

# **Tools of safety management**

**MEC-E3004 Safety management in complex  
sociotechnical systems**

**Teemu Reiman**

# MEC-E3004 Safety management in complex sociotechnical systems

1. 2.3. Introduction and the basic concepts of safety management
2. 9.3 Basic concepts: Human Factors and Safety Management (Douglas Owen)
3. 16.3 Accident models
4. 23.3 Accident case (BP Texas City refinery explosion in 2005)
  - Mid-term assignment
5. 30.3 Organizational learning

## 6.4 NO LECTURE

*13.4 Returning the mid-term assignment*

6. 13.4. Safety culture
7. 20.4. Safety leadership
8. 27.4. The basic principles of safety management
9. 4.5 Safety management systems
- 10.11.5. Tools of safety management I**
- 11.17.5 Tools II and future of safety management (TIME!)
- 12.25.5 Recap and Q&A
  - Deadline for returning the paper 31.5.2023

# Learning logs

- Pros and cons of integrated versus separate management systems? When to integrate and how?
- How “living” should the SMS be?
- What are the main challenges standing in the way of the successful integration of safety management systems into the business processes of an
- The need for a “macroscope” was borrowed from a book: James Bridle. *Ways of Being. Animals, Plants, Machines: The Search for a Planetary Intelligence*. Penguin Books, 2023.

## **Recap: Safety management systems**

# Potential drawbacks of safety management systems (Accou & Reniers 2020)

- The SMS can be made too burdensome and complex, resulting in processes that are incompatible with an organization's core activities and going against the common sense found in local practice
- SMS is often perceived as too normative and bureaucratic, pushing companies directly to a “work as imagined” and compliance-focused perspective
  - They may end up being a paper-based system specifically developed for demonstrating compliance with the regulatory framework
  - Since they are verifiable regulators also typically require companies to have one => potential for vicious circle where regulator requires verifiable & quantifiable performance, and the company builds simplified SMS with simplistic indicators detached from the workplace reality
- SMS is based on a top-down control approach where information about the field is gathered and analysed by the “controller”, who then in turn plans, implements and follows up corrective actions
  - The continuous self-organizing (cf. CAS) in the field is seen as a threat, not as a potential safety mechanism
  - By putting the focus on the organization and processes, focus on operational activities (deference to expertise) may suffer => also the regulatory focus shifts from verifying technical issues to verifying processes
- Despite being a formal and systematic way of managing safety, there is large variance in safety management systems in practice

# Typical issues covered by safety management systems

1. Management commitment
2. Employee involvement
3. Organizing
4. Risk and hazard identification and assessment
5. Hazard prevention and control
6. Communication
7. Competence management
8. Monitoring and assessment
9. Learning from experience
10. Continuous improvement

# Typical issues covered by safety management systems

1. Management commitment
2. Employee involvement
3. Organizing
4. Risk and hazard identification and assessment
5. Hazard prevention and control
6. Communication
7. Competence management
8. Monitoring and assessment
9. Learning from experience
10. Continuous improvement

As the safety management system is only a framework for organizing, these ten activities / issues can be carried out in various ways and each issue includes multiple methods based on different premises – today we take a look at some of them

**Safety management systems are a collection of tools, methods and practices for systematic identification, evaluation and management of safety issues**

**They contain various tools and methods based on several safety management principles**

**Understanding of the different safety management principles as well as understanding of nature of complex sociotechnical systems is required to properly use the tools of safety management**



**How to adapt safety management to the  
sociotechnical system requirements – which tools to  
use and how?**

# Three models of managing safety critical organizations (Amalberti 2013)

HRO, High Reliability Organization (P.Schulman, T.La Porte, K.Roberts; cf. Weick & Sutcliffe 2007)

- the 'HRO model' of safety with its emphasis on both self-organizing and standard operating procedures, combined with risk-averse operations
  1. sensitivity to operations (*ie*, heightened awareness of the state of relevant systems and processes);
  2. reluctance to simplify (*ie*, the acceptance that work is complex, with the potential to fail in unexpected ways);
  3. preoccupation with failure (*ie*, to view near misses as opportunities to improve, rather than proof of success);
  4. deference to expertise (*ie*, to value insights from staff with the most pertinent safety knowledge);
  5. practicing resilience (*ie*, to prioritize emergency training for many unlikely, but possible, system failures).
- Military operations during peace time, some nuclear power plants

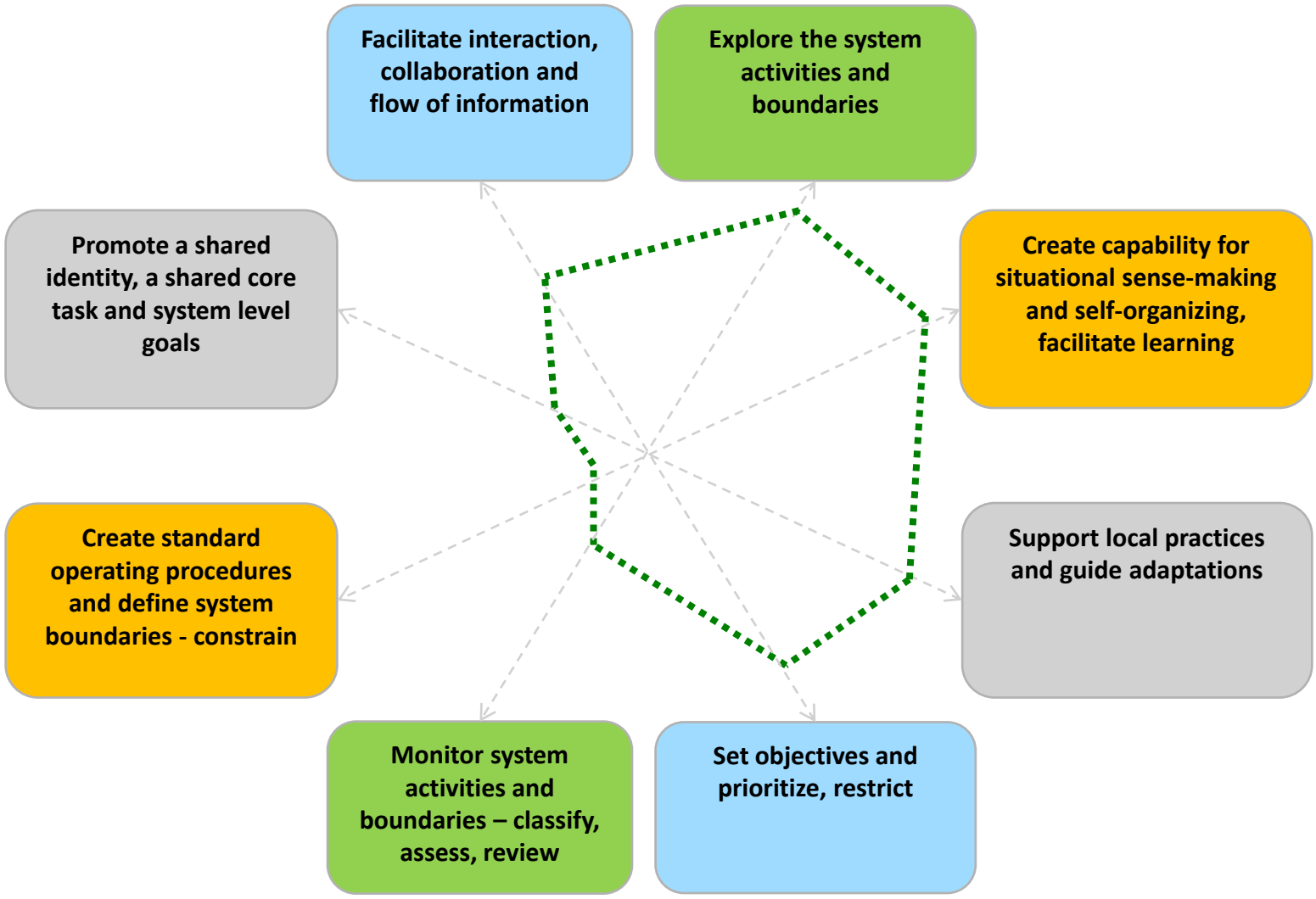
Resilience Engineering (cf. Hollnagel et al. 2006)

