Development of Safety Functions

- The development of safety functions requires the following steps:
  - Identify and analyze the risks
  - Determine the tolerability of each risk
  - Determine the risk reduction necessary for each intolerable risk
  - Specify the safety requirements for each risk reduction, including their safety integrity levels (SILs)
  - Design safety functions to meet the safety requirements
  - Implement the safety functions
  - Validate the safety functions

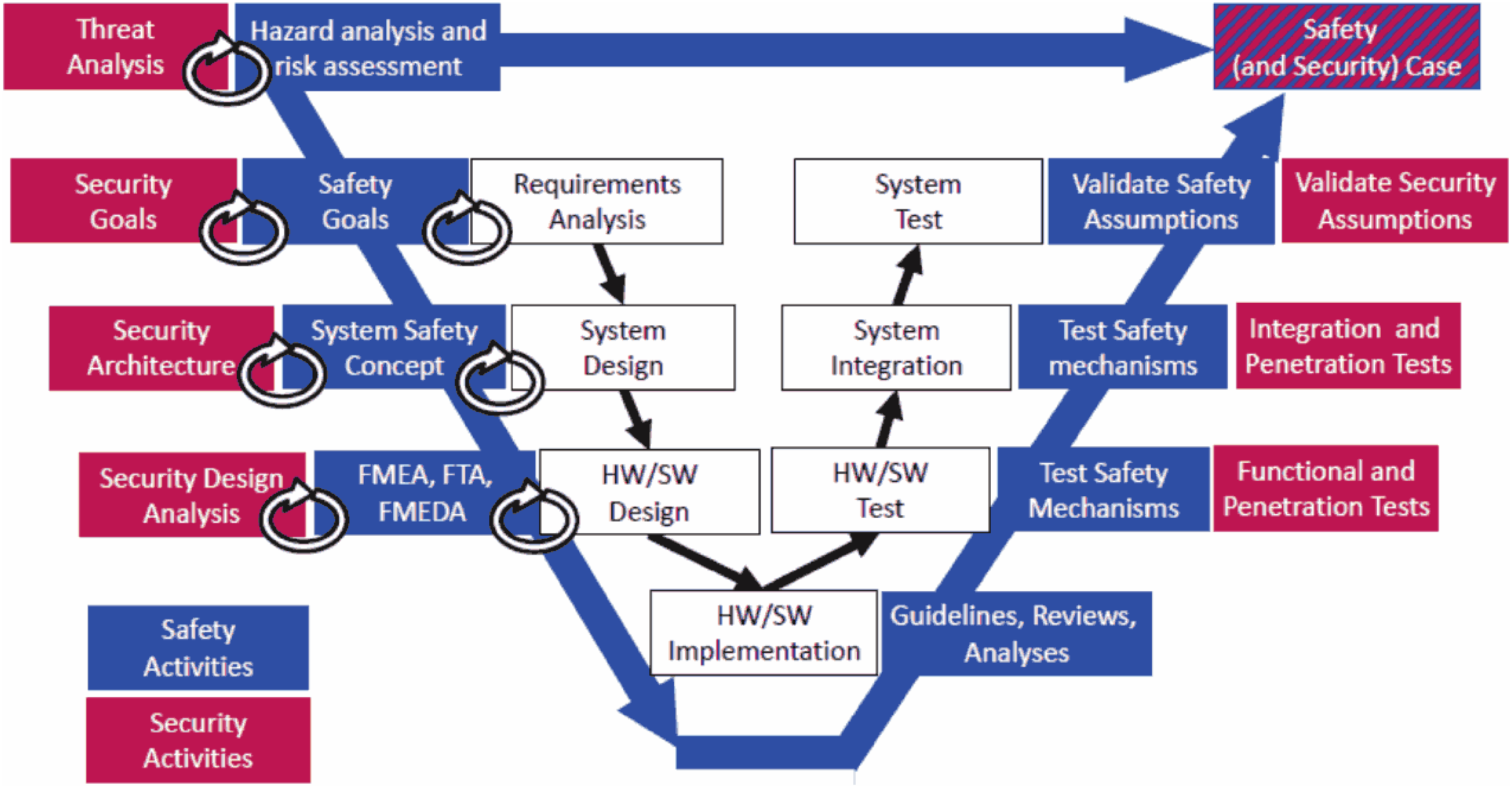
Life Cycle Activities Related to Safety Functions


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall system requirements
5 Safety requirements allocation
6 Overall planning
6 Overall operation & maintenance planning
7 Overall validation planning
8 Overall installation & commissioning planning
9 Realization with electrical /electronic /programmable
10 Realization with other technology
11 External risk reduction facilities
12 Overall installation & commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation & maintenance
15 Overall modification & retrofit
16 Decommissioning

Functional Safety Development Life-Cycle



Functional Safety = Safety + Security



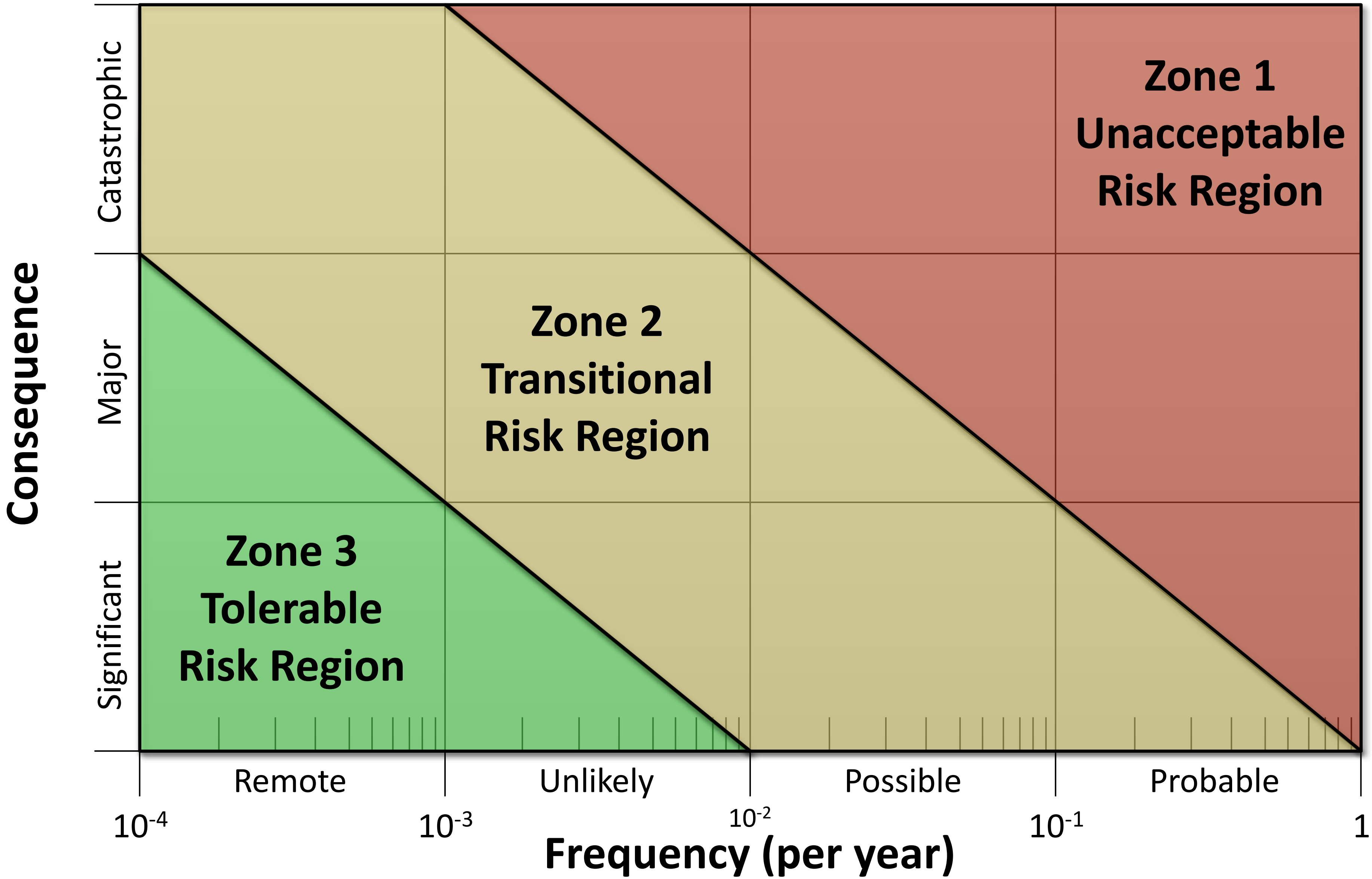
The Risk Assessment Framework

- The three main stages of Risk Assessment are:
  1. Establish the tolerable risk criteria with respect to
     - the frequency (or probability) of the hazardous event
     - and its specific consequences
  2. Assess the risks associated with the equipment under control
  3. Determine the necessary risk reduction needed to meet the risk acceptance criteria
     - this will determine the Safety Integrity Level of the safety-related systems and external risk reduction facilities

Tolerable Risk Criteria

- Qualitative criteria use words
  - such as probable, frequent, unlikely, remote, etc. to describe the likelihood of the hazardous event, and
  - such as minor, major, catastrophic, etc. to describe the consequences
  - it is often necessary to introduce quantitative numbers to provide a clear definition of how to interpret these words
- Quantitative criteria use numbers to describe the likelihood and severity of the event
  - This can include criteria such as an event having a frequency of less than 10^{-3} per year, or between 2 and 5 fatalities or serious injuries, etc.

