Erfaringer fra kjernekraft

ESRA Seminar

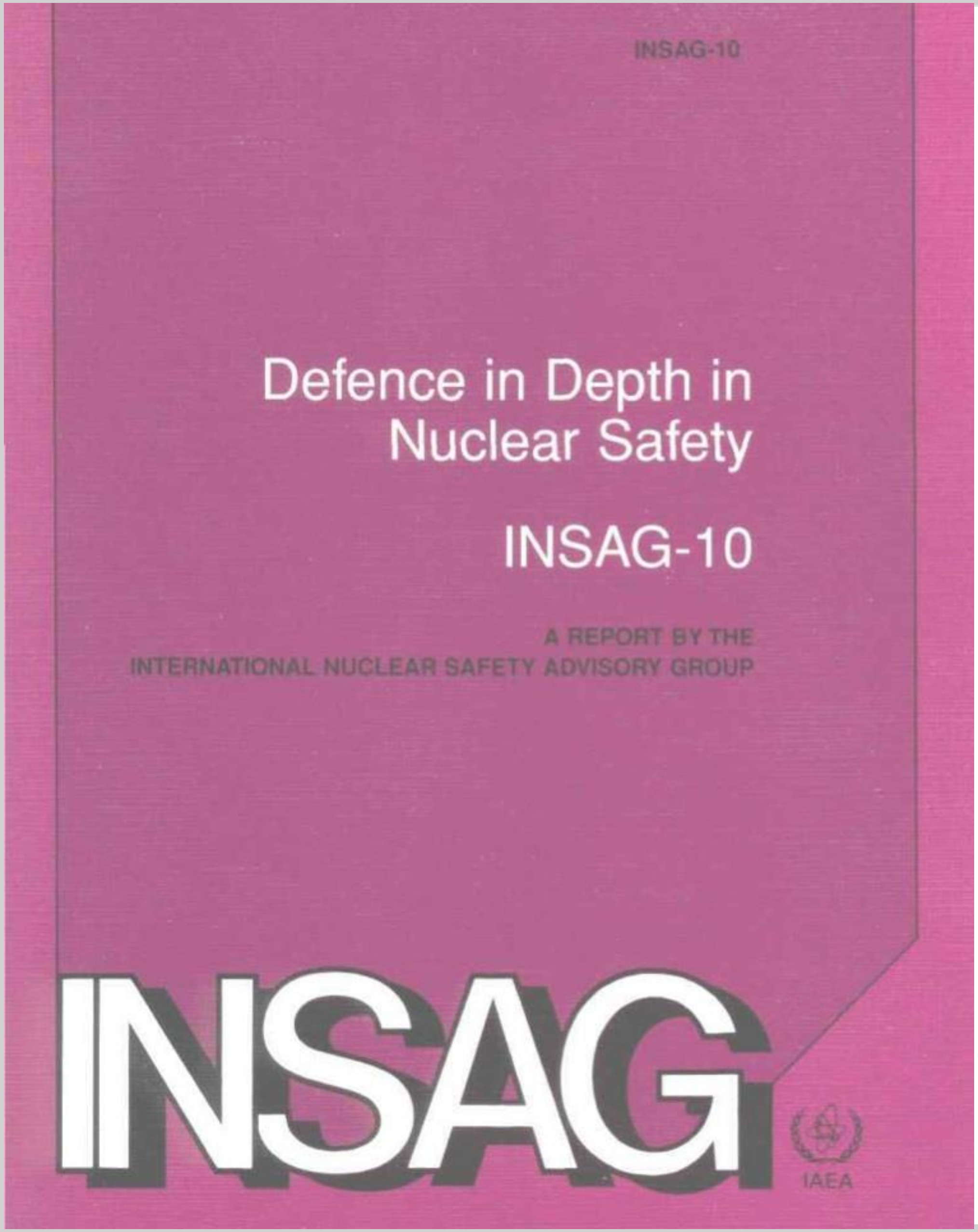
April 10, 2013

Salvatore Massaiu
Industrial Psychology Department
Institute for Energy Technology

Outlook

- Different barrier concepts
  - Defense in Depth and barriers
  - Technical and organizational barriers
  - Safety management and risk analysis

- Main technical point: Integrating human and organizational factors in risk analysis



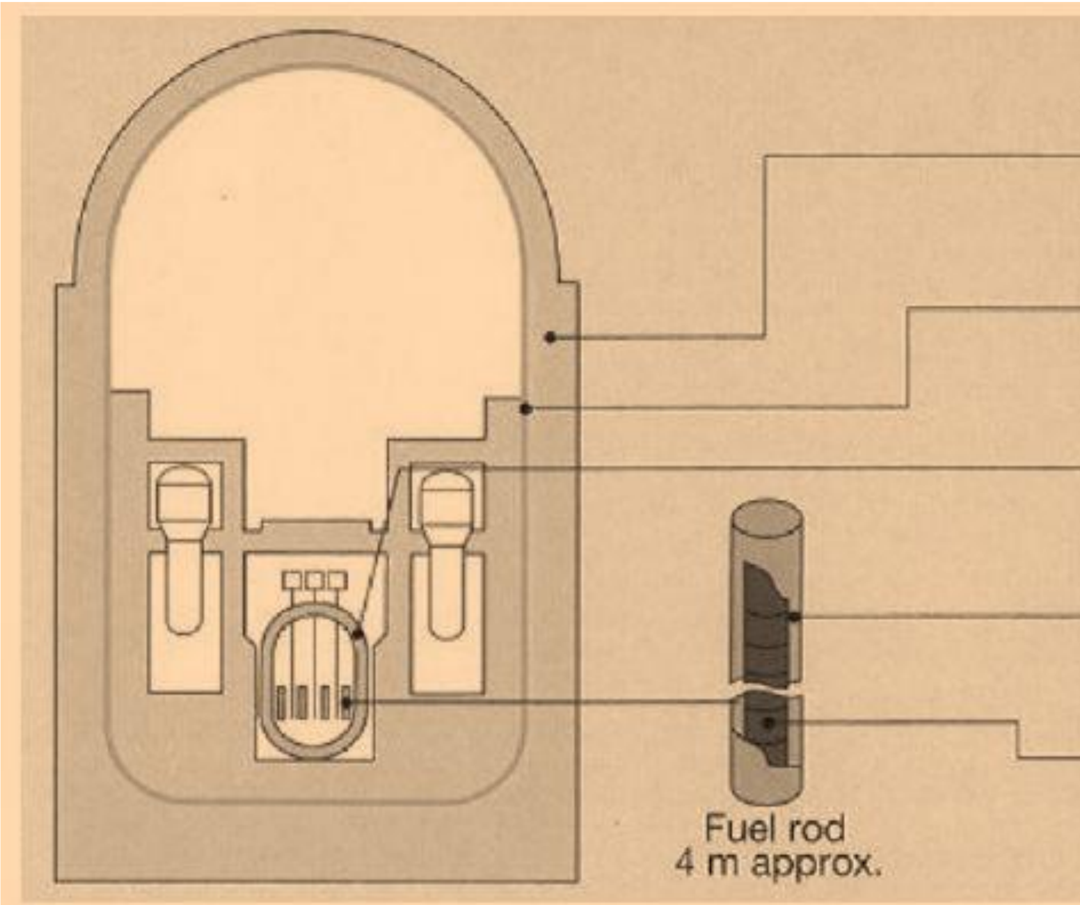
Defence in Depth

- **The idea of multiple levels of protection** is the central feature
- Includes the means to provide the barriers themselves with successive layers of protection