- the 'resilience model' of safety: the nature of the activity involves risk taking and individuals' autonomy and expertise take precedence over standards and hierarchy
- Situational adaptation, flexibility, ability to recover from perturbations
- Medicine, maritime, fire fighter etc.

Ultra-safe systems

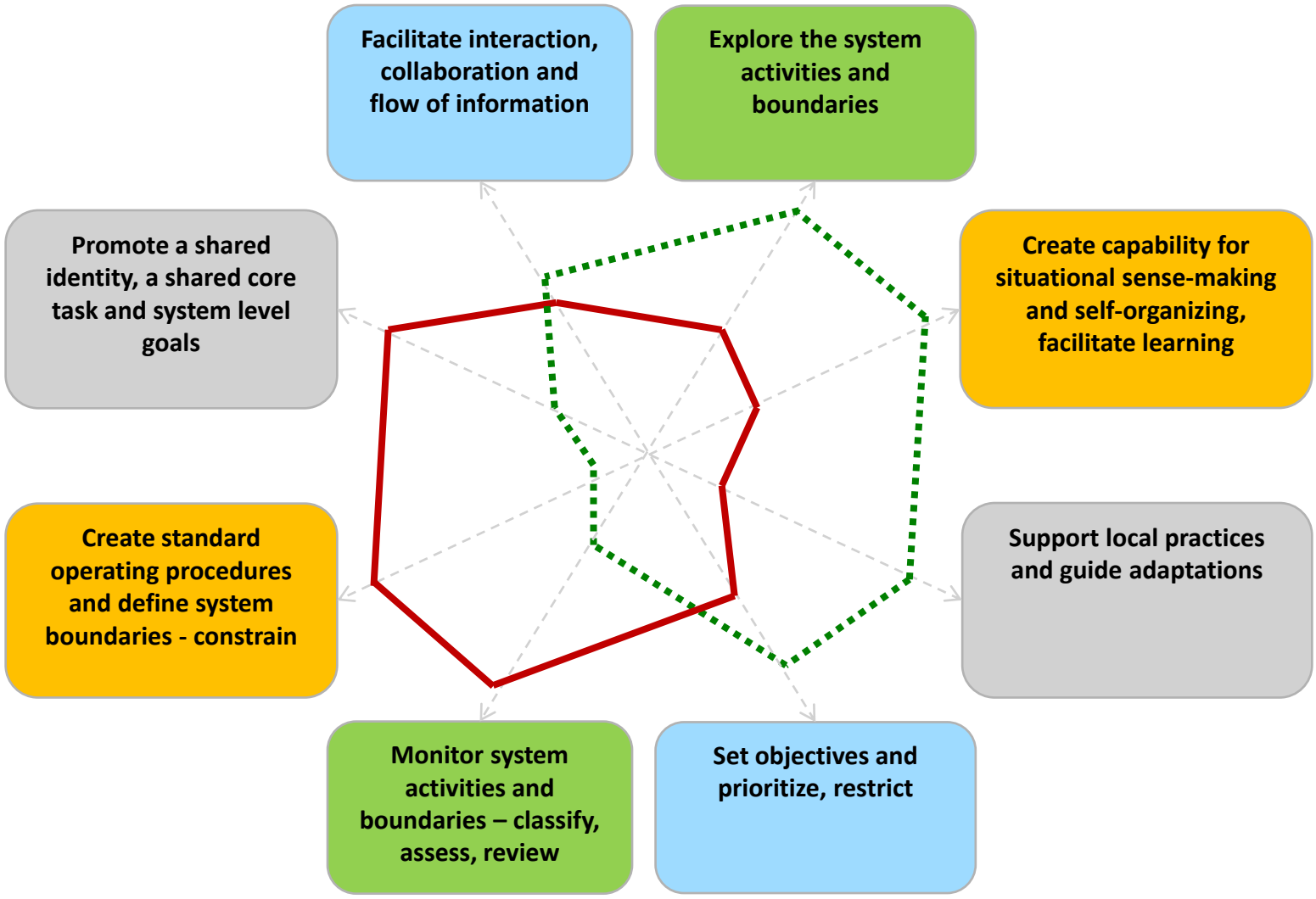
- the 'ultra-safe model' of safety: risk-averse, relying on interchangeable operators and standard operating procedures, acting in stable environments.
- Nuclear power plants and airlines operate according to this model
- Requires stable environment and a well-known process (where there is a possibility to get direct process data)

