Modelling of Digital I&C — MODIG project

Jan-Erik Holmberg[1], Ola Bäckström[2], Markus Porthin[3], Tero Tyrväinen[3]

NKS Seminar, January 12-13, 2016, Solna

[1] Risk Pilot AB

[2] Lloyd's Register Consulting - Energy AB,

[3] VTT Technical Research Centre of Finland Ltd

RISK PILOT©
YOUR RISK NAVIGATOR

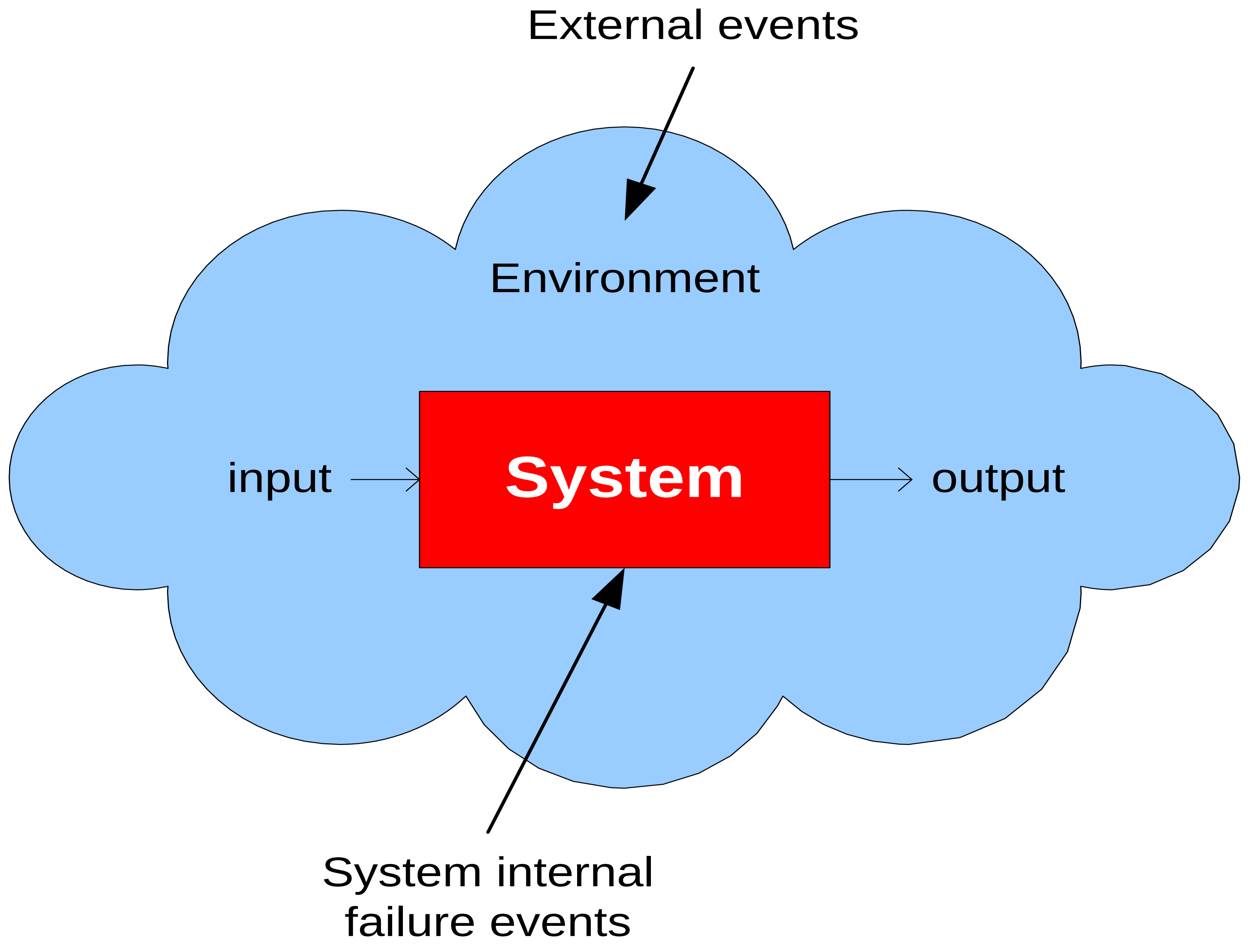
ACKNOWLEDGMENTS

- The work is financed by NKS (Nordic nuclear safety research), SAFIR2018 (The Finnish Research Program on Nuclear Power Plant Safety 2015–2018) and the Swedish Radiation Safety Authority
- MODIG project partners: Risk Pilot AB, Lloyd's Register Consulting - Energy AB, VTT Technical Research Centre of Finland Ltd

- NKS conveys its gratitude to all organizations and persons who by means of financial support or contributions in kind have made the work possible

MODIG background

- How to demonstrate safety of complex socio-technological system?
  - Deterministic safety analysis
    - Postulated scenarios may not lead to unwanted consequences
  - Probabilistic safety assessment (PSA)
    - Quantitative risk criteria shall be met