Example Risk Bands for Tolerability of Hazards



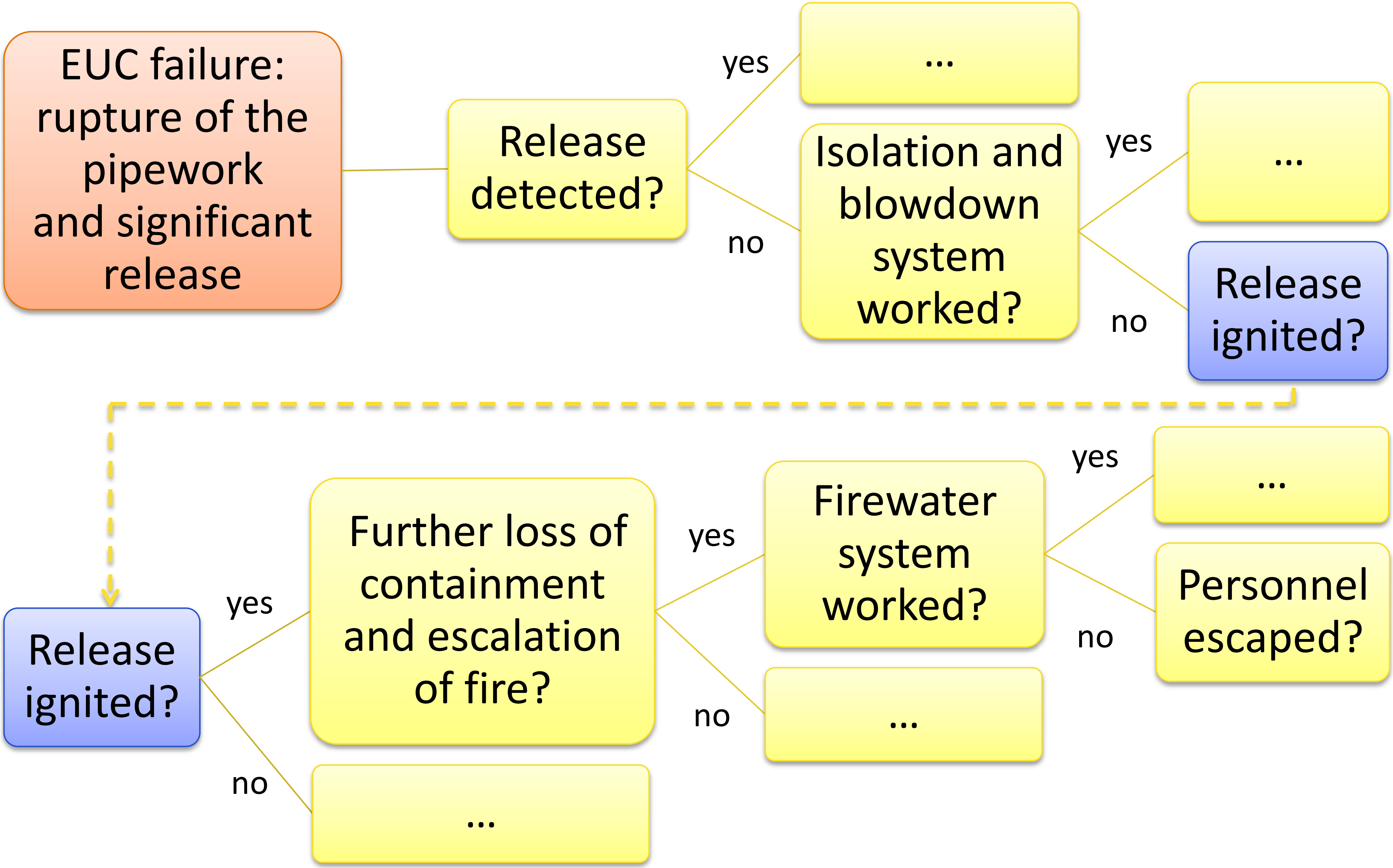
Assessing the Frequency of Hazardous Event

- The risk assessment can be summarized as asking:
  - How likely is the equipment under control to fail?
  - If it does fail, what is the outcome?
- The likelihood or frequency of an event relating to the EUC is determined by
  - Intrinsic causes such as component failures, software failures, or human error within the EUC
  - Extrinsic demand (mode of operation): e.g. safety systems
    - only need to function when some failure within the plant occurs
- Therefore, the assessment must consider both the intrinsic failure rate and the extrinsic demand rate of the equipment under control.

Assessing the Consequence of Hazardous Event

- The consequences of an event relating to EUC
  - can range from the direct effects
  - to all subsequent events along the escalation path
- This introduces a dilemma, since
  - the true consequences of an event can only be determined if the escalation path is assessed through to the end conclusions
  - however, the escalation path itself may contain other separate functions that are themselves subject to FSA

Example: Over-Pressurization Protection System



EUC failure: rupture of the pipework and significant release

Release detected?

yes

…

no

Isolation and blowdown system worked?

yes

…

no

Release ignited?

Release ignited?

yes

Further loss of containment and escalation of fire?

yes

Firewater system worked?

yes

…

no

Personnel escaped?

no

…

no

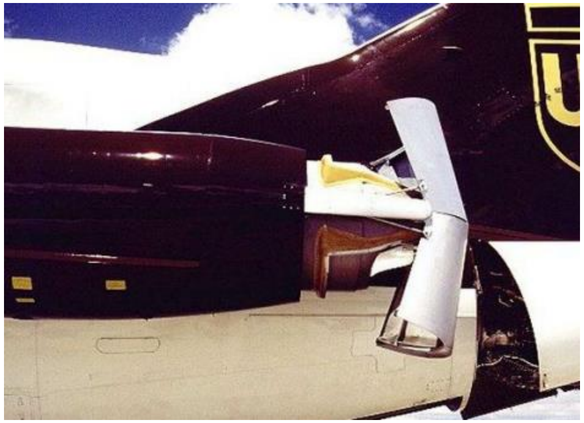
…

Issues with FSA (IEC 61508 gives no guidance)

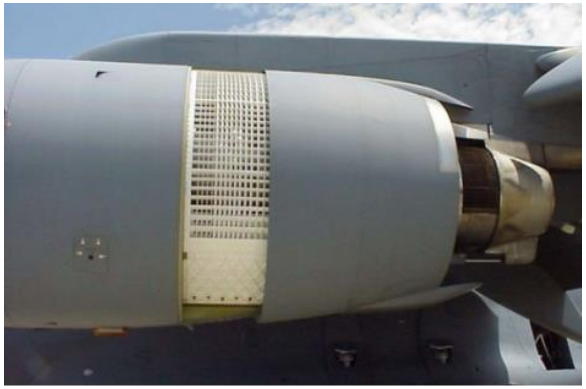
- In order to accurately determine the EUC risk, the boundary of the analysis has to extend to the end of the event tree
  - However, if the boundary is extended cover every potential path within the event tree, the analysis will include
    - systems not directly affected by the EUC
    - which themselves may be subject to FSA
- Another important issue is that the overall safety performance could be improved by achieving a high availability for any element in the escalation path
  - such as gas detection; isolation and blowdown; protection against ignition; prevention of escalation to adjacent plant; the firewater system; etc. in the previous example

Example: Thrust Reverser Interlock

- Thrust reverser deployment in flight almost inevitably leads to loss of control of the aircraft
  - Catastrophic event
- On the Boeing B767 aircraft, there is a hydromechanical interlock, which physically prevents the thrust reverse mechanism from operating
  - on “weight on wheels” or WoW criterion
- In May of 1991, a Lauda Air Boeing B767 crashed over Thailand
  - cause: deployment of the left engine thrust reverser in flight, leading to loss of control
  - previously unknown failure mode due to disintegration of the rubber-compound seals