**RESILIENT MODEL** .....



**ULTRA SAFE MODEL** —————

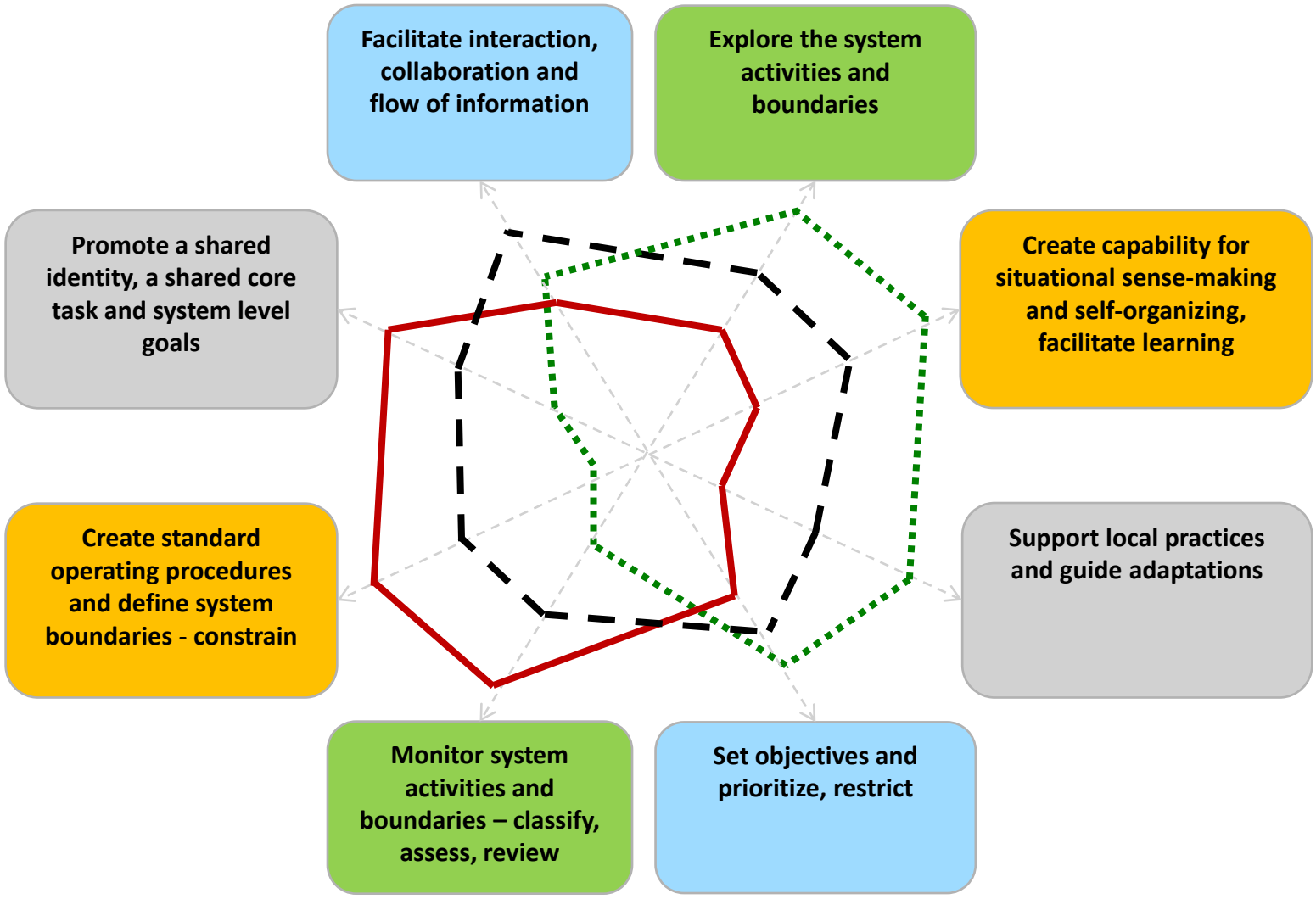
**RESILIENT MODEL** ······



**ULTRA SAFE MODEL** —————

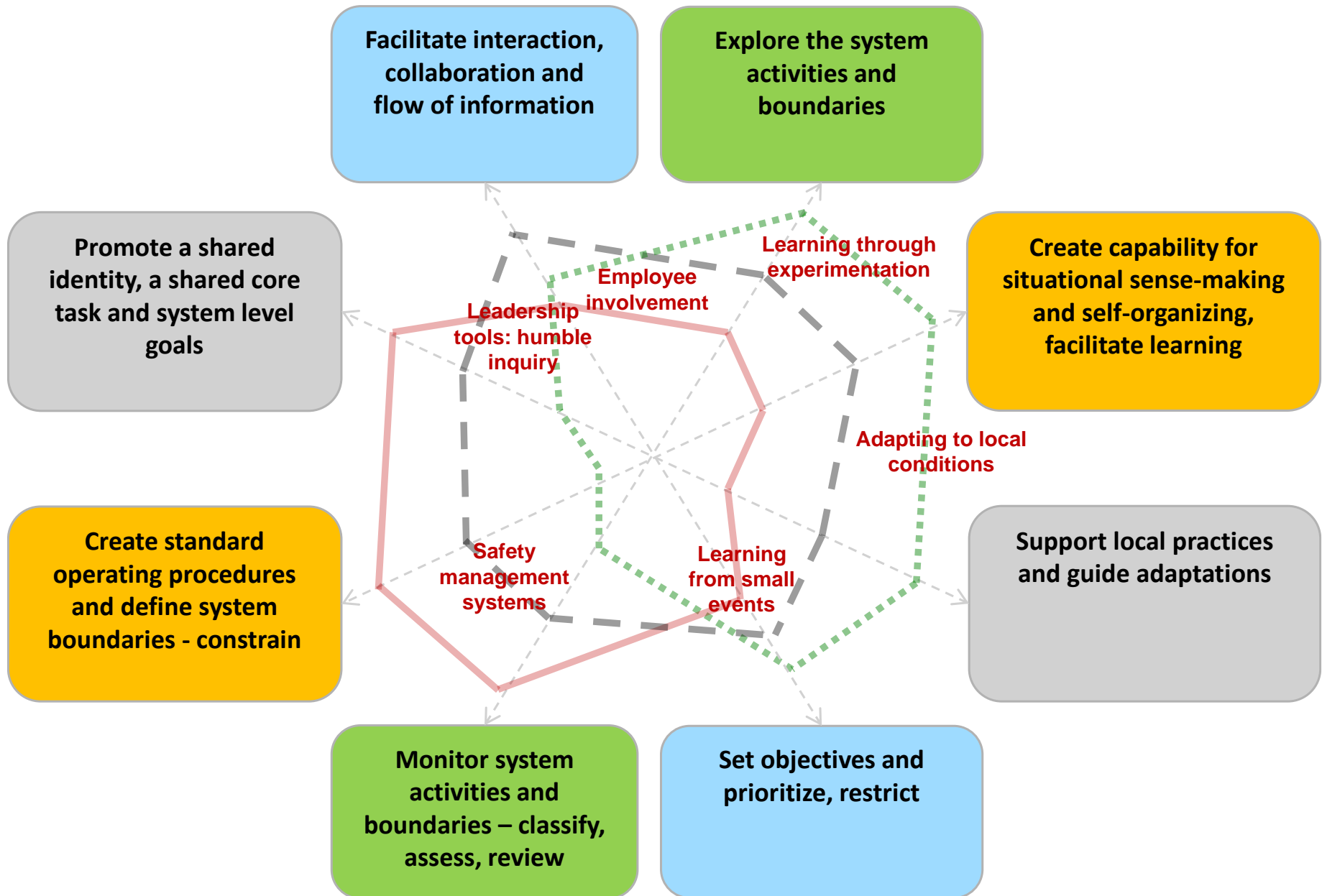