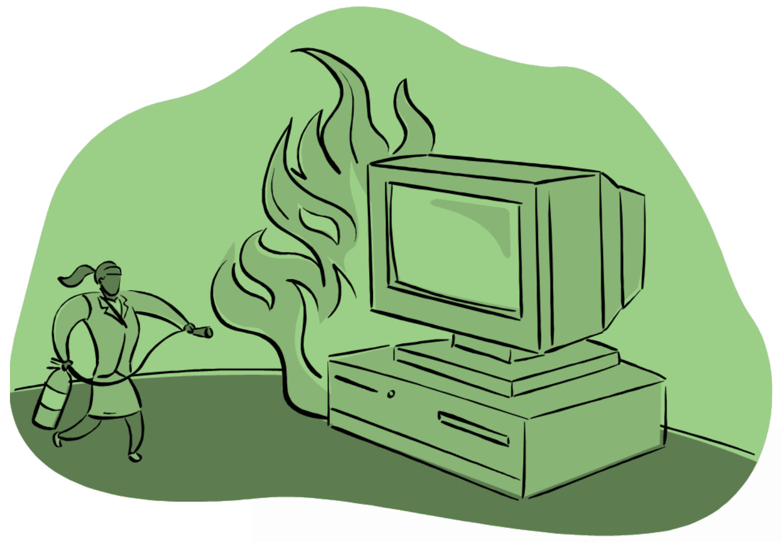


- I&C consist consist of several system related to practically all safety functions of a nuclear power plant
  - Practical and justifiable approaches are needed to assess I&C

MODIG objectives

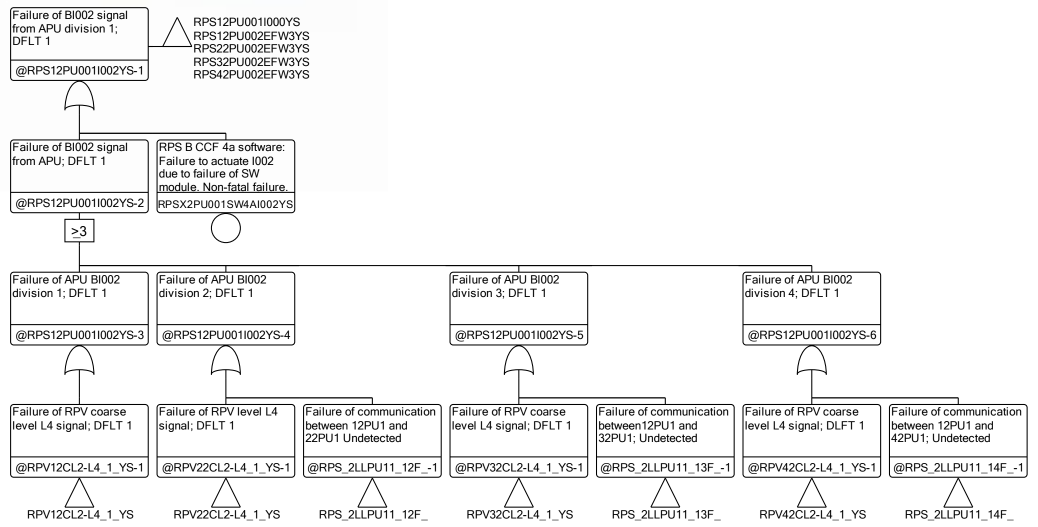
- To get a consensus approach for a reliability analysis of a plant design with digital I&C
- To get improved integration of probabilistic and deterministic approaches in licensing of digital I&C
- To improve failure data collection including software failure probability quantification
- To perform practical application of PSA to compare design alternatives

What do we try to do better?

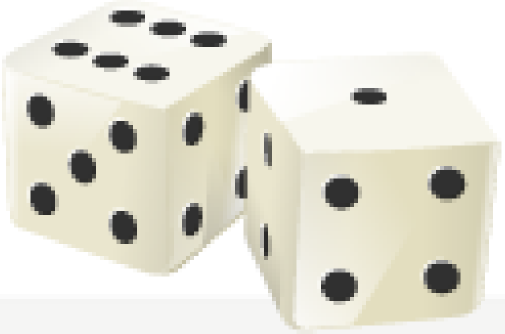


- More accurate consideration of failure modes
  - ”not just processor crash”

- More accurate consideration of the I&C architecture
  - a processor is ”not just a single black box”



- Reasonable approach to model a complex system
  - relevant dependences and failure modes are accounted for
  - understandable model structure and designation system