Deployed clamshell thrust reverser

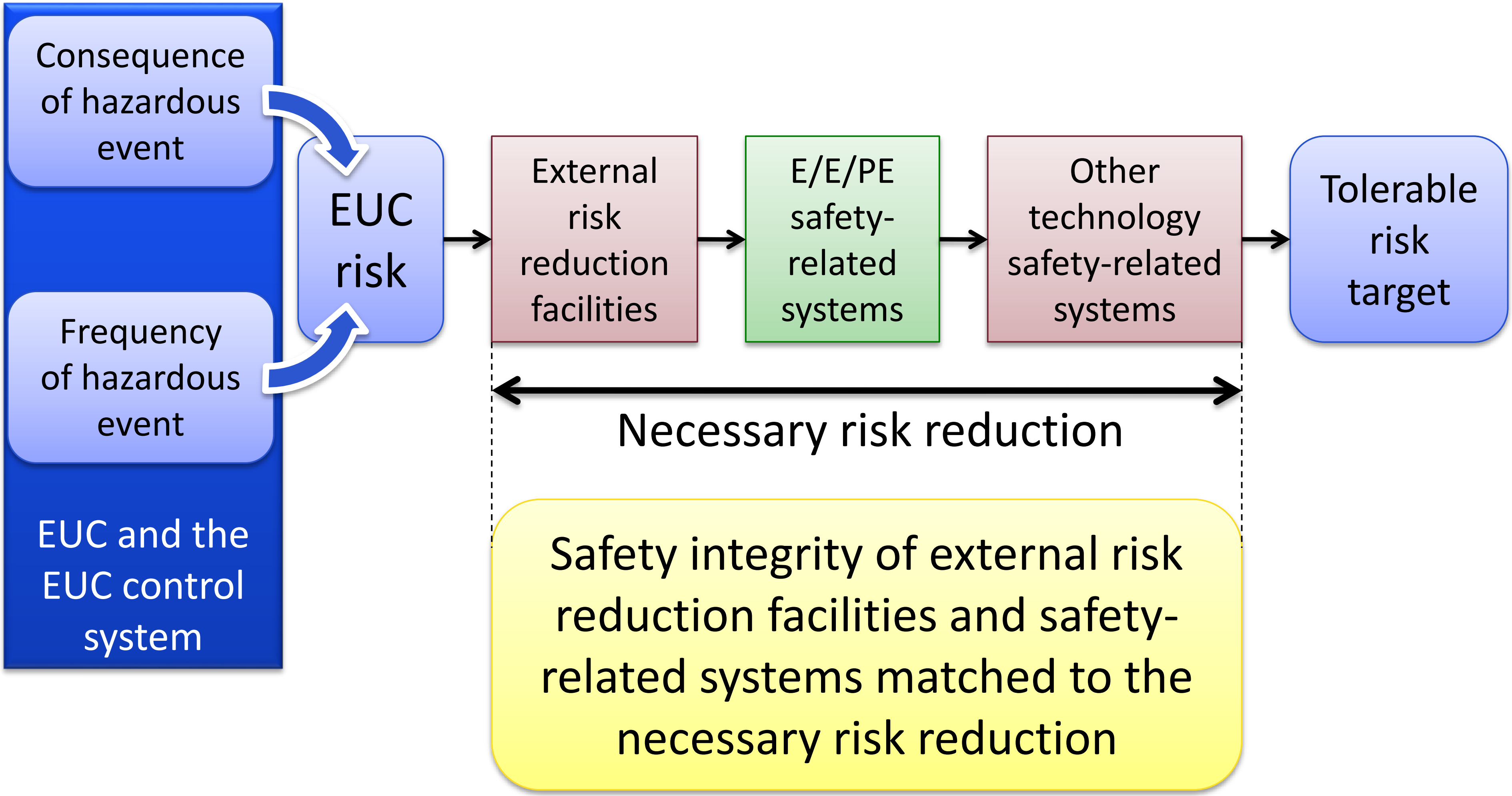


Deployed cascade reverser

Risk Reduction: Balancing the Options

- Example: anti-misting kerosene (AMK) aircraft fuel
  - idea was to inhibit ignition of the fuel in the case of an aircraft accident
- The fuel had different physical characteristics from the usual jet fuels
  - increased risk of engine problems during flight
- Let us suppose we have two hazards:
  - H1 is immediate, deadly conflagration of jet fuel in the case of a tank rupture
  - H2 is all engines cutting out in flight
- Suppose we eliminate hazard H1 (e.g. by introducing AMK into daily commercial flight operations), and thereby increase the risk associated with H2
  - How to reduce the joint risk as far as possible?

Risk and Safety Integrity Concepts



Consequence of hazardous event

Frequency of hazardous event

EUC and the EUC control system

EUC risk

External risk reduction facilities

E/E/PE safety-related systems

Other technology safety-related systems

Tolerable risk target

Necessary risk reduction

Safety integrity of external risk reduction facilities and safety-related systems matched to the necessary risk reduction

Risk Reduction

- The EUC risk shall be evaluated, or estimated, for each determined hazardous event
- Necessary risk reduction: risk reduction to be achieved by
  - E/E/PE safety-related systems
  - other technology safety-related systems and
  - external risk-reduction facilities

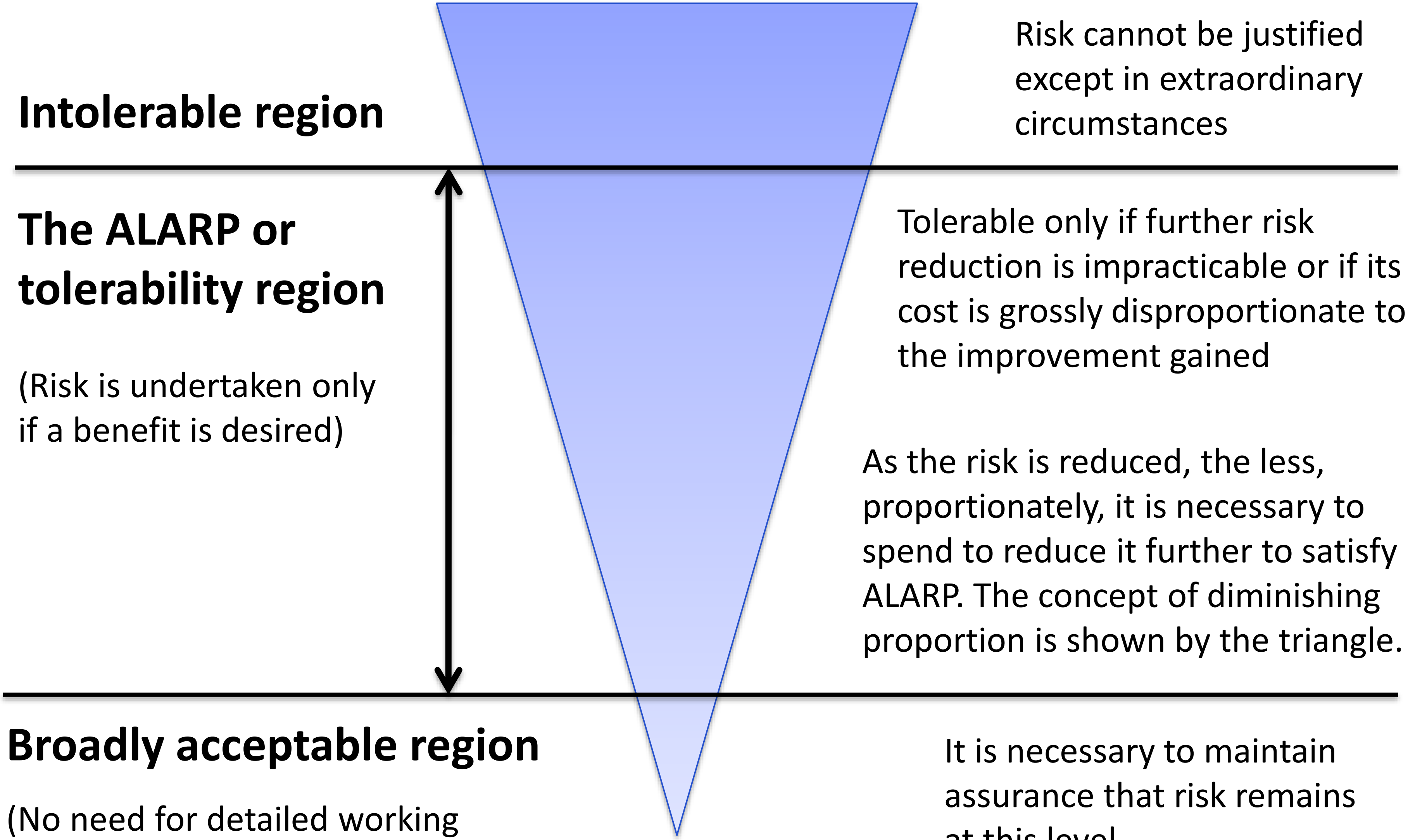
  in order to ensure that the tolerable risk is not exceeded
- The necessary risk reduction shall be determined for each determined hazardous event. May be determined in a
  - quantitative and/or
  - qualitative manner

The ALARP Principle

- The As Low As Reasonably Practicable (ALARP) principle must be used to calculate the required risk reduction
  - Origins: English law
    - Lord Asquith (1949)
    - Lord Cullen (1989)
      - Piper Alpha oil platform fire investigation

- Risks are classified as
  - Acceptable
    - so low that it can for all practical purposes be ignored
  - Intolerable
    - so high as to be unacceptable in all circumstances
  - The ALARP region
    - the region between acceptable and intolerable
    - in which the system developer is required to reduce the risk to be „as low as reasonably practicable“

Tolerable Risk and ALARP



Intolerable region

Risk cannot be justified except in extraordinary circumstances

The ALARP or tolerability region

(Risk is undertaken only if a benefit is desired)

Tolerable only if further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained

As the risk is reduced, the less, proportionately, it is necessary to spend to reduce it further to satisfy ALARP. The concept of diminishing proportion is shown by the triangle.

Broadly acceptable region

(No need for detailed working to demonstrate ALARP)

It is necessary to maintain assurance that risk remains at this level

Negligible risk

Example: Principles of Radiation Protection

- The principles of radiation protection are based on the recommendations of the International Commission on Radiological Protection (ICRP)
- Radiation use must fulfill three basic principles:
  - Principle of justification
    - The benefits of using radiation must outweigh the drawbacks
  - Principle of optimization
    - ALARA principle, As Low As Reasonably Achievable
    - Radiation exposure caused by the use of radiation must be kept as low as reasonably achievable
  - Principle of limitation
    - Exposure of radiation workers and individuals of public must not exceed dose limits

Taking the ALARP concept into consideration

The matching of a consequence with a tolerable frequency can be done through risk classes. Table on the next slide is an example showing four risk classes (I, II, III, IV) for a number of consequences and frequencies.

- The risks within these risk class definitions are the risks that are present when risk reduction measures have been put in place.
- The risk classes are as follows:
  - risk class I is in the unacceptable region;
  - risk classes II and III are in the ALARP region, risk class II being just inside the ALARP region;
  - risk class IV is in the broadly acceptable region.
- For each specific situation, or sector comparable industries, a similar table would be developed taking into account a wide range of social, political and economic factors.

Example of risk classification of accidents

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	II
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Risk class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
Class IV	Negligible risk

Safety Integrity Level (SIL)

- Each SRS is assigned a SIL
  - It expresses the Safety Integrity required from the SRS
  - SI is the probability that the SRS fulfils its safety function(s)
  - Represents objectively the reliability of its safety function(s)
  - Product requirement
- The SIL is assigned according to the required risk reduction
  - from EUC risk at least to the tolerable risk
- A quantitative difference is made between
  - Continuous-operation (high-demand) functions
  - Low-demand functions (also known as on-demand functions)
- Development of an SRS with a designated SIL requires a certain development process
  - Process requirement

Safety integrity level (SIL)

Safety integrity level (SIL)	**Low demand mode of operation** (Average probability of failure to perform its function on demand)	**High demand or continuous mode of op.** (Probability of a dangerous failure per hour / frequency of dangerous failures, or dangerous failure rate)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

It is important to note that the failure measures for safety integrity levels 1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgments have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity.