**HRO MODEL** - - - - -

**RESILIENT MODEL** ······



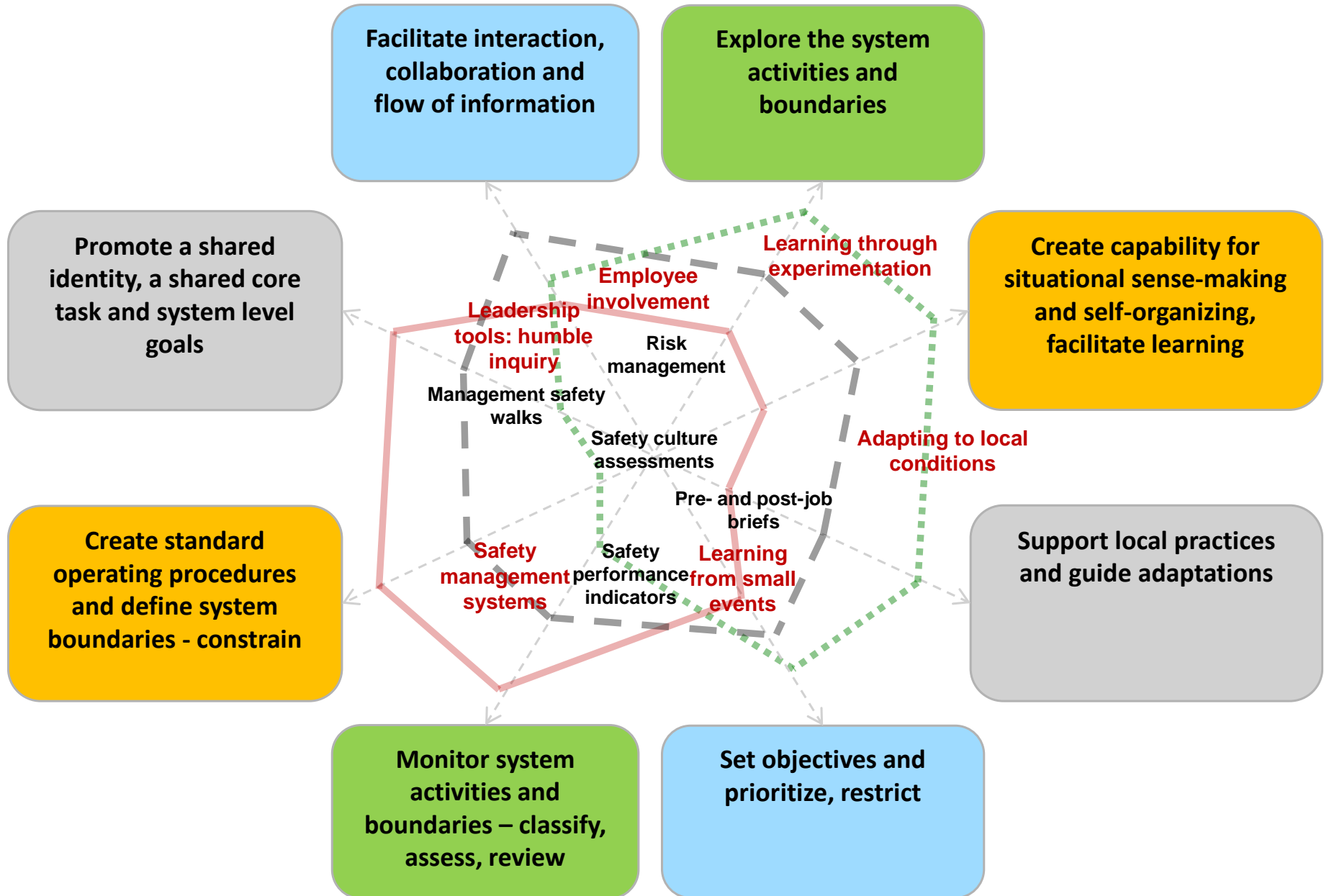
# We have already discussed many tools of safety management

Today we look at a few other useful tools applicable for most types of sociotechnical systems