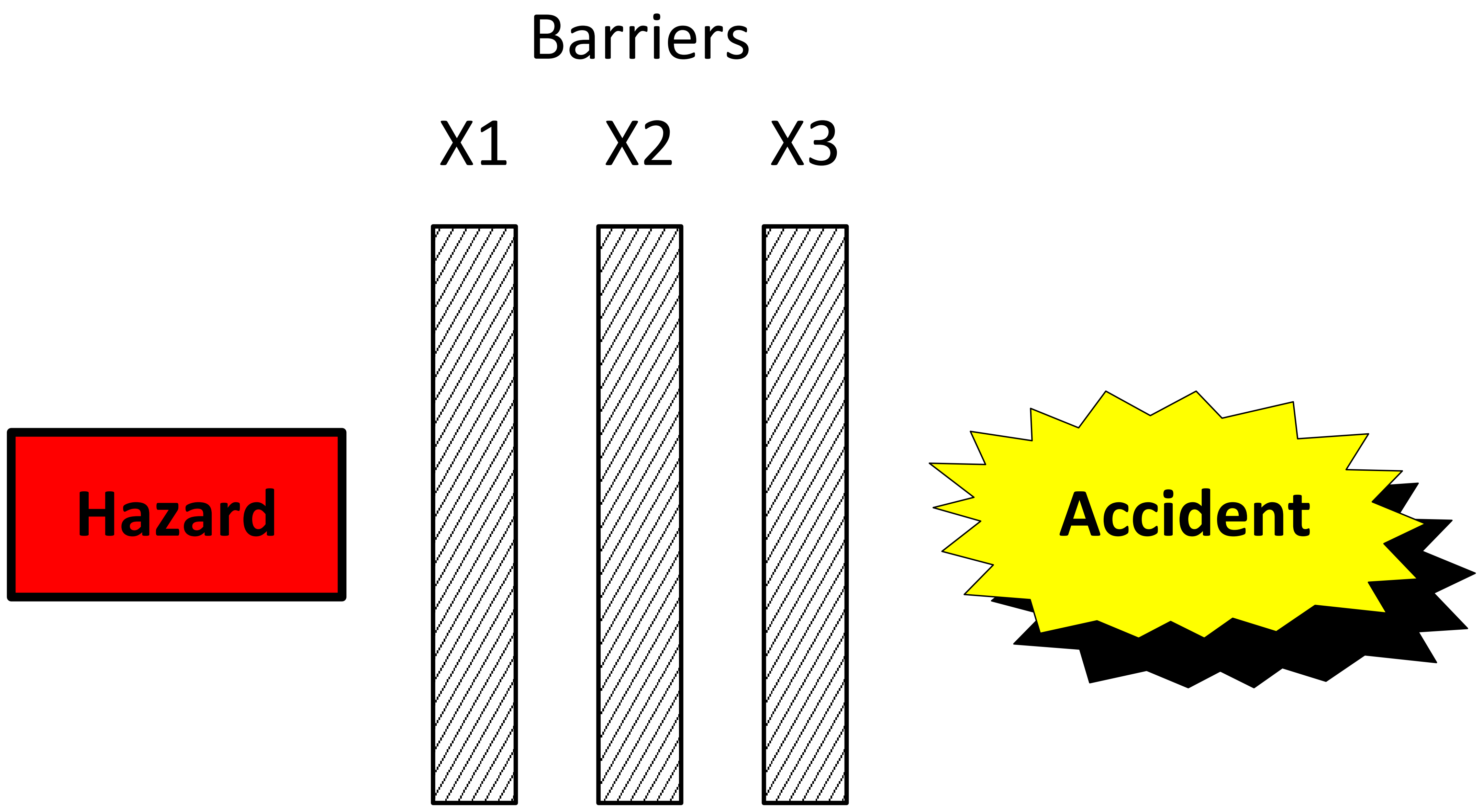


- Better justification of reliability numbers
  - use of operating experience where applicable and justifiable
  - coherent use of expert judgements