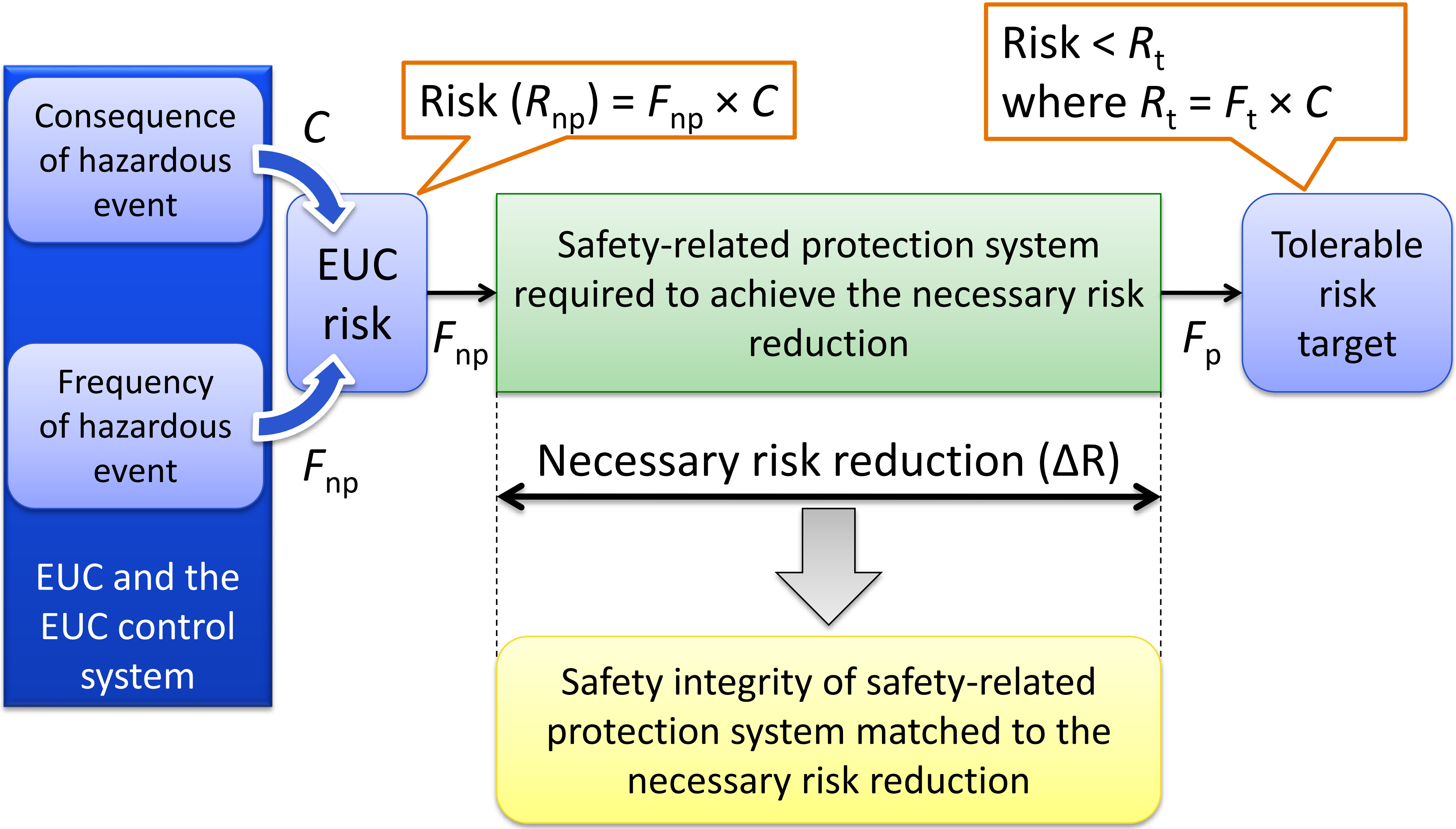
Example Methods to Determine the SIL

- Safety integrity levels are means of satisfying the safety integrity requirements of the safety functions allocated to the safety-related systems
- The methods used to allocate the safety integrity requirements depend upon whether the necessary risk reduction is specified
  - in a numerical manner (quantitative method) or
  - in a qualitative manner
    - Risk Graph Method
    - Hazardous Event Severity Matrix Method

Quantitative Method to Determine the SIL

- The key steps in the method are as follows:
  - determine the tolerable risk
    - from a table such as the ALARP tolerable risk frequencies
  - determine the EUC risk
  - determine the necessary risk reduction to meet the tolerable risk
  - allocate the necessary risk reduction to the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities
- These steps need to be done for each safety function to be implemented by the E/E/PE SRS

Safety Integrity Allocation



Risk $(R_{np}) = F_{np} \times C$

Risk $< R_t$
where $R_t = F_t \times C$

Consequence of hazardous event
C
Frequency of hazardous event
F_{np}
EUC and the EUC control system
EUC risk
F_{np}
Safety-related protection system required to achieve the necessary risk reduction
F_p
Tolerable risk target
Necessary risk reduction (ΔR)
Safety integrity of safety-related protection system matched to the necessary risk reduction

Example Calculation of Target Safety Integrity

A single safety-related protection system is used to achieve the necessary risk reduction:

$$PFD_{avg} \leq F_t \,/\, F_{np}$$

- PFD_{avg} is the average probability of failure on demand of the safety-related protection system
  - it is the safety integrity failure measure for safety-related protection systems in a low demand mode of operation
- F_t is the tolerable risk frequency
- F_{np} is the demand rate on the safety-related protection system
- C is the consequence of the hazardous event
- F_p is the risk frequency with protective features

Obtaining The Safety Integrity Level

- Determine the frequency (F_{np}) and consequence (C) elements of the EUC risk without any protective features
- Determine, by use of the ALARP tolerable risk frequencies table, whether for F_{np} and C the risk level is tolerable:
    - If this leads to Risk class I, then further risk reduction is required
    - Risk class II would require further investigation
    - Risk class IV or III would be tolerable risks
- Determine the probability of failure on demand for the SRS (PFD_{avg}) to meet the necessary risk reduction (ΔR):
    - for a constant consequence: $PFD_{avg} = (F_t / F_{np}) = \Delta R$
- The safety integrity level can be obtained from the SIL table
    - for example, if $PFD_{avg} = 10^{-2} – 10^{-3}$, the safety integrity level = 2

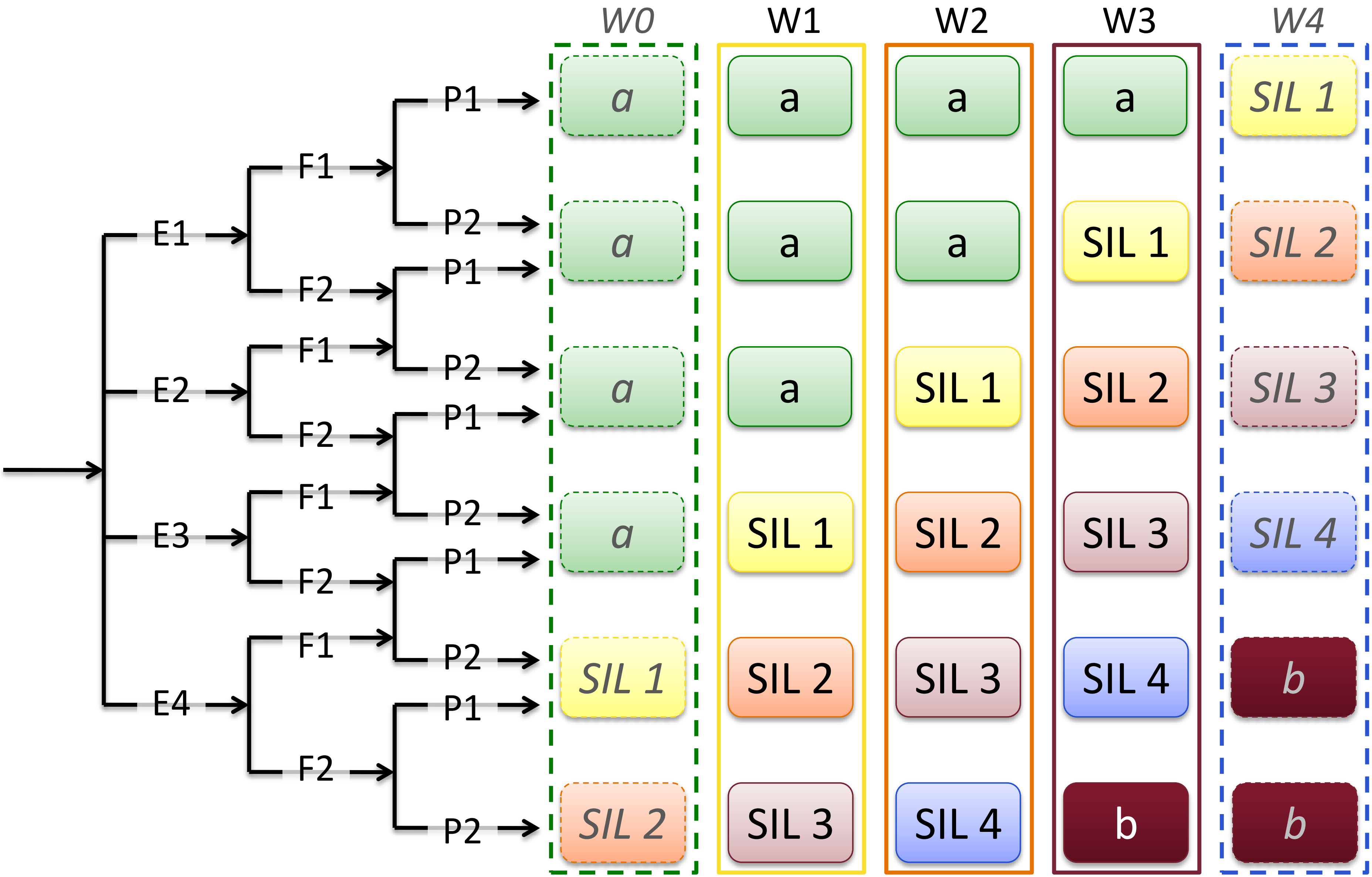
Example: Dead Man's Handle

- Driver's Safety Device
  - must be continually activated
  - may be a pedal or a lever
  - if released, emergency brakes are automatically applied (with some delay)
- In January 2003, near Waterfall, Australia, a train driver suffered a heart attack but the “dead man's brake” did not activate: the train derailed
  - Statistics on train drivers being incapacitated are known
  - Rail authorities set tolerable risk, or Target Levels of Safety
- The required risk reduction can be determined
  - Dead man's handle implements on-demand function which is triggered less than once a year, system-wide
  - The device can be designed to a SIL 2 or SIL 3 requirement