Defence in depth

A hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment

Physical barriers between the reactor core and the environment



5 Concrete containment building: 1,3 meter thick

4 Steel containment building sheet: 6 mm thick steel

3 Reactor pressure vessel : 20 cm thick steel container

2 Fuel cladding tubes: Strong metallic zirconium alloy

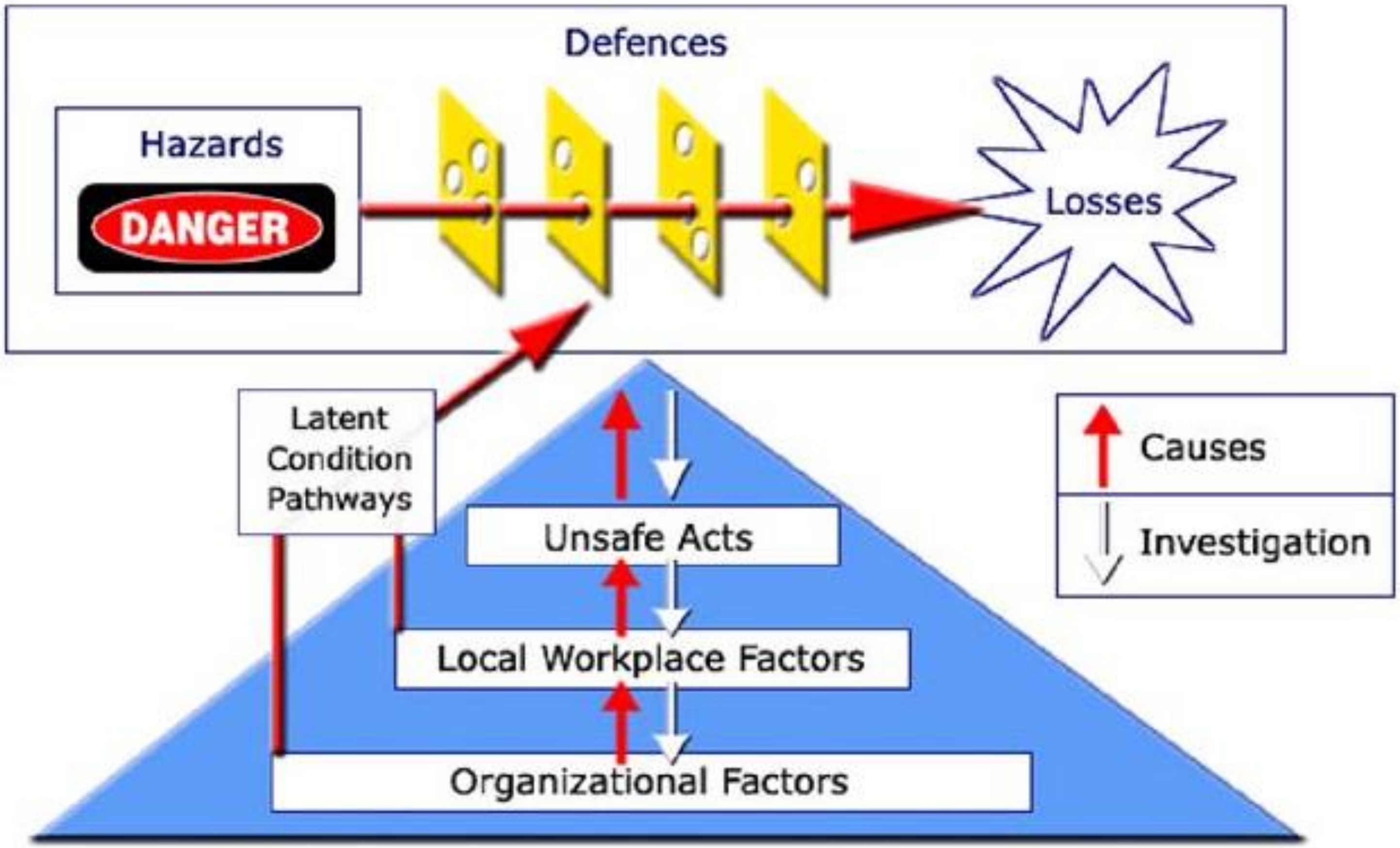
1 Pellet: Uranium fuel baked hard at high temperatures

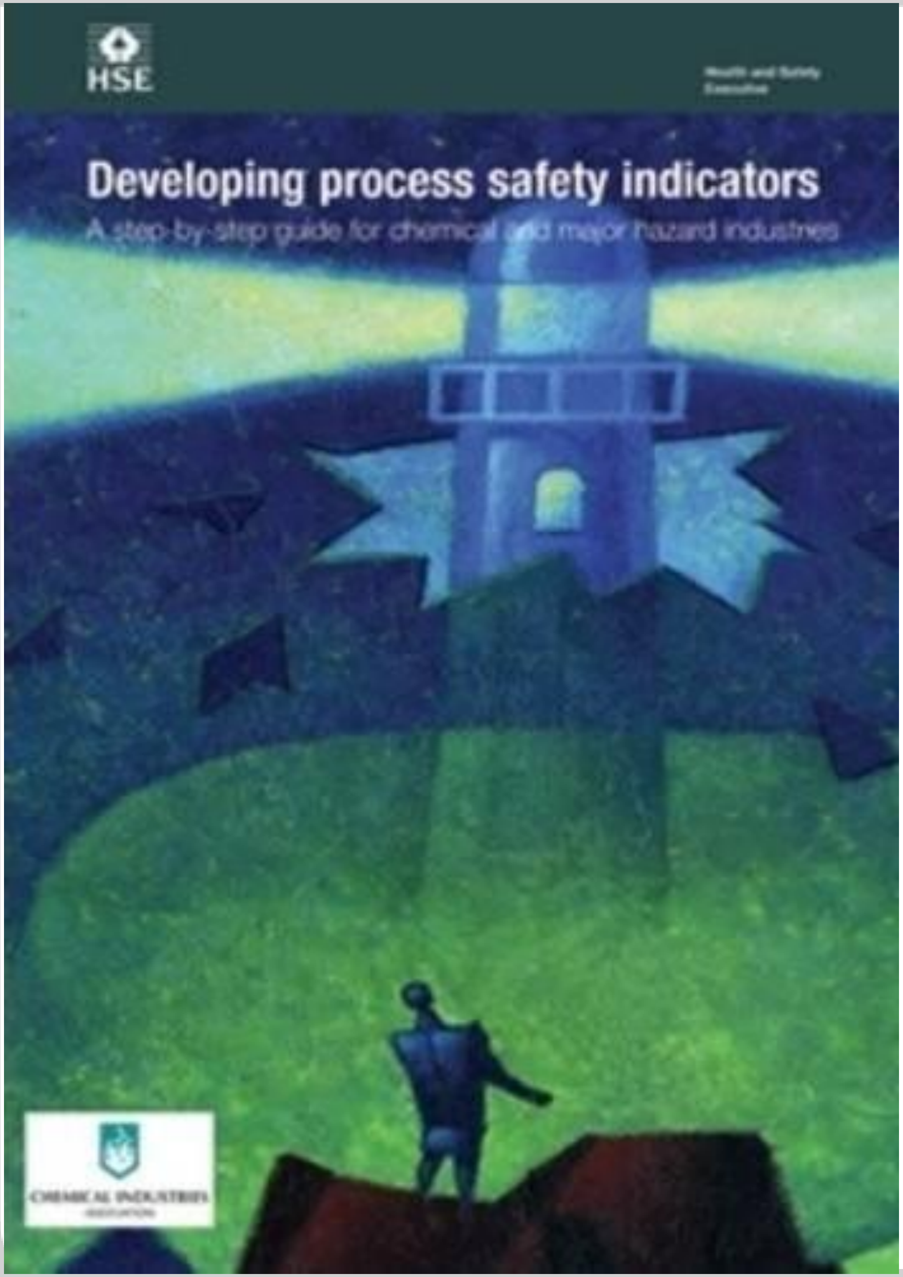
Preventing release of radioactive material

Organizational barriers

Equipment and procedures maintain the effectiveness of physical barriers

Reason's Anatomy of an Organizational Accident





HSE's safety indicators

The **indicators** monitor that systems and procedures continue operating as intended

Process safety management system: the parts of an organisation's management system intended to prevent major incidents

Risk control systems (RCS): the constituent part of a process **safety management** system that focuses on a specific risk or activity