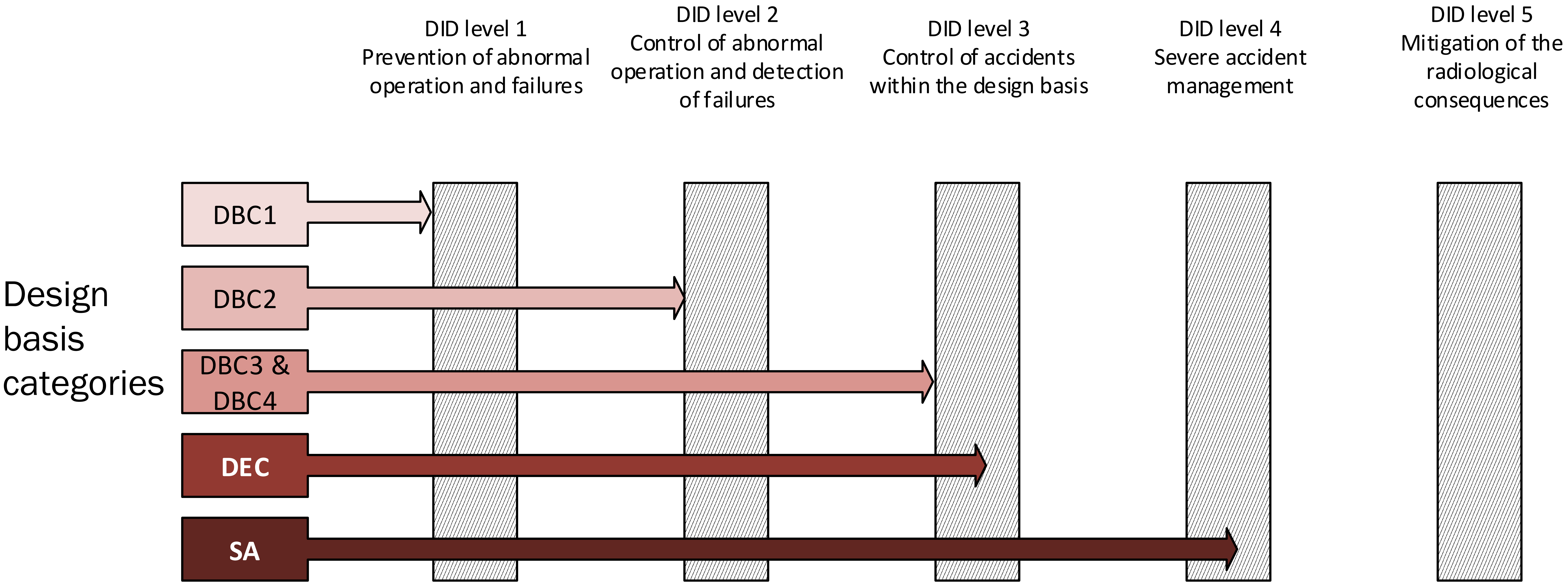
RISK PILOT©
YOUR RISK NAVIGATOR

Defence-in-depth (DiD)

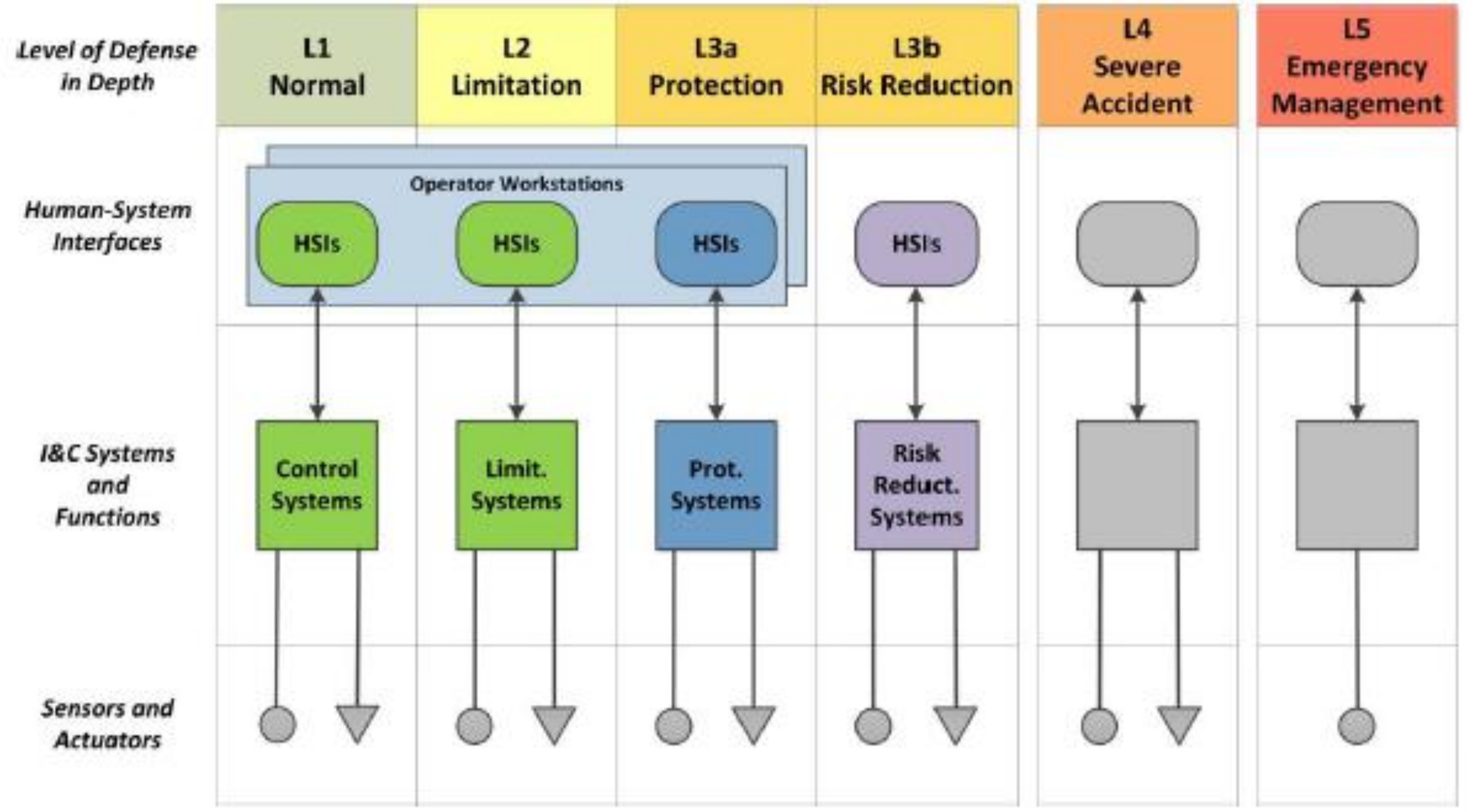
- More than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails
  - inherent safety features
  - use of multiple barriers, engineered safety features
  - accident prevention and mitigation
  - principles and procedures followed in design, construction, operation, maintenance and decommission of the system