# We have already discussed many tools of safety management

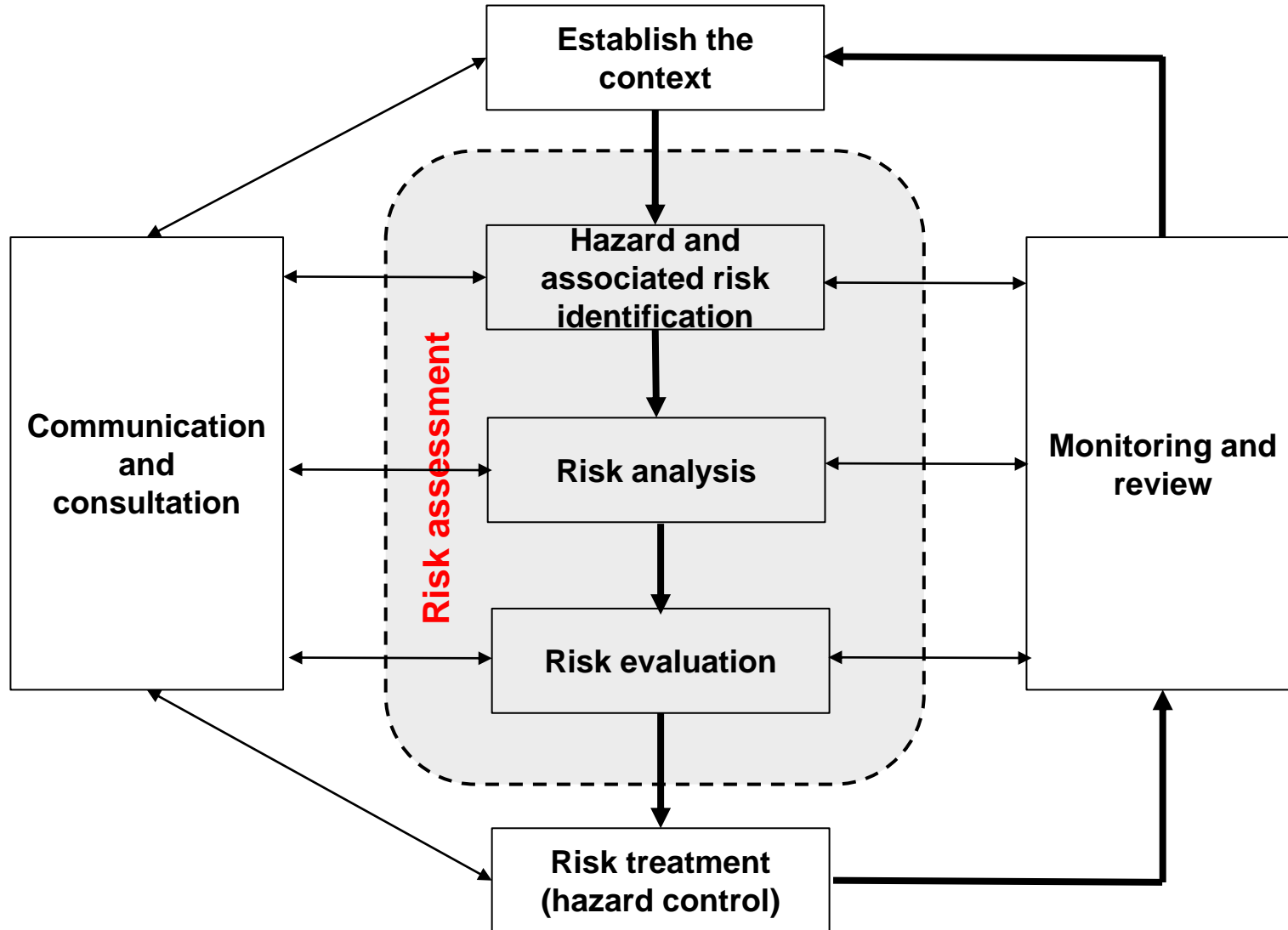
Today we look at a few other useful tools applicable for most types of sociotechnical systems



# **Risk management**



## The general risk management process based on ISO 31000, as applied in the safety context



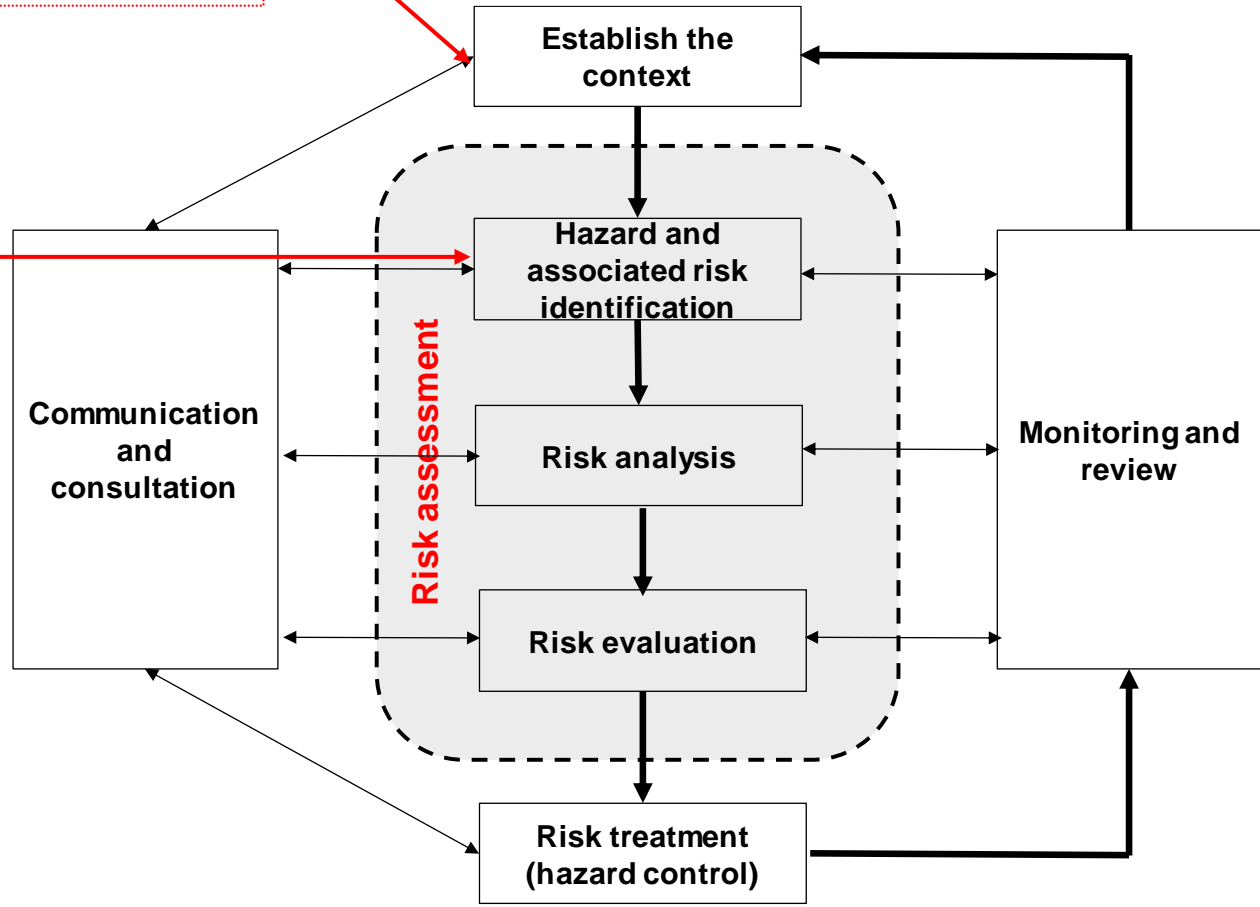
The four main risk categories of risk are *hazard risks*, such as fires or injuries; *operational risks*, including turnover and supplier failure; *financial risks*, such as economic recession; and *strategic risks*, which include new competitors and brand reputation. In safety management the hazard risks are in main focus, but other risk types can also contribute to hazard risks.