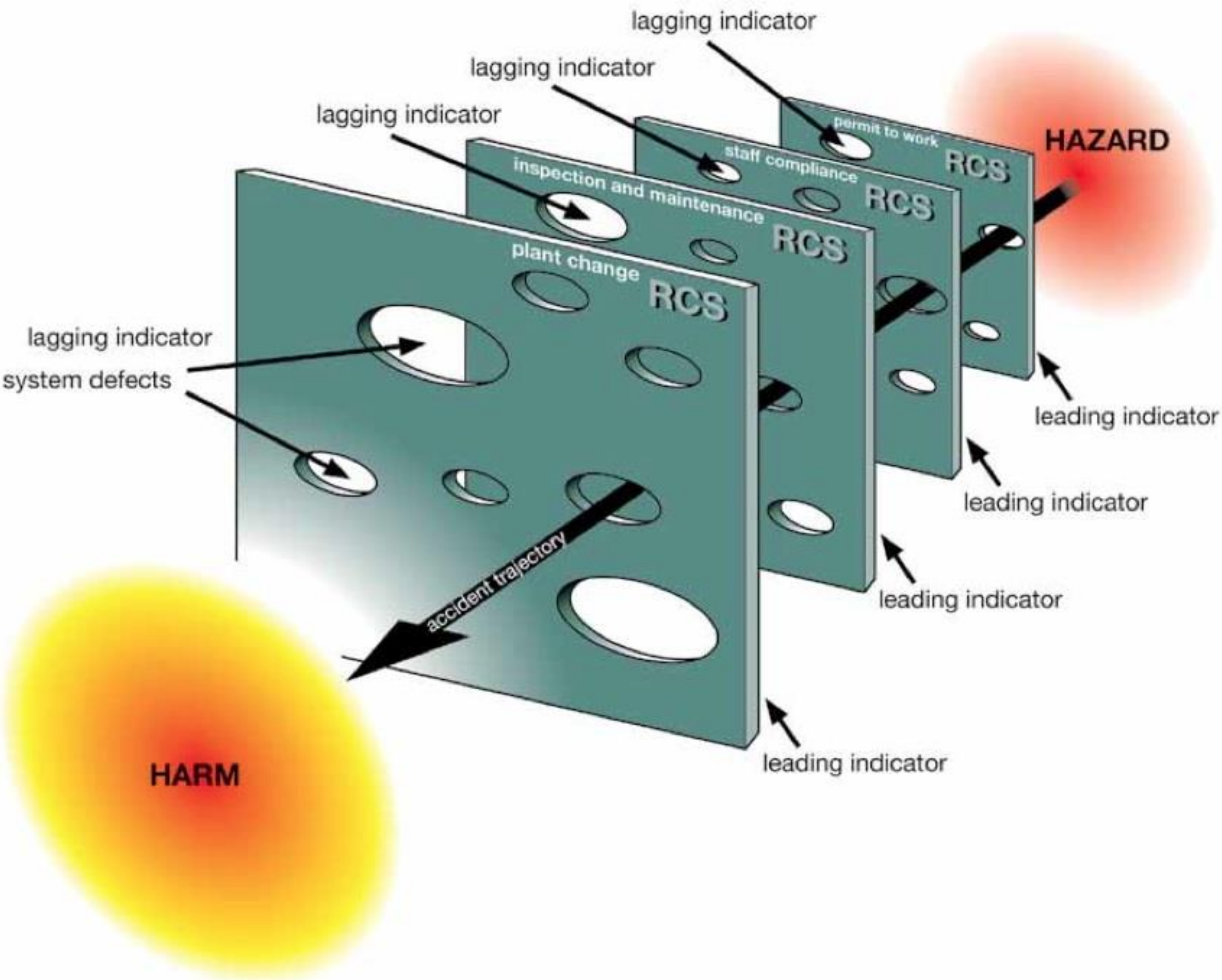

lagging indicator
lagging indicator
lagging indicator
permit to work
staff compliance
inspection and maintenance
plant change
RCS
RCS
RCS
RCS
HAZARD
lagging indicator
system defects
leading indicator
leading indicator
leading indicator
leading indicator
accident trajectory
HARM

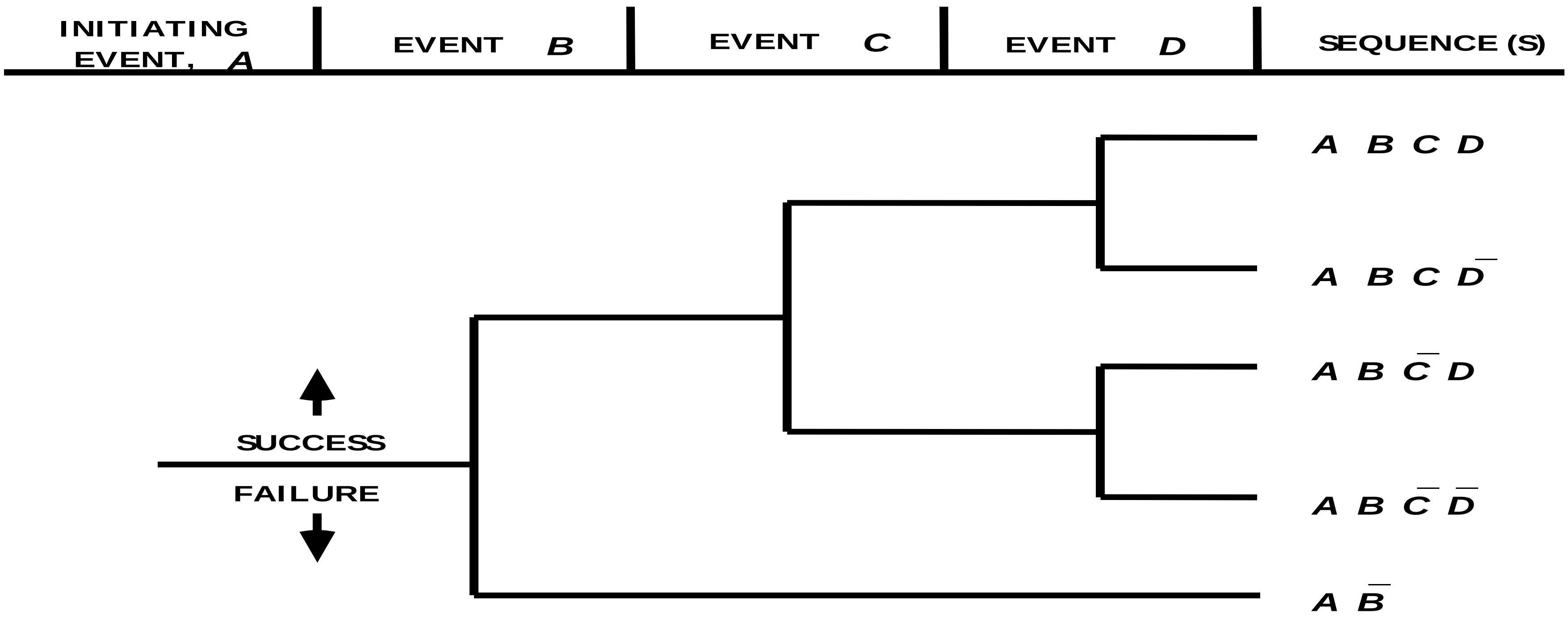
Table 3 Risk control matrix

	Challenges to plant integrity						
	Wear	Corrosion	Damage	Over/under pressurisation	Fire and explosion	Overfilling	Other accidental release
Inspection and maintenance of:							
Flexi hoses, couplings, pumps, valves, flanges, fixed pipes, bulk tanks	✓	✓	✓		✓		
Instrumentation				✓		✓	
Earth bonding					✓		
Tank vents				✓			
Fire detection and fighting equipment					✓		
Staff competence, covering:							
Selection of compatible tank		✓		✓	✓		
Selection of route and tank with adequate capacity						✓	
Driver error			✓				✓
Correct coupling, opening/closing valves, starting pumps etc				✓			✓
Suitable skills and experience to undertake inspection and maintenance tasks	✓	✓	✓	✓	✓	✓	✓
Emergency arrangements					✓		