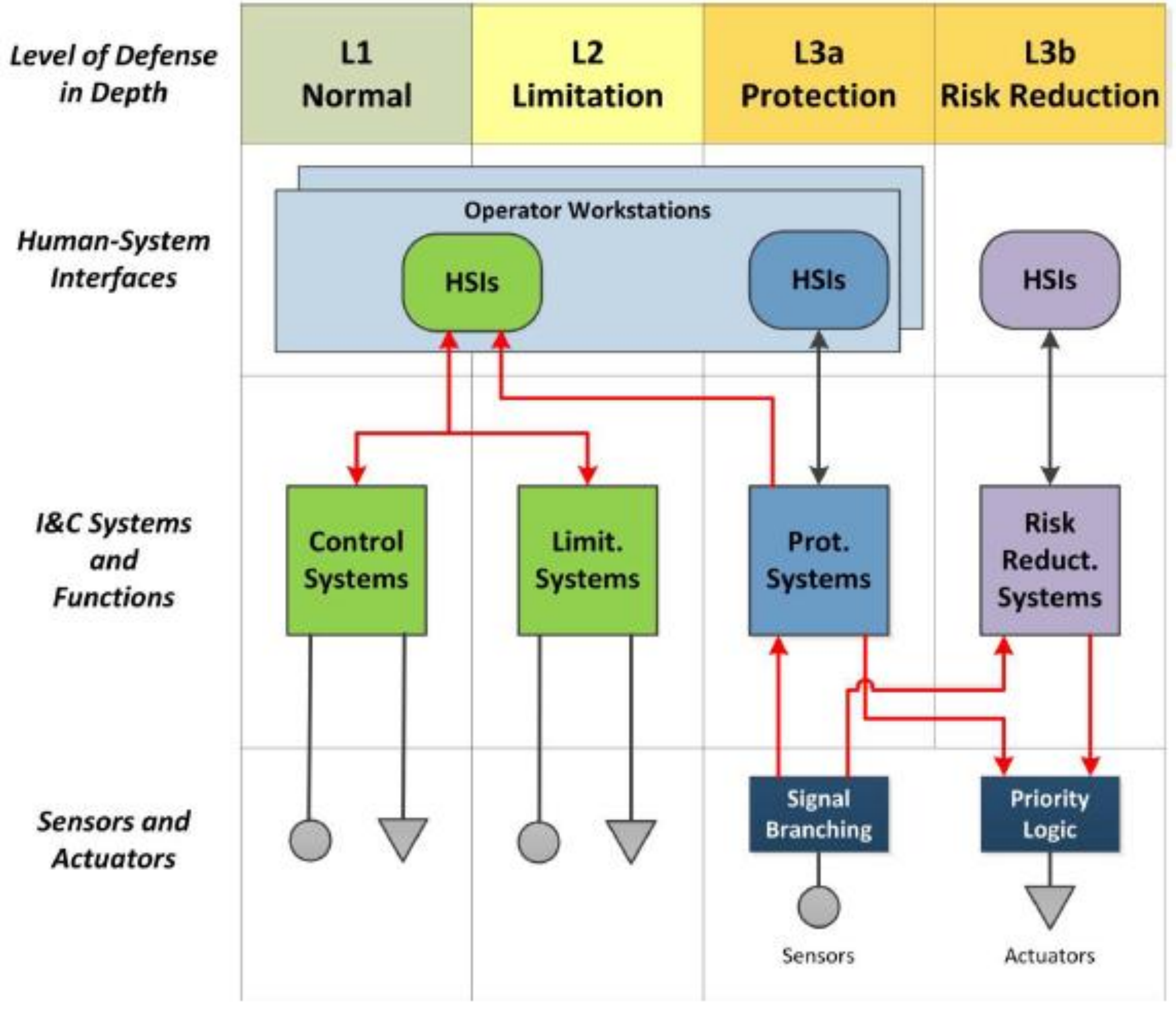
Deterministic criteria for DiD [STUK/YVL]



Idealized I&C architecture [EPRI]