# The general risk management process based on ISO 31000, as applied in the safety context

Establishing the context includes planning the remainder of the process and mapping out the scope of the exercise, the identity and objectives of stakeholders, the basis upon which risks will be evaluated and defining a framework for the process, and agenda for identification and analysis.

Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.



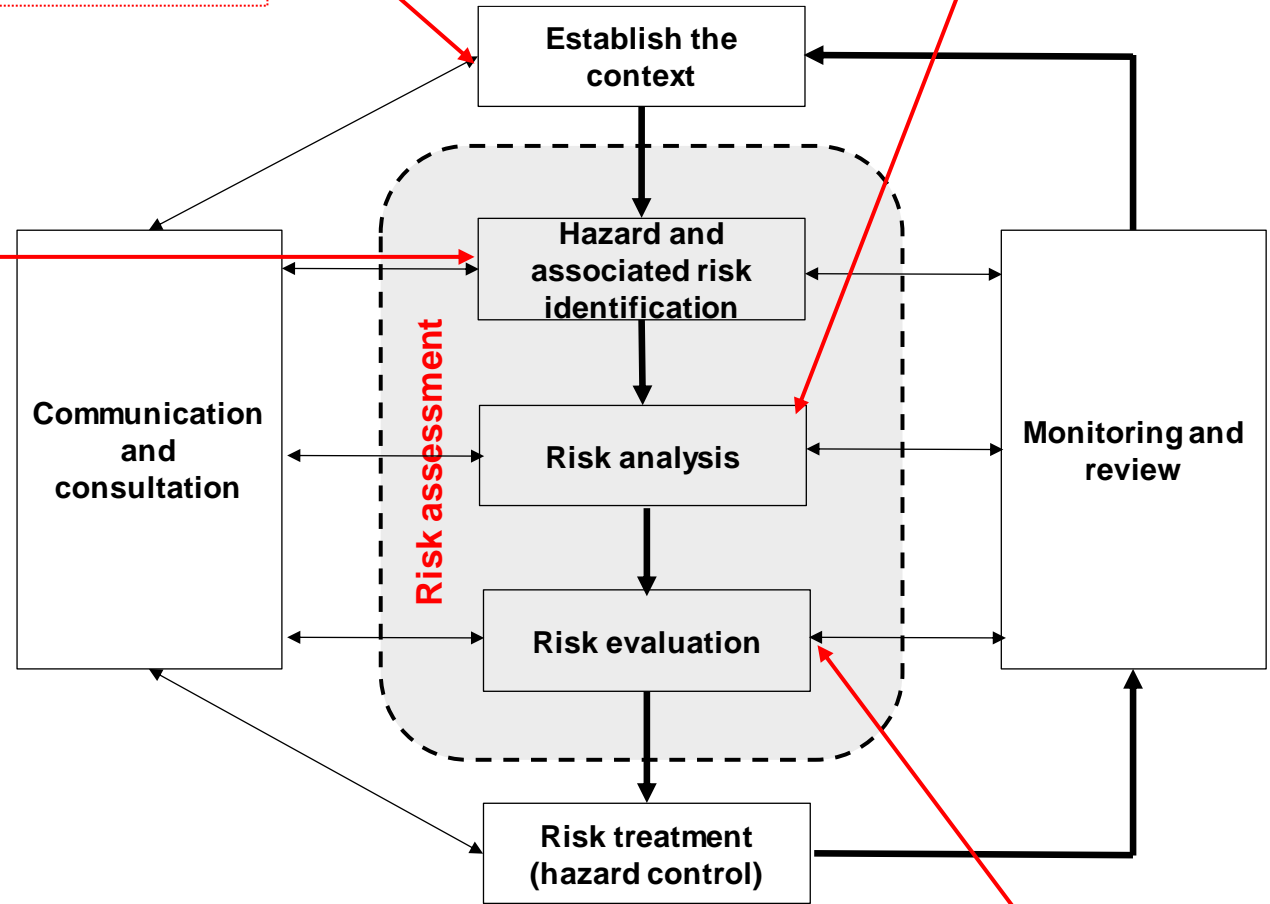
# The general risk management process based on ISO 31000, as applied in the safety context

Establishing the context includes planning the remainder of the process and mapping out the scope of the exercise, the identity and objectives of stakeholders, the basis upon which risks will be evaluated and defining a framework for the process, and agenda for identification and analysis.

Risk analysis determines the significance of any identified risk factors discovered in the risk assessment process and provides a quantification of risk as the product of risk likelihood and impact.

Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.



Risk evaluation refers to the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