Probabilistic risk analysis

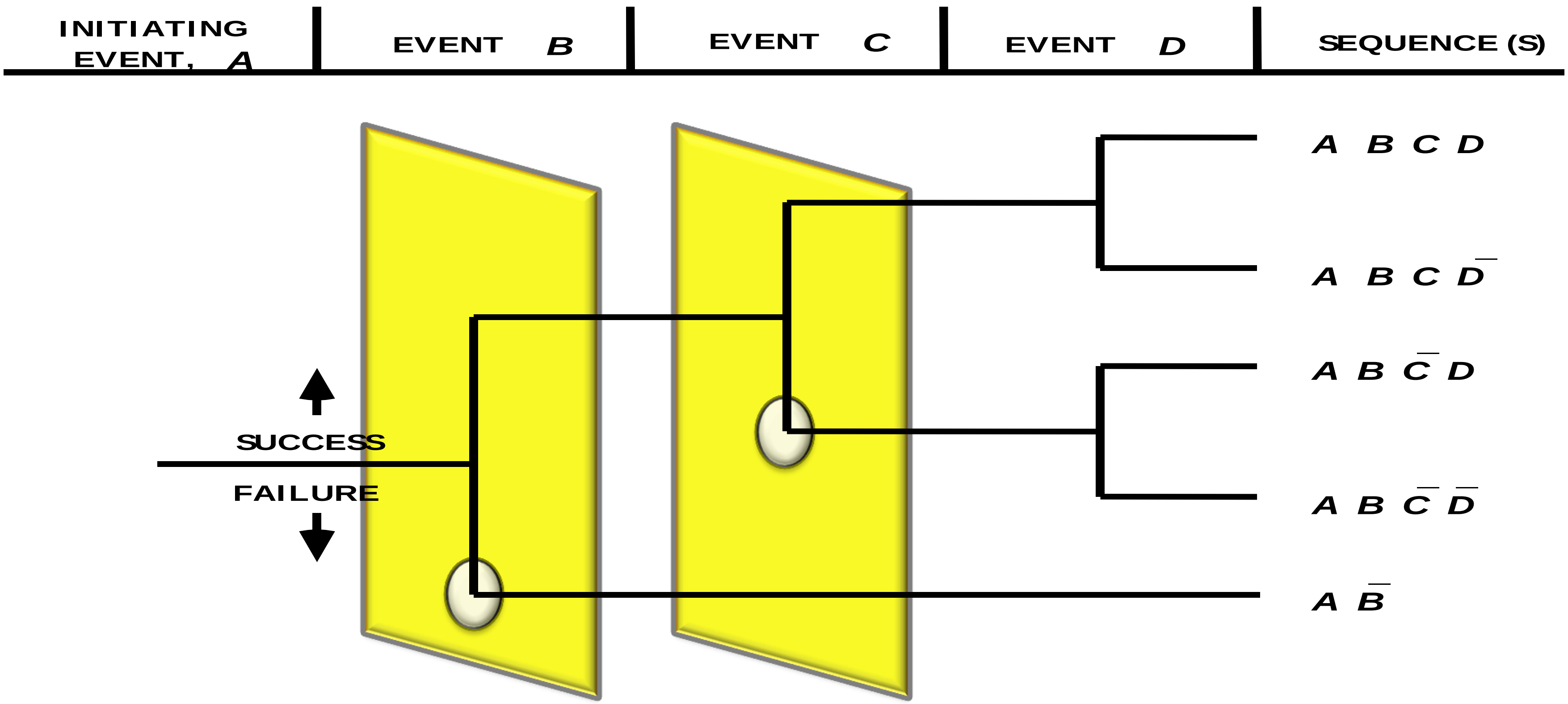
- Incidents and accidents postulated as initiating events
    - selected according to their frequency, estimated from general industrial experience
- Considers equipment failures and human errors
- Well defined risk models
    - How the initiating events can lead to uncontrolled release of radioactive materials outside the plant

Event trees



- Events: safety features and protection systems
- Activated by the operators or by automation

Event trees



Events = Barriers

Risk Assessment vs. Indicators process

1. What can go wrong? Initiating events (e.g. small-break loss of coolant) Event sequence logic 2. How frequently does it happen? Quantification 3. What are the consequences? Consequence modeling	1. What can go wrong? Hazard scenarios (e.g. leakage) and their causes (e.g. valve wear) List of generic causes (wear, corrosion) 2. What control systems control these risks (risks = generic causes) 3. What are the outcomes of and critical parts of these systems? Identify leading and lagging indicators

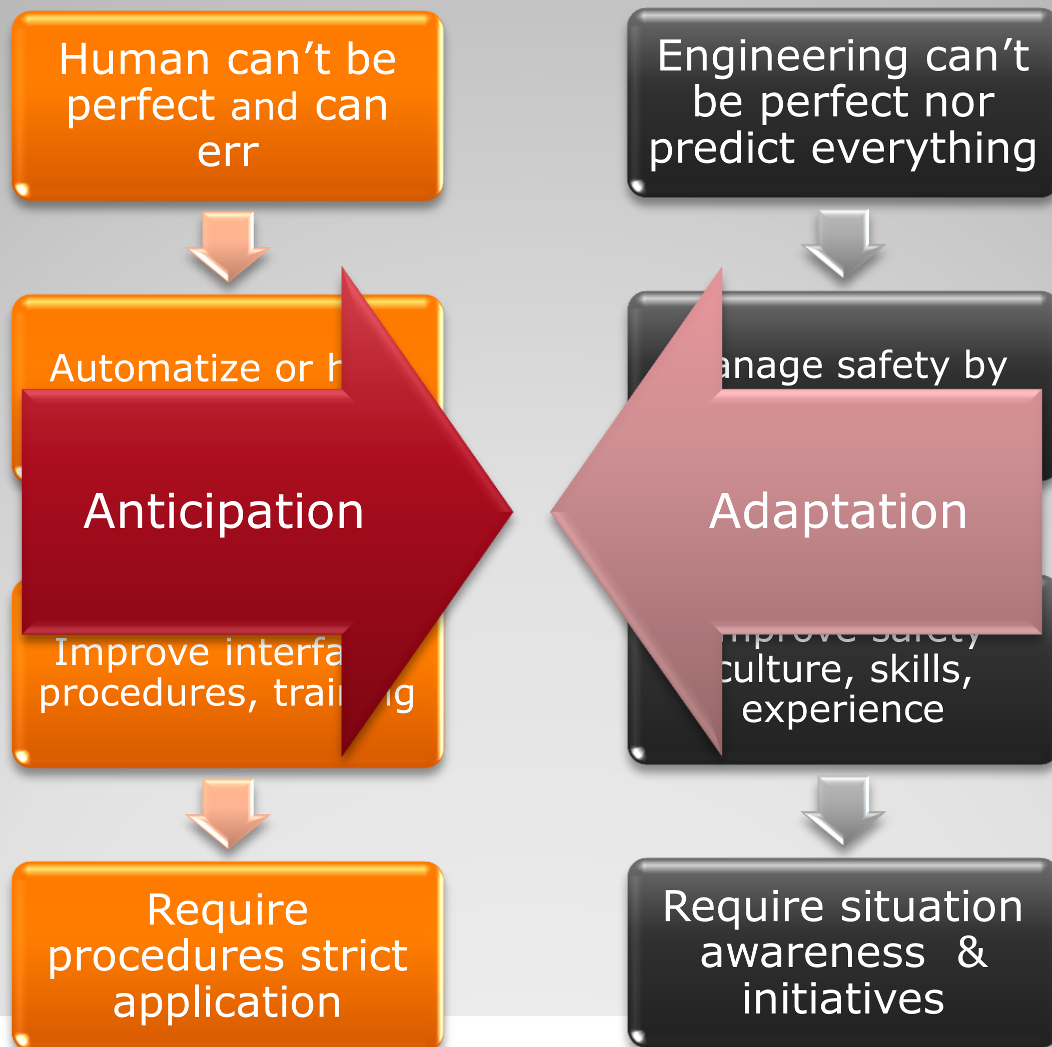
Human Reliability Analysis (HRA)

- Probability Risk Analysis estimates the reliability of the barrier functions (engineered safety features)
- Some of these functions are executed by operators
- HRA assess the reliability of the operators
  - Takes into account the task difficulty
  - And the context of performance
- Organizational influences are not accounted for explicitly
  - E.g. Procedures are correct