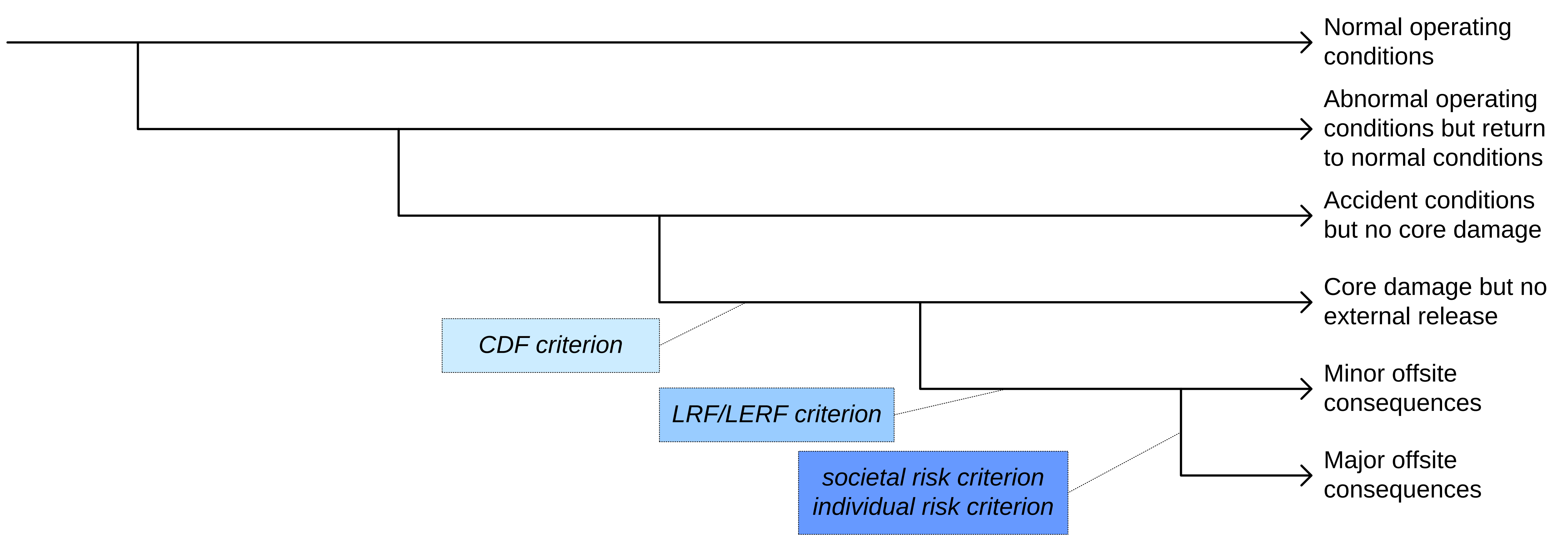


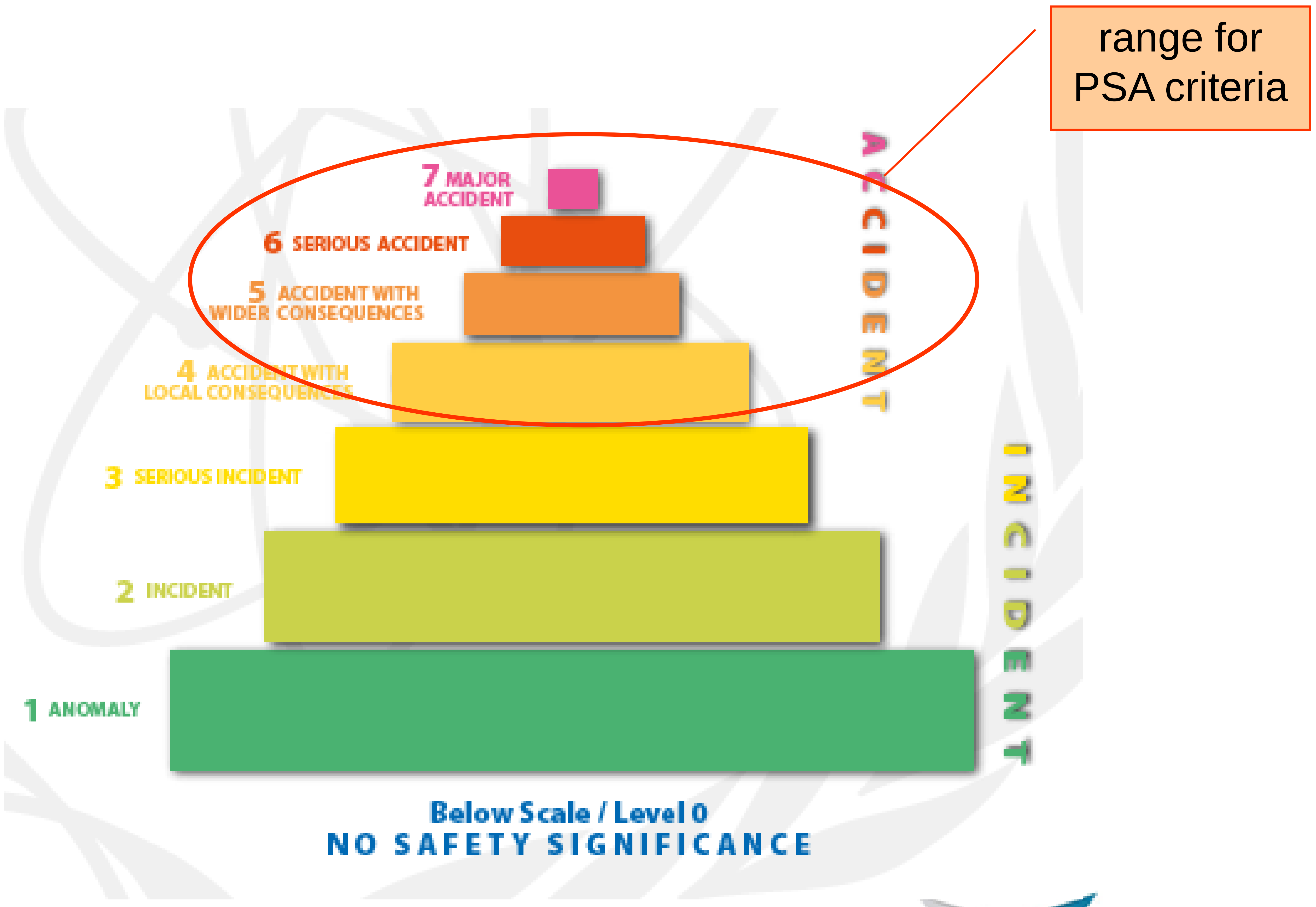
Possible sharing and interconnections among DiD levels [EPRI]