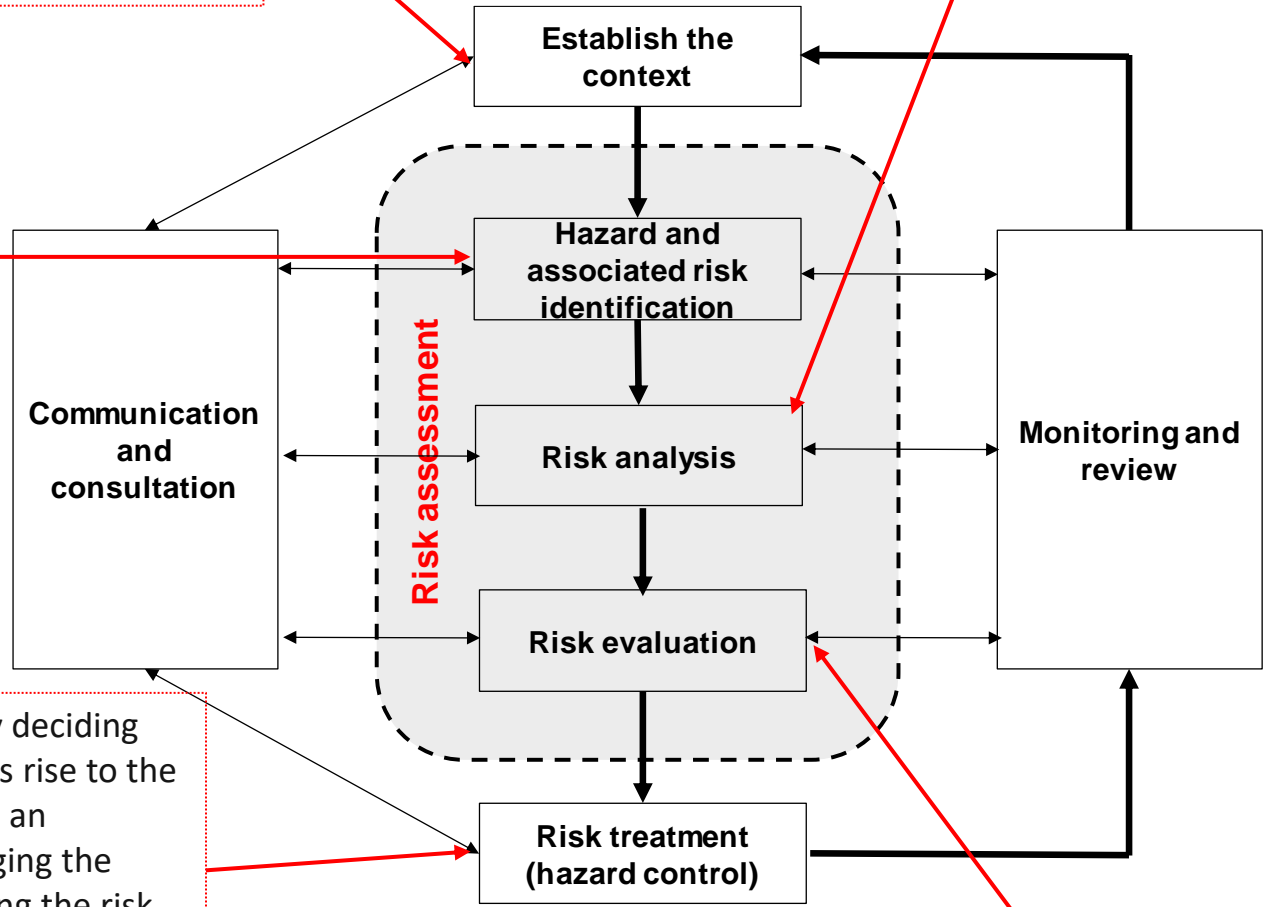
# The general risk management process based on ISO 31000, as applied in the safety context

Establishing the context includes planning the remainder of the process and mapping out the scope of the exercise, the identity and objectives of stakeholders, the basis upon which risks will be evaluated and defining a framework for the process, and agenda for identification and analysis.

Risk analysis determines the significance of any identified risk factors discovered in the risk assessment process and provides a quantification of risk as the product of risk likelihood and impact.

Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.



Risk treatment can involve: 1) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, 2) taking or increasing risk in order to pursue an opportunity, 3) removing the risk source, 4) changing the likelihood, 5) changing the consequences 6) sharing the risk with another party or parties (including contracts and risk financing); and 7) retaining the risk by informed decision.

Risk evaluation refers to the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

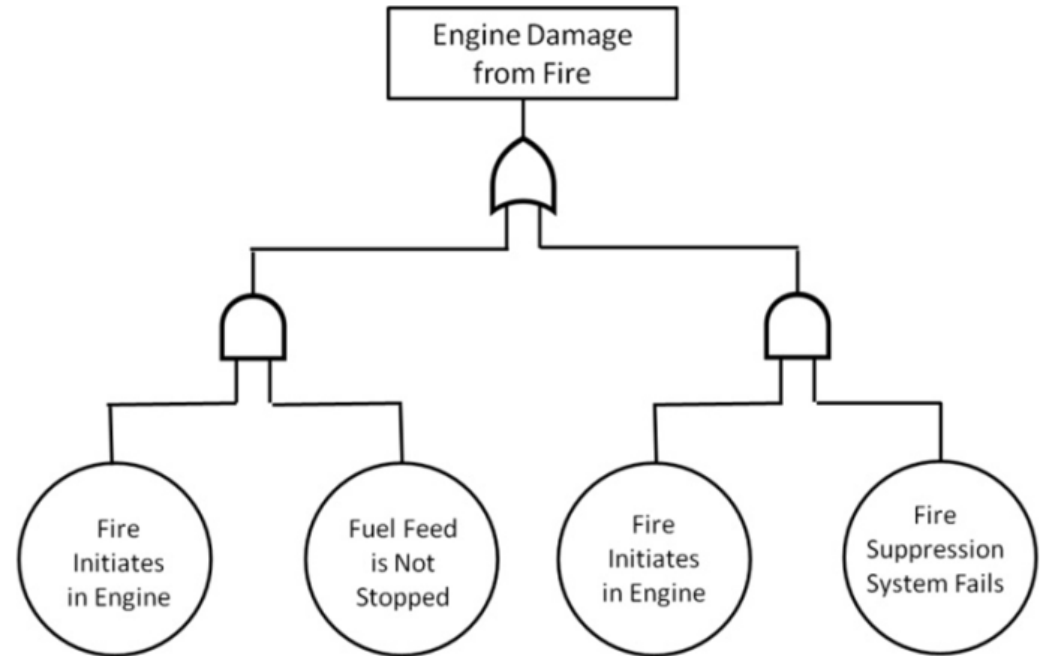
# Tools for hazard identification & risk analysis

(Amalberti 2013; Manuele 2013; Hardy 2014)