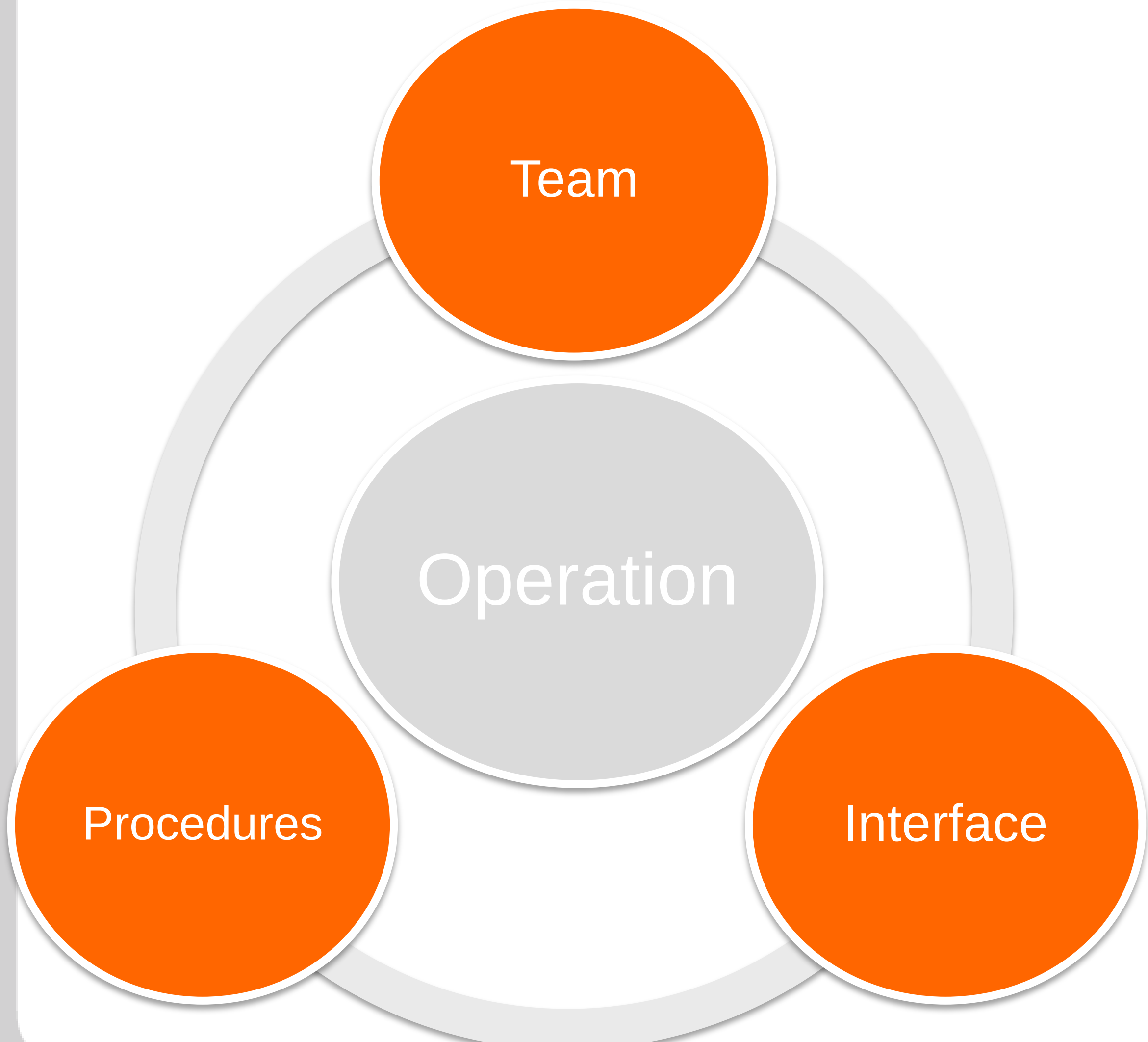
First Generation: operators as components

- Operator = machine
  - Follows procedures
  - Has known limitations
  - Is unreliable
- Human failures:
  - Individual errors
  - Operator directed by interface and procedures
  - If response is not as expected→ **Error**

Humans role in safety: two views

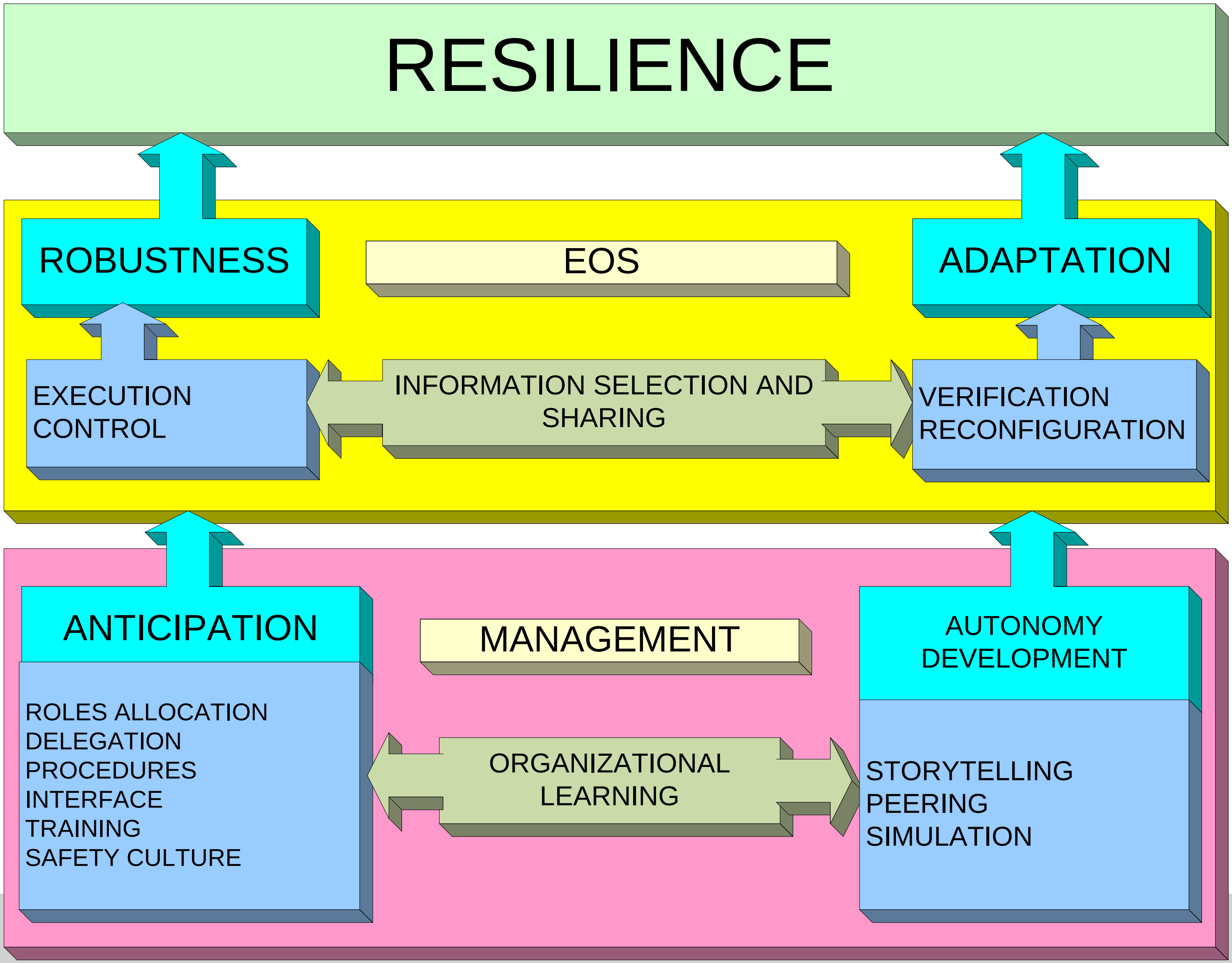


Second generation: The Emergency Operating System



- Emergency operation results from the interaction between **operators, procedures and interfaces**
- The EOS is a **cognitive and distributed system**
  - It uses prior knowledge and produces new knowledge in real time
  - Knowledge is deposited in and elaborated by different system components
- **Technology and organization are joined**