Risk Graph Implementation

- The (Extended) Risk Graph is a qualitative method
  - It can be considered as a decision tree approach
- Enables the SIL rating of a safety-related system to be determined from the risk factors associated with EUC
- The review team considers four risk parameters:
  - Consequence parameter (E1, E2, E3 and E4)
  - Frequency and exposure time parameter (F1 and F2)
  - Possibility of failing to avoid the hazard parameter (P1 and P2)
  - Probability of the unwanted occurrence parameter (W0, W1, W2, W3 and W4)

Example of Extended Risk Graph



W0	W1	W2	W3	*W4*
a	a	a	a	*SIL 1*
a	a	a	SIL 1	*SIL 2*
a	a	SIL 1	SIL 2	*SIL 3*
a	SIL 1	SIL 2	SIL 3	*SIL 4*
SIL 1	SIL 2	SIL 3	SIL 4	*b*
SIL 2	SIL 3	SIL 4	b	*b*

Example Data Relating to Example Risk Graph

Risk parameter		Classification
Consequence (E)	E1 E2 E3 E4	Minor injury Serious permanent injury to one or more persons; death to one person Death to several people Very many people killed
Frequency and exposure in the hazardous zone (F)	F1 F2	Rare to more often exposure in the hazardous zone Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event (P)	P1 P2	Possible under certain conditions Almost impossible
Probability of the unwanted occurrence (W)	W1 W2 W3	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

Issues with the Risk Graph Method

- The clear and unambiguous definition and understanding of the four parameters is essential
  - they must be calibrated against the tolerable risk criteria in use
  - the calibration must be tested by considering some example cases to ensure that the resulting SIL rating will achieve the necessary risk reduction
- A common pitfall is the inconsistency (or lack of repeatability) of results
- Different SIL ratings have been determined when
  - different teams have been used to carry out repeat SIL assessment for the same system
  - and even with the same teams used for the same system, when the assessment has been repeated a short time later
- This is due to poor calibration or uncertainties in the information used by the review team

Example: ASIL determination (ISO 26262)

Severity	Probability	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

ASIL determination parameters

- Severity
  - estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

- Exposure
  - state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

E0	E1	E2	E3	E4
Incredible	Very low probability	Low probability	Medium probability	High probability

- Controllability
  - ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control/uncontrollable

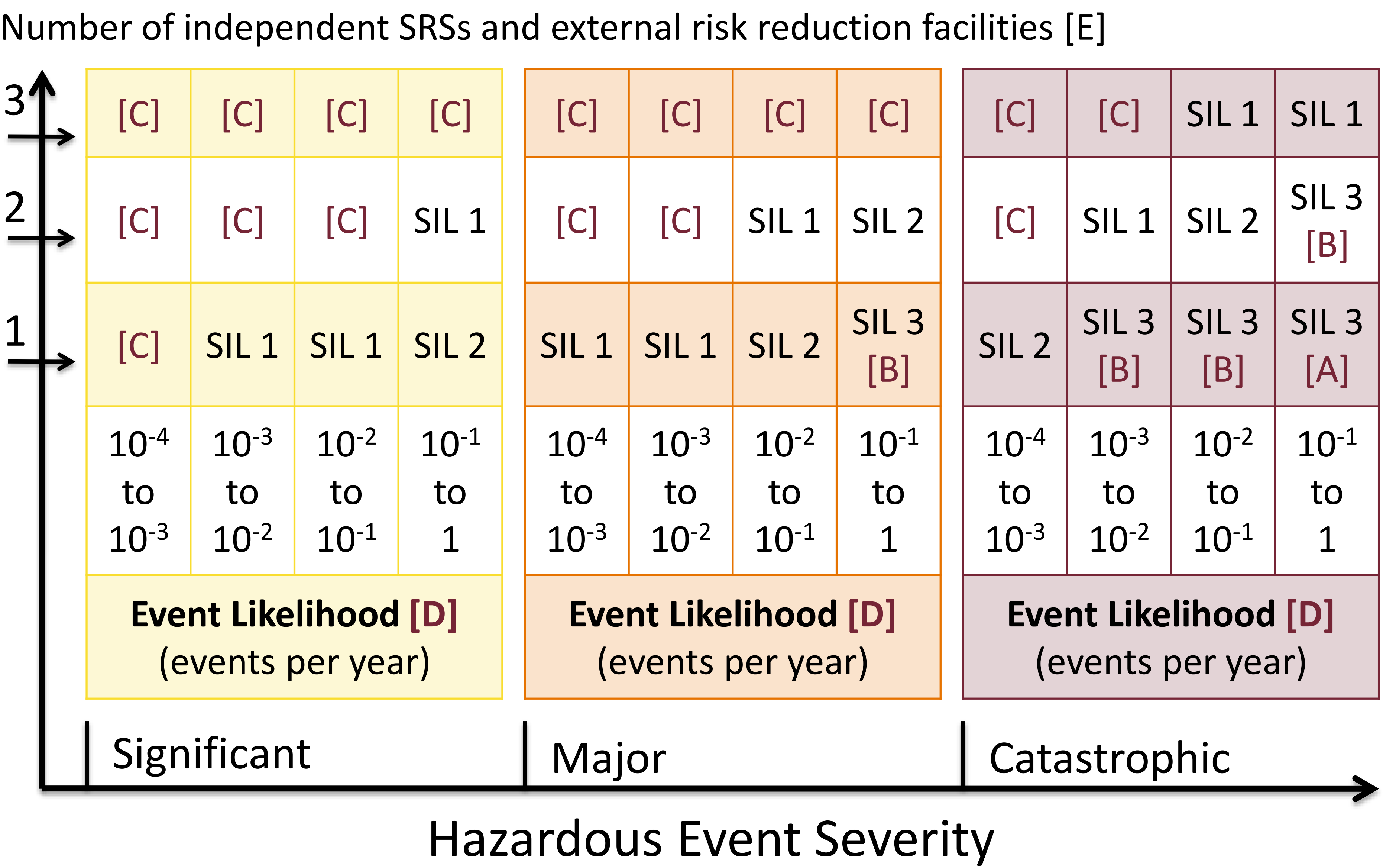
The Hazardous Event Severity Matrix Method

- The Hazardous Event Severity Matrix is also a qualitative method
  - primarily applicable to protective functions using multiple independent protective systems
- It can be considered as a decision matrix approach
- The review team considers three parameters to arrive at the required SIL rating:
  - Consequence risk parameter
  - Frequency risk parameter
  - Number of independent protective functions parameter

The Hazardous Event Severity Matrix Method

- The following requirements are necessary for the method to be valid:
  - the safety-related systems (E/E/PE and other technology) and the external risk reduction facilities are independent
  - each safety-related system (E/E/PE and other technology) and external risk reduction facilities are considered as protection layers which provide partial risk reductions
  - when one protection layer is added, then one order of magnitude improvement in safety integrity is achieved
  - only one E/E/PE safety-related system is used (but this may be in combination with an other technology safety-related system and/or external risk reduction facilities), for which this method establishes the necessary safety integrity level

Extended Hazardous Event Severity Matrix



Number of independent SRSs and external risk reduction facilities [E]

[E]	Significant				Major				Catastrophic			
3	[C]	[C]	[C]	[C]	[C]	[C]	[C]	[C]	[C]	[C]	SIL 1	SIL 1
2	[C]	[C]	[C]	SIL 1	[C]	[C]	SIL 1	SIL 2	[C]	SIL 1	SIL 2	SIL 3 [B]
1	[C]	SIL 1	SIL 1	SIL 2	SIL 1	SIL 1	SIL 2	SIL 3 [B]	SIL 2	SIL 3 [B]	SIL 3 [B]	SIL 3 [A]
	10^{-4} to 10^{-3}	10^{-3} to 10^{-2}	10^{-2} to 10^{-1}	10^{-1} to 1	10^{-4} to 10^{-3}	10^{-3} to 10^{-2}	10^{-2} to 10^{-1}	10^{-1} to 1	10^{-4} to 10^{-3}	10^{-3} to 10^{-2}	10^{-2} to 10^{-1}	10^{-1} to 1
	Event Likelihood [D] (events per year)				**Event Likelihood** [D] (events per year)				**Event Likelihood** [D] (events per year)			

Hazardous Event Severity

Comments to the Previous Figure

[A] One SIL 3 E/E/PE safety-related system does not provide sufficient risk reduction at this risk level. Additional risk reduction measures are required.

[B] One SIL 3 E/E/PE safety-related system may not provide sufficient risk reduction at this risk level. Hazard and risk analysis is required to determine whether additional risk reduction measures are necessary.

[C] An independent E/E/PE safety-related system is probably not required.

[D] Event likelihood is the likelihood that the hazardous event occurs without any safety related systems or external risk reduction facilities.