DiD and INES scales vs. nuclear risk criteria

Initiating event Level 1 PSA		Safety functions Level 1 PSA	Safety functions Level 2 PSA	Consequence Level 3 PSA	
DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management	DID level 5 Mitigation of the radiological consequences	Consequence





Conclusions from current PSAs

- Level 1 PSA evaluates DiD levels 1-3
  - Without some diversity for DiD level 3 difficult to achieve the core damage frequency goal 1E−5/yr

- Level 2 PSA evaluates DiD level 4
  - DiD level 4 must be independent from DiD levels 1-3 to achieve large release freqeuncy goals 1E−7…1E−6/yr

Use of PSA for deterministic assessment

- PSA model is an excellent tool to handle complex dependencies
- It is also excellent for sensitivity analysis
- Minimal cut sets provide the necessary and sufficient information to judge whether deterministic failure criteria are fulfilled

- Examples:
  - For DBC2-4 events it must be, e.g., shown that “it shall be possible to accomplish decay heat removal from the reactor and containment by one or several systems that jointly meet the (N+2) failure criterion…”

  - For DEC-A events (= DBC2 or DBC3 combined with a CCF in a safety system) a diverse N+1 system is needed to reach a safe state

Some questions related to the assessment of DiD of typical NPP designs

- Can a system requiring an operator action be (N+1) failure tolerant?
- Shall the (N+1) failure criterion be applied to structures like the demineralized water tank?

- How different hazards, such as fire events should be classified?
- Can Loss-of-offsite-power (LOOP) be classified into different design basis categories depending on the duration of the LOOP?

- Which type of software CCF:s should be counted as a common cause failure in the DEC-A analysis?
  - System software CCF (platform failure)?
  - CCF between nearly identical application software modules?

RISK PILOT©
YOUR RISK NAVIGATOR

Software reliability

- Functionality of I&C is implemented by software modules running in hardware modules
- Failures of software based systems are due to specification errors
  - Latent errors triggered by the context
  - Risk for common cause failures
  - Difficult to apply statistical methods in the reliability assessment

- How to deal with software reliability is very debated => no consensus
- Licensing of software based safety systems has become difficult (deterministic problem)

- It should be noted that many debatable questions are not actual software specific

Software modules:
- system software (operating system)
- application function modules
- library functions
- proprietary software modules
- data communication protocol
- data tables
- functional requirements specification (virtual software)

Approach to define failure modes and effects for software

- In principle, we may assume a fault in any of the software module and then consider maximum, reasonable failure effects

- Simplifications are needed to keep the number of fault-effect combinations reasonable