Model of Resilience in Situation

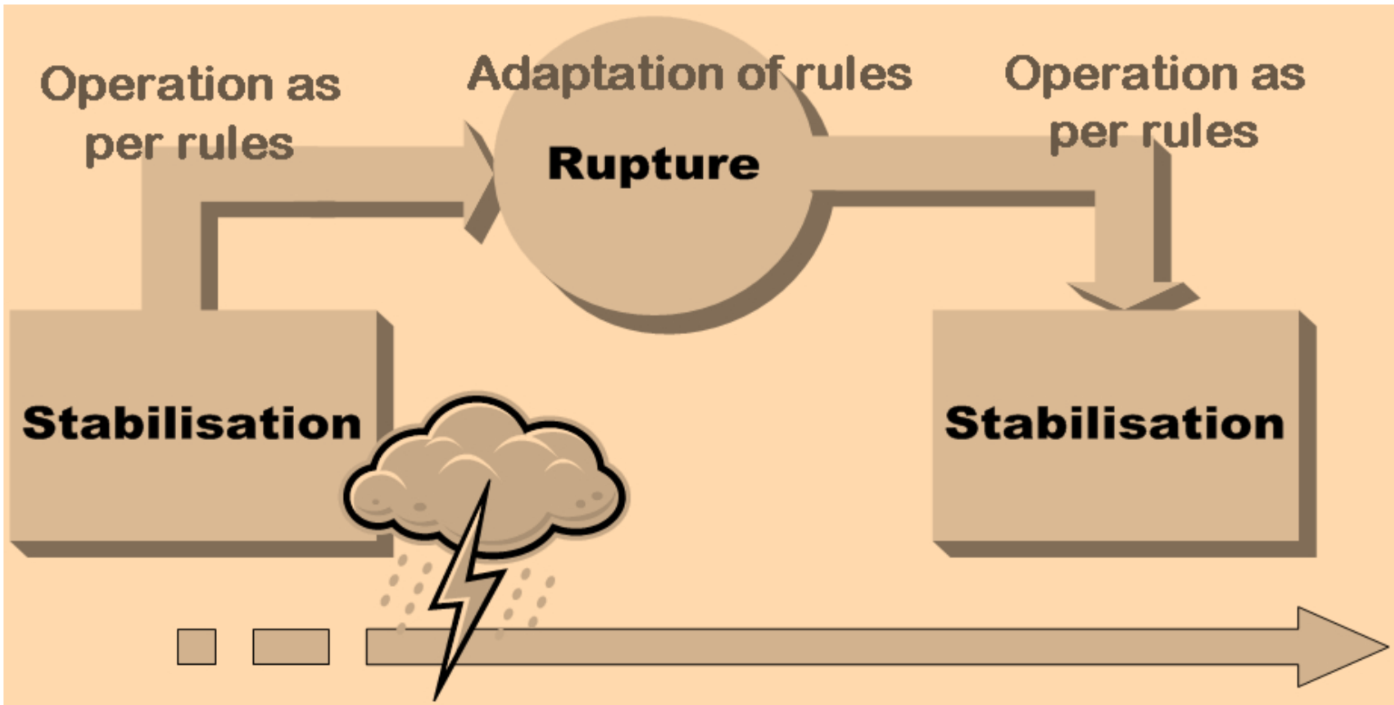


The MRS includes organizational and the team influences in risk analysis

- Today:
  - Performance Shaping Factors, e.g., team dynamics
  - Analysts' knowledge of the plant/organization

- The EOS approach:
  - Produces a model of Organizational and teamwork influences on control room operators capabilities

The dynamics of emergency operation



Central concepts: Rules and In-situation Regulation

MRS model: combines the two views

Human can't be perfect and can err

Automatize

interface, procedures training

Require procedures strict application

Engineering can't be perfect nor predict everything

anage safety

lture, skills, experience

Require situation awareness & initiatives

Anticipation

Adaptation

Example :

Follow strictly the procedure. No deviations, no violations.