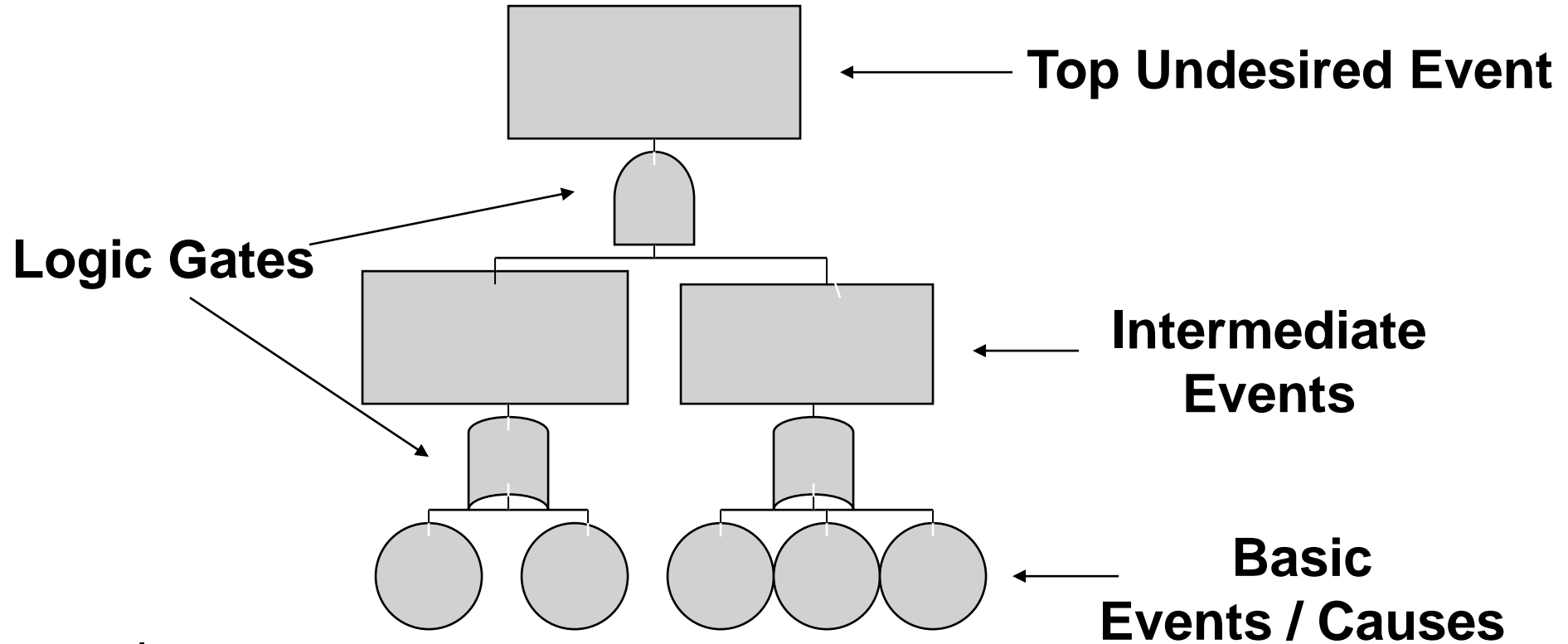
- Hazard identification
  - Process analysis
  - Job hazard analysis
  - Task analysis
  - Functional Hazard Analysis (FHA)
  - Preliminary Hazard Analysis (PHA)
  - Hazard and Operability Study / Analysis (HAZOP)
  - Brainstorming / analysis sessions
- Risk analysis
  - Failure Modes and Effects Analysis (FMEA)
  - Fault tree analysis (FTA)
  - Event tree analysis (ETA)
  - Risk rating matrixes


# Fault tree analysis

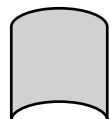
- Analysis starts from failure
  - A top-down deductive method aiming to answer the question “what will cause the given hazard to occur”
- Provides qualitative and quantitative measures of the likelihood of a failure and identifies the causes leading to the failure
- Does not help in identifying all possible hazards, needs FMEA etc to help
- The logic tree limits possibilities to model complex system phenomena
- Is used in system engineering to understand how systems can fail and what are the best ways to reduce risk
  - Changing OR gates to AND gates, or adding AND gates



# Symbols used in fault trees

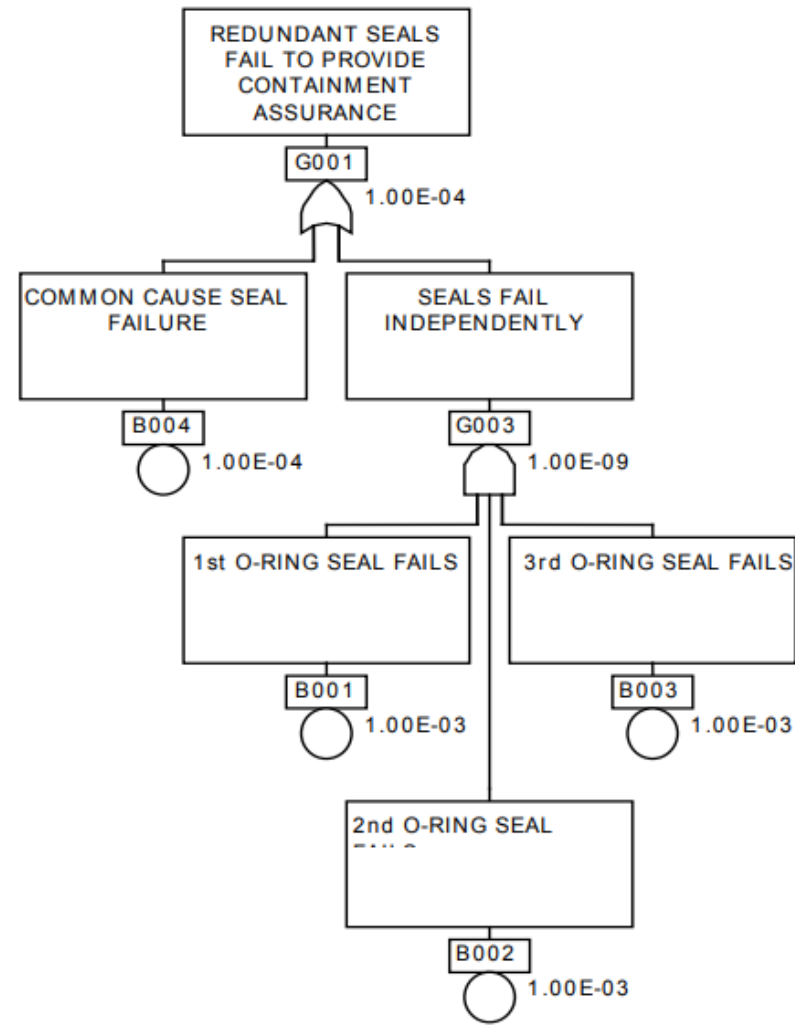


 = and

 = or

# Fault tree analysis