[E] SRS = safety-related system. Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

SIL Ratings for Combined Subsystems

0.5% Common Cause Failures		Primary Subsystem SIL Rating		
		SIL 1	SIL 2	SIL 3
Secondary Subsystem SIL Rating	SIL 1	SIL 1	SIL 2	SIL 3
	SIL 2	SIL 2	SIL 3	SIL 4
	SIL 3	SIL 3	SIL 4	> SIL 4

1% Common Cause Failures		Primary Subsystem SIL Rating		
		SIL 1	SIL 2	SIL 3
Secondary Subsystem SIL Rating	SIL 1	SIL 1	SIL 2	SIL 3
	SIL 2	SIL 2	SIL 3	SIL 4
	SIL 3	SIL 3	SIL 4	SIL 4

5% Common Cause Failures		Primary Subsystem SIL Rating		
		SIL 1	SIL 2	SIL 3
Secondary Subsystem SIL Rating	SIL 1	SIL 1	SIL 2	SIL 3
	SIL 2	SIL 2	SIL 3	SIL 4
	SIL 3	SIL 3	SIL 4	SIL 4

10% Common Cause Failures		Primary Subsystem SIL Rating		
		SIL 1	SIL 2	SIL 3
Secondary Subsystem SIL Rating	SIL 1	SIL 1	SIL 2	SIL 3
	SIL 2	SIL 2	SIL 3	SIL 3
	SIL 3	SIL 3	SIL 3	SIL 3

Summary of Points to Consider

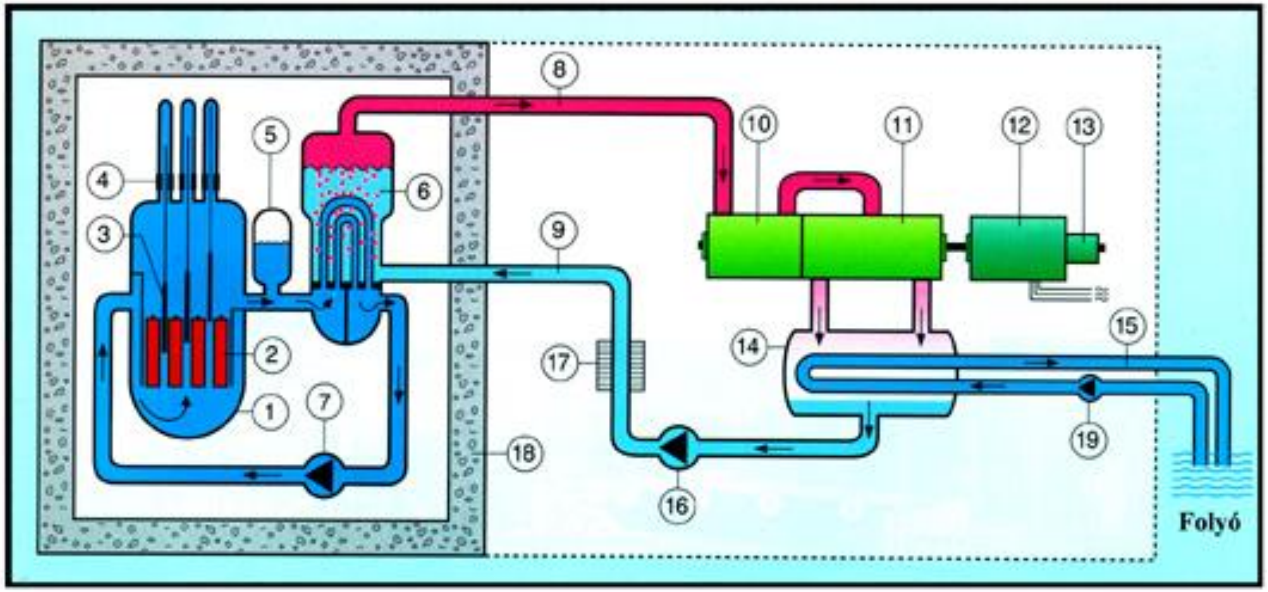
- The boundary of the equipment under control being considered in the FSA should be clearly defined as the detection, initiation and operation of the safety related system.
- It is essential that accurate information is available on the likelihood and consequences of the hazardous events that the protective functions mitigate against.
- A rigorous calibration exercise must be carried out
    - to ensure that the parameters are clearly and unambiguously defined
    - and tested to ensure that the resulting SIL rating will achieve the necessary risk reduction in accordance with the tolerable risk criteria.
- When assessing safety related systems, the possibility of common mode failures must be carefully assessed in order to arrive at valid SIL ratings.

Case Study: Reactor Rod Control System

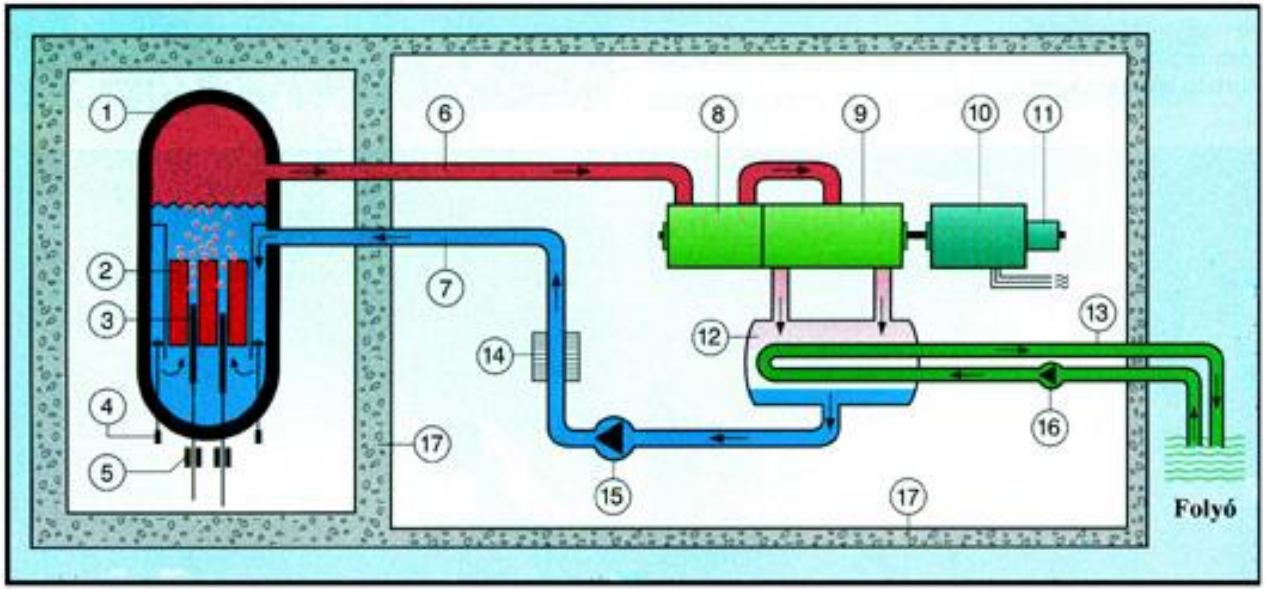
Derivation of Tolerable Hazard Rate Criteria for a Reactor Rod Control System in a Nuclear Power Plant

Generation II Light Water Reactor Types

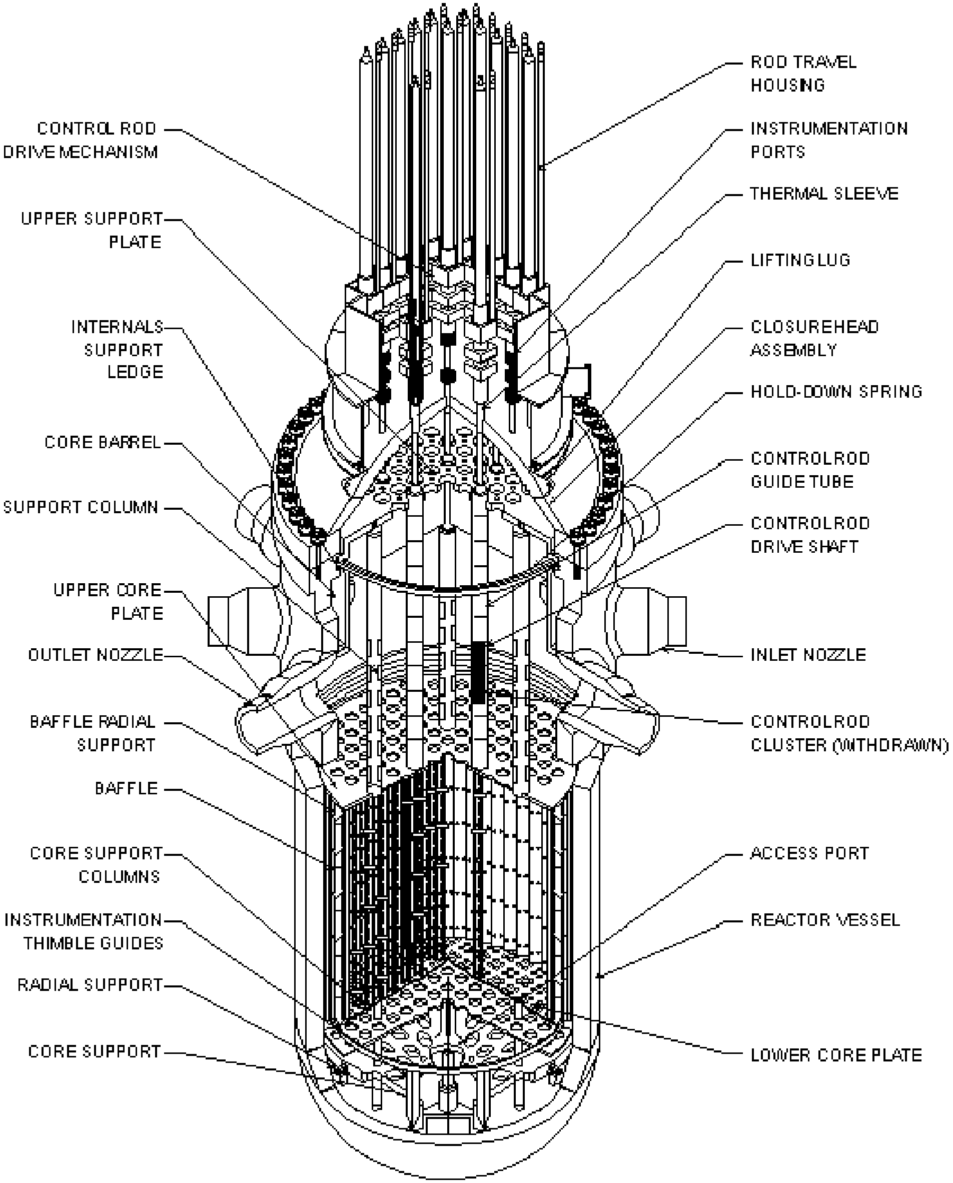
- Pressurized Water Reactor (PWR)
  - primary circuit
  - secondary circuit
  - steam generator
  - control rods from the top