Rule

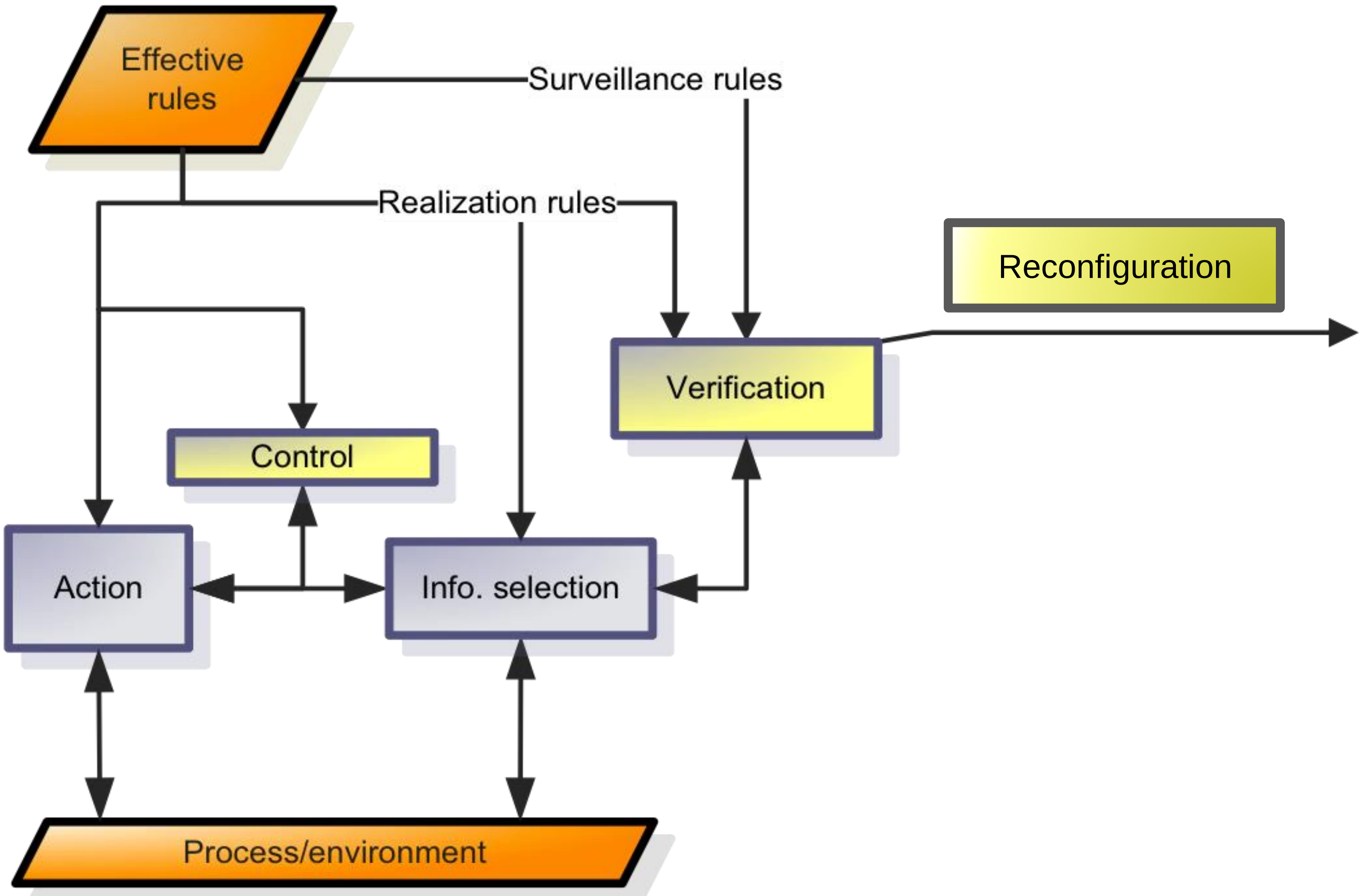
AND

Be able to the operate without or against the procedure

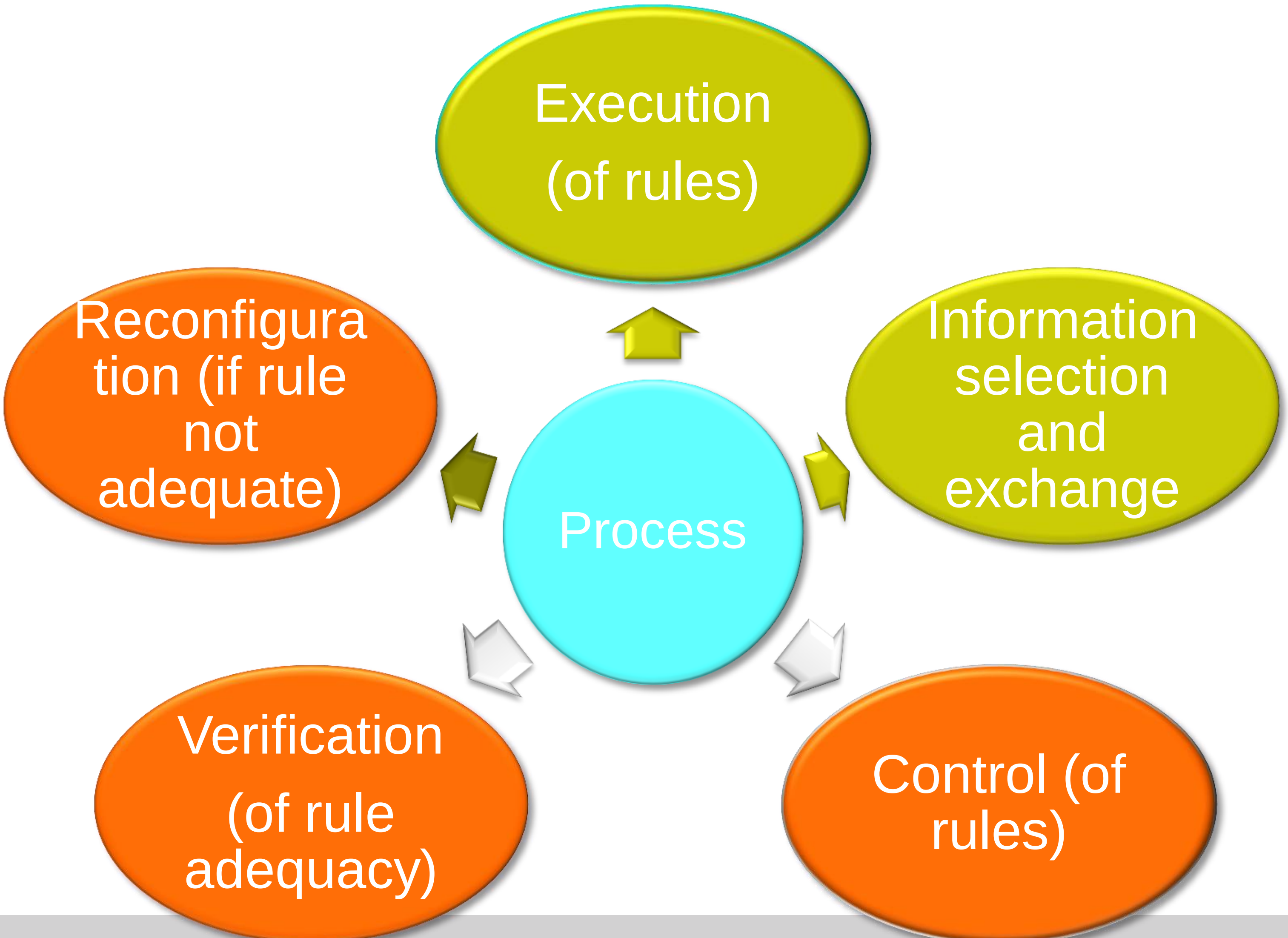
Rule

Two opposite rationalities

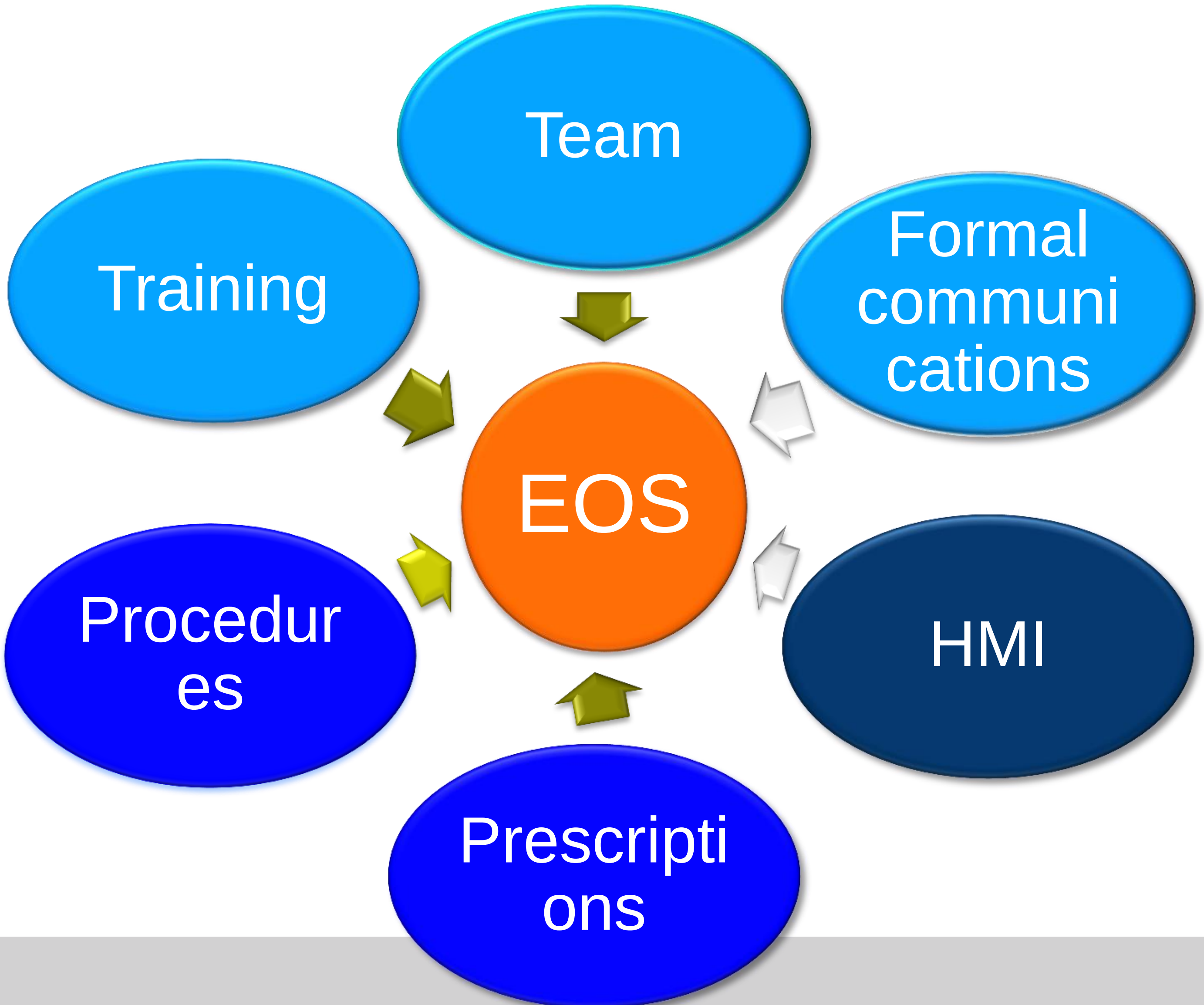
The functions of an EOS



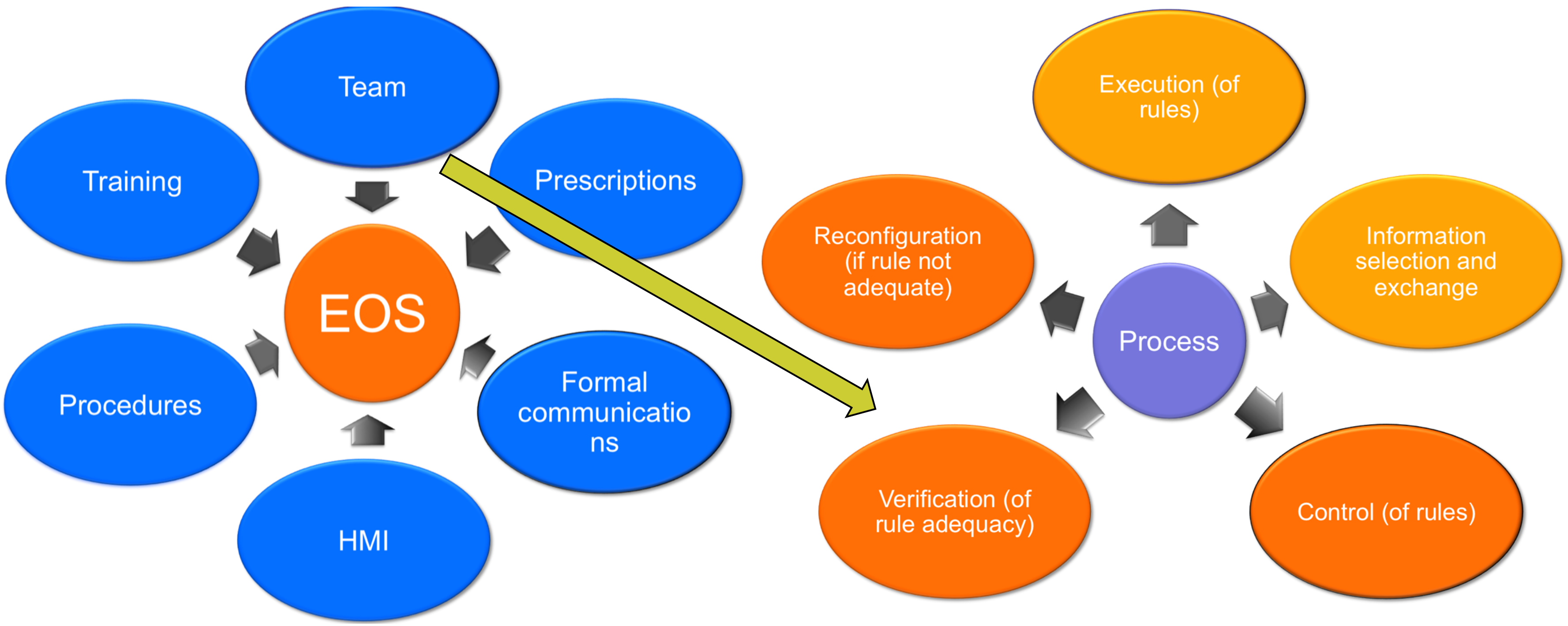
Five EOS functions



The EOS characteristics



Example

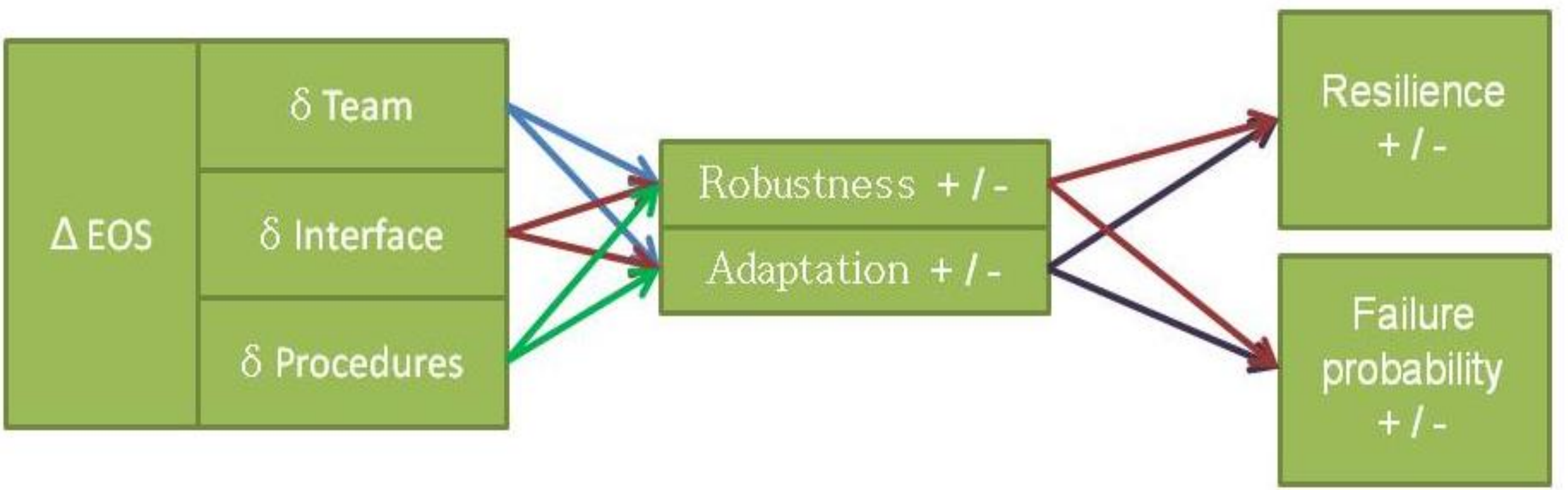

Team
Training
Prescriptions
EOS
Procedures
Formal communicatio ns
HMI
Execution (of rules)
Reconfiguration (if rule not adequate)
Information selection and exchange
Process
Verification (of rule adequacy)
Control (of rules)

Team Influences on Verification

	Openess/Democracy	Supervisory role	Team size
Redundant checks			To look for extra information To assess reliability of cues
New info and anomalies		To keep track of reminders	
Global overview	To question current mission To evaluate procedure is appropriate To reconsider priorities	To keep global overview To evaluate procedure is appropriate To look ahead in procedure	

Applications: Comparing EOSs

- Evaluate the effects of EOS differences on resilience and failure probabilities
- Relate data collected in one organization/reactor to a different one
- Integrated system validation: Same EOS before/after modification



Status

- The EOS approach has been developed by EDF, with support form PSI and IFE
- Closely related to EDFs HRA method MERMOS
- EDF is using the Delta-approach in the design and evaluation of a new reactor (EPR)
- Still under developement

Conclusion

- **It is possible to account for the effect of organizational barriers on safety**, provided that
- It is about ultra-safe system:
  - Individual errors are recovered, failure is collective
  - Failures are wrong diagnoses or strategies in unusual situations, not slips and lapses
  - Extensive preparedness (e.g. procedures, training)
- There is substantial time from the initiating event up to the point at which harm occurs
- There exist a risk model (e.g. the PRA)