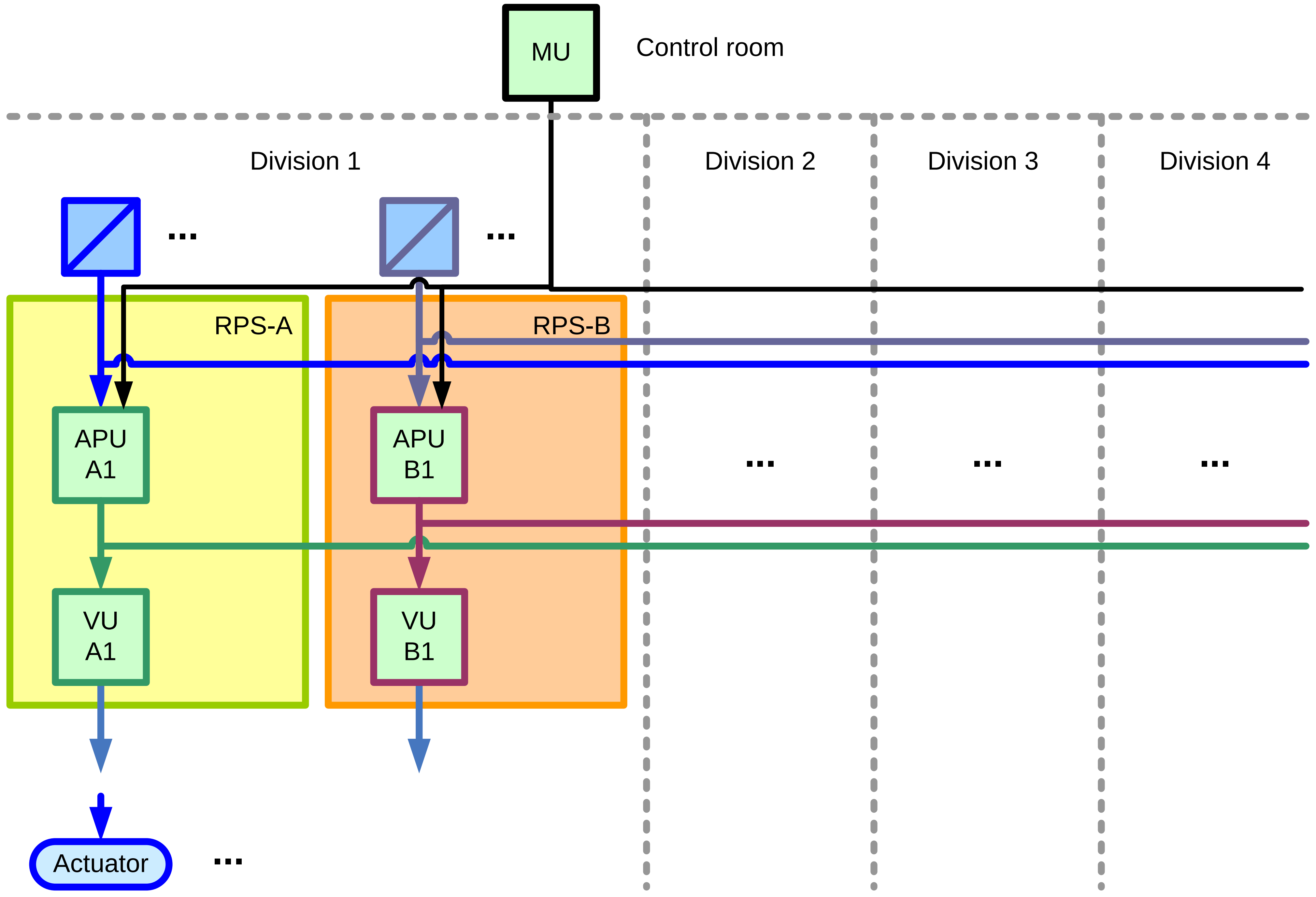
  - postulated fault locations can be reduced to certain software modules
    - other cases are covered by these cases

  - there is a simple way of defining failure effects which is not only sufficient but also exhaustive

Software fault cases for the reactor protection system with two diverse subsystems (RPS-A & RPS-B)

Effects	Software fault location			
	System software	Data communication software	APU application software	VU application software
Loss of complete system	case 1	case 1		
Loss of one subsystem	case 2a	case 2b		case 2a
Loss of one group of redundant APU in one subsystem			case 3a	
Loss of one group of redundant voters in one subsystem				case 3b
Loss of one function in all divisions of one subsystem			case 4a	case 4b
Loss of one function in one division of one subsystem			case 4c	

Fatal failure
Fatal or Non-fatal



Approach to quantify software reliability

- Different approach depending on the type of software module
- There can be a lot operational experience available for the system software (operational SW running in processors)
- For application software use of operating experience is more questionable
  - Which data is representative? How to pool data?
  - Alternatively use of indirect evidence such as complexity and V&V metrics has been studied
    - More complex => less reliable
    - More V&V (higher safety class) => more reliable

Further questions related to the software reliability

- Judgements on representativeness of operating experience
- Justification of the complexity and V&V metrics for application SW
- CCF between nearly identical SW modules
- Appropriate level of details in the modelling

Conclusions

- DiD is a multi-faceted safety principle, many interpretations, implies a lot of requirements for the design
- Deterministically difficult to demonstrate complete fulfilment of all desired requirements
- PSA can evalute risk criteria related to DiD levels 3-5
  - probabilistic argumentation should be used to compare I&C design alternatives
  - PSA's logic model facilitates the analysis of failure criteria
- Software reliability assessment is an inherently challenging task
- International collaboration is needed to achieve a consensus approach

Jan-Erik Holmberg

jan-erik.holmberg@riskpilot.fi
+358(0)40 827 6656

RISK PILOT©
YOUR RISK NAVIGATOR