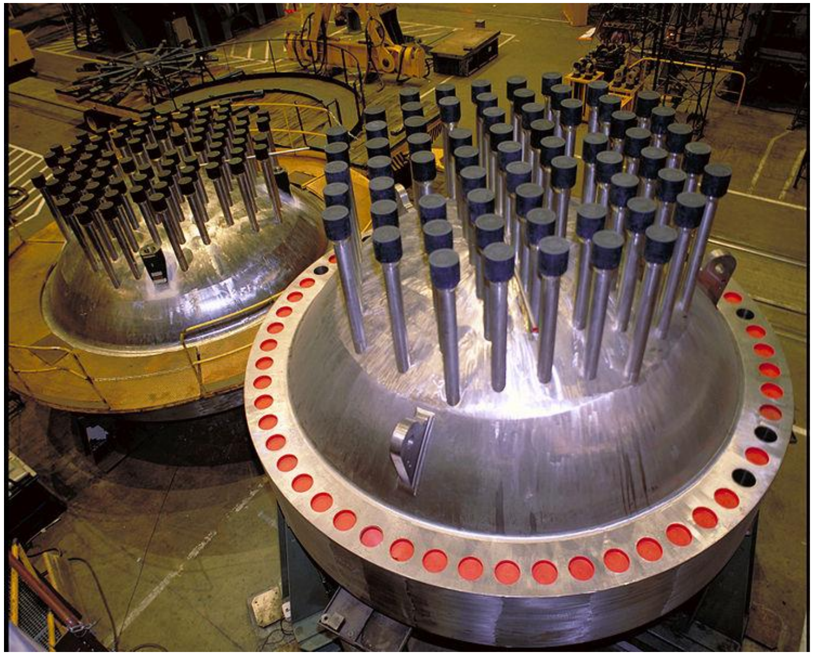


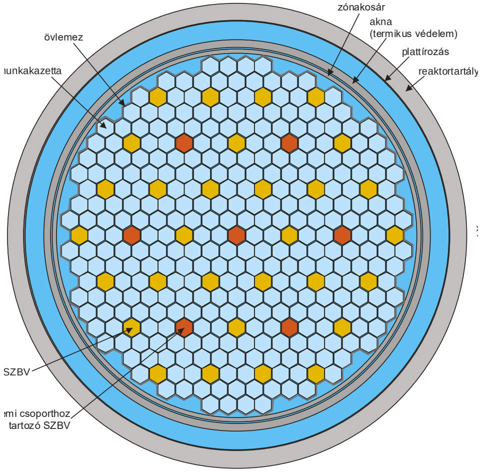
- Boiling Water Reactor (BWR)
  - single circuit
  - primary water is boiling
  - control rods from the bottom