Thanks for your attention

2nd generation HRA: MERMOS

- Joint-system perspective
  - Failure is mismatch not information overload
  - Focus on team not individual and attention/memory errors
- Close integration with HF
  - Rich inputs for error identification and reduction
  - Qualitative insights conveyed in the application
  - More than numbers in PRA

ITEM 1) HEP of HFE1A1

Probability of mission failure (HEP):	4,6 E-2
Uncertainty:	

The probability of the mission is the sum of the probabilities of all the "MERMOS scenarios of failure" (including residual probability) : see item 2

ITEM 2) SUMMARY OF MOST INFLUENCING FACTORS

List of the MERMOS scenarios leading to the failure of the HF mission (the scenarios found by the analysts are detailed in item 3)

Function	Prob.	N°	Scenario
Strategy Total: 99,5 %	0	1	**Not relevant for Hammlab**
	2,4 E-2	2	**No strategy** - The system scrupulously follows the EOPs spending time on points irrelevant to the situation and doesn't complete feed and bleed on time
	0	3	**Not relevant for Hammlab**
	8,1 E-5	4	**Erroneous strategy** - The system spends time in its attempt to recover the condensate pumps system and puts off too long completion of feed and bleed
	2,2 E-2	5	**Erroneous strategy** - In its hope to recover the AFS the system delays too long the completion of feed and bleed
Action Total: 0 %	0	6	**Not relevant for Hammlab**
	0	7	**Not relevant for Hammlab**
Diagnosis Total: 0,5 %	0	8	**Not relevant for Hammlab**
	2,4 E-4	9	**Erroneous state diagnosis** - The system doesn't perform the state diagnosis on time
Residual probability	1,0 E-4		(this probability represents all the scenarios that we are not able to imagine: we assign the upper value given the lack of data))

Levels of protection

Levels	Objective	Essential Means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, testing, limiting & protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant release of radioactive materials	Off-site emergency response