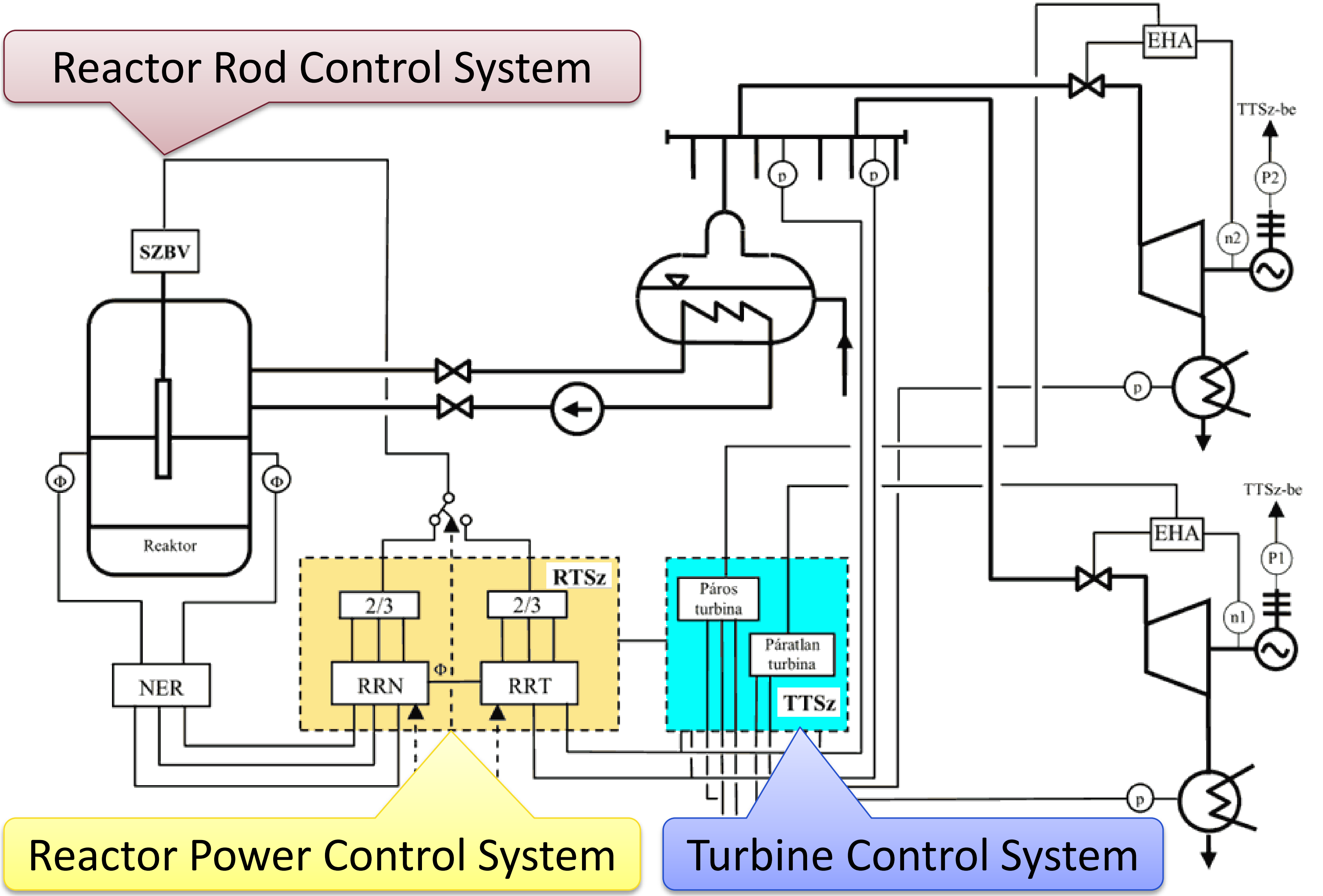
Reactor Control Rods







Reactor Power Control Scheme of Paks NPP

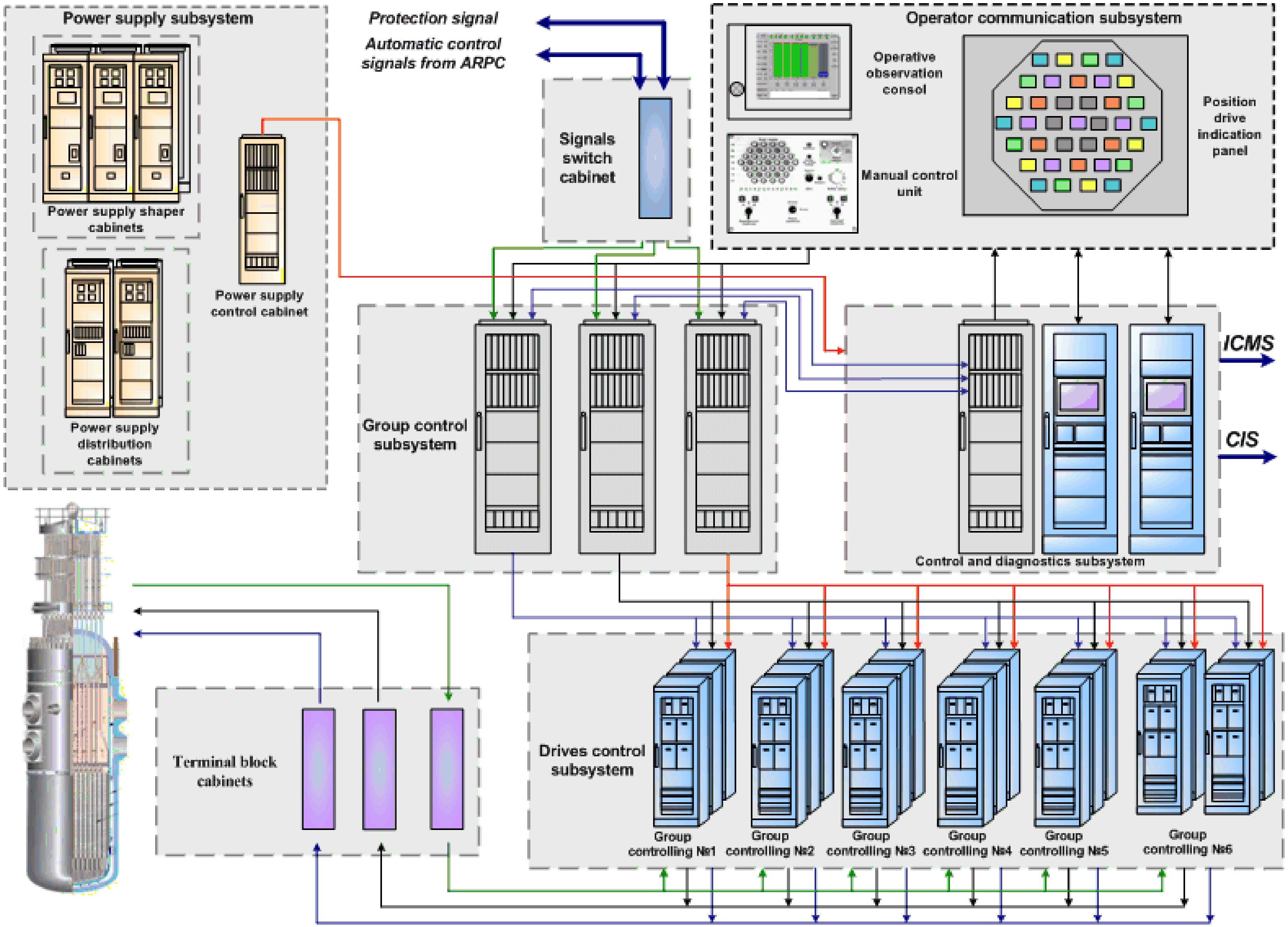


Reactor Rod Control System

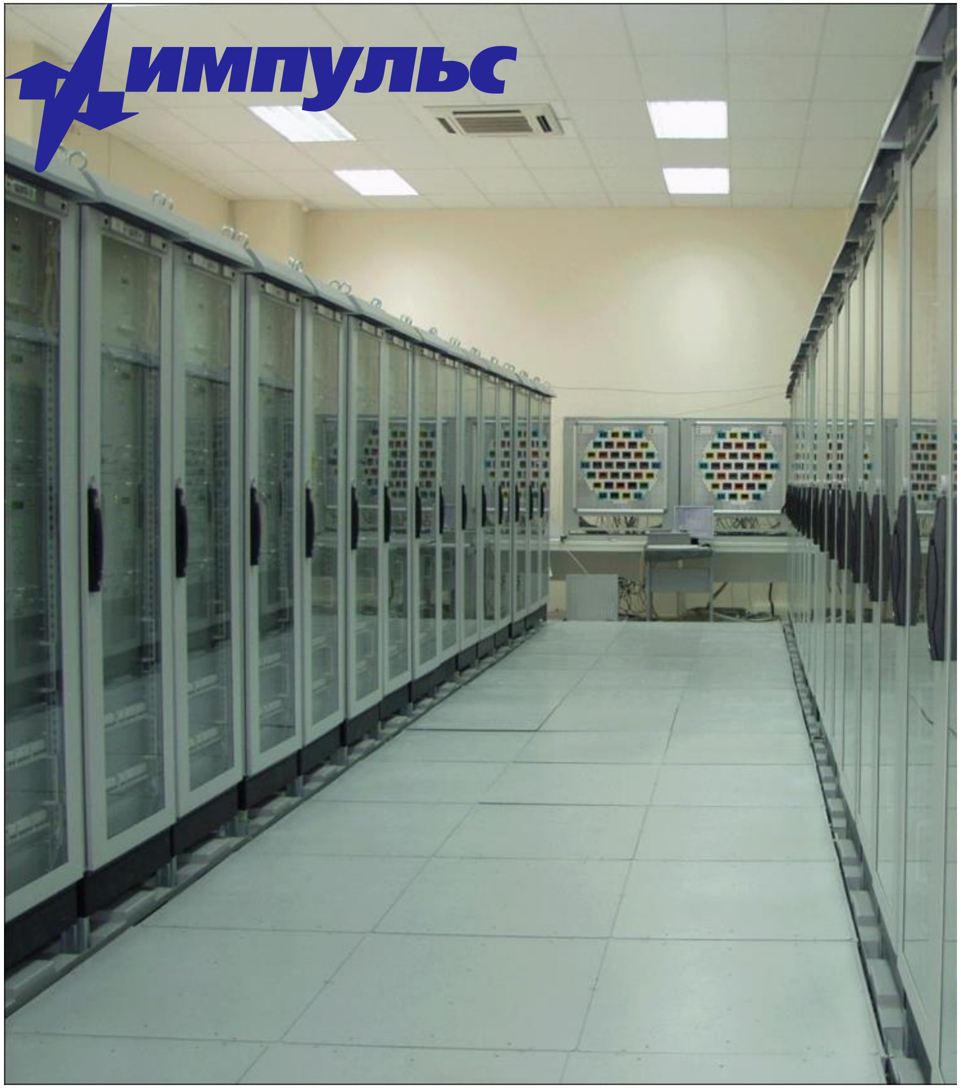
Reactor Power Control System

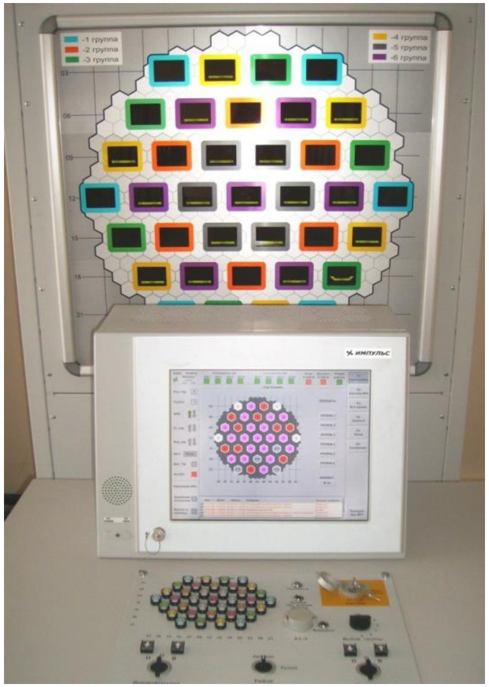
Turbine Control System

RCS-440 Reactor Rod Control System Scheme



RCS-440 Reactor Rod Control System





Scope and Functions of the RRCS

- The main functions of the RRCS are
  - the actuation of the rods that are primarily responsible for the power regulation in the NPP and
  - carrying out the respective actions according to
    - the operators' interventions and
    - the EP-1, EP-3, and EP-4 (Emergency Protection) signals originating from the Reactor Protection System
- The RRCS incorporates
  - the logic defining the direction & speed of rod movement
  - the frequency converters for the servo actuators
  - the rod position sensors
  - and the instrumentation and control devices in the main and auxiliary control rooms

Detailed Functions of the RRCS

1. Holding an individual rod in a given position
2. Moving an individual rod downwards with normal operational speed
3. Moving an individual rod upwards with normal operational speed
4. Moving (dropping) of an individual rod downwards with high speed (in case of EP-1)
5. Arranging rods into groups, realizing the functions F1-F3 for the defined groups
6. Handling the predefined groups, realizing the functions F1-F3 for the predefined groups
7. Controlling the rods downwards in case of EP-3
8. Prohibiting the upward control of rods in case of EP-4

Qualitative Classification of Consequences

- Catastrophic
  - Significant amount of radioactive contaminant released to the environment
  - Multiple deaths
  - Long term (e.g. several months) inoperability of a reactor unit
- Critical
  - Insignificant amount of radioactive contaminant released to the environment
  - One death or multiple severe injuries
  - Medium term (e.g. several days) inoperability of a reactor unit
  - Significant stress to a reactor unit (e.g. reactor trip/scram is necessary)
- Marginal
  - No release of radioactive contaminant to the environment
  - One severe injury or multiple minor injuries
  - Short term (e.g. shoutdown) inoperability of a reactor unit
- Negligible
  - No release of radioctive contaminant to the environment
  - One minor injury
  - Disruption of the normal operation, necessity of operator intervention

Hazard Identification and the Consequences

Function deviation	Consequence
F1. Holding an individual rod in a given position	
FD1-1. An individual rod remains erroneously in the given position	
• one rod:	Negligible
• multiple rods:	Marginal
• several rods:	Critical
FD1-2. Impossible to hold an individual rod in the given position, moves downwards	
• one rod:	Negligible
• multiple rods:	Marginal
FD1-3. Impossible to hold an individual rod in the given position, moves upwards	
• one rod:	Negligible
• multiple rods:	Marginal
• several rods:	Critical

Tolerable Risk Frequencies

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	II
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

- Class I: Not permissible, the risk must be reduced by all means
- Class II: Permissible if and only if the risk is demonstrably cannot be reduced any more
- Class III: Permissible, but it needs to be examined if the risk can be reduced further in an economical way
- Class IV: The risk is tolerable without any further action

Risk Reduction Requirements

- To get a risk into Class III or below:
  - In case of catastrophic consequence: improbable or lower frequency of occurrence is needed.
    - The RRCS does not have a function whose deviation can cause catastrophic consequences, due to the fact that the emergency protection is initiated by the safety-critical Reactor Protection System.
  - In case of critical consequence: remote or lower frequency of occurrence is needed.
    - The RRCS does have functions whose deviation can cause critical consequences, due to the fact that the emergency shutdown of the reactor unit (reactor trip) belongs to this category.
  - In case of marginal consequence: occasional or lower frequency of occurrence is needed.
  - In case of negligible consequence: probable or lower frequency of occurrence is needed.

Quantification of the Hazard Rates

Frequent	1 event per 0,1 year	THR=10 1/year $\approx 10^{-3}$ 1/h
Probable	1 event per 1 year	THR=1 1/year $\approx 10^{-4}$ 1/h
Occasional	1 event per 10 years	THR=0,1 1/year $\approx 10^{-5}$ 1/h
Remote	1 event per 100 years	THR=0,01 1/year $\approx 10^{-6}$ 1/h
Improbable	1 event per 1000 years	THR=0,001 1/year $\approx 10^{-7}$ 1/h
Incredible	1 event per 10000 years	THR=0,0001 1/year $\approx 10^{-8}$ 1/h

Frequency of occurrence values are assigned according to the safety indices of the NPP and the threshold limits used in the reactor protection system (e.g. allowed frequency of false EP-1 operation is 1 per 100 years)

Safety Requirements: Tolerable Hazard Rate

- **THR = 10^{-6} 1/h for the following events:**
  - **FD.1.1.** An individual rod remains erroneously in the given position; several rods event
  - **FD.1.3.** Impossible to hold an individual rod in the given position, moves upwards; several rods event
  - …
- **THR = 10^{-5} 1/h for the following events:**
  - **FD.1.1.** An individual rod remains erroneously in the given position; multiple rods event
  - **FD.1.2.** Impossible to hold an individual rod in the given position, moves downwards; multiple rods event
  - **FD.1.3.** Impossible to hold an individual rod in the given position, moves upwards; multiple rods event
  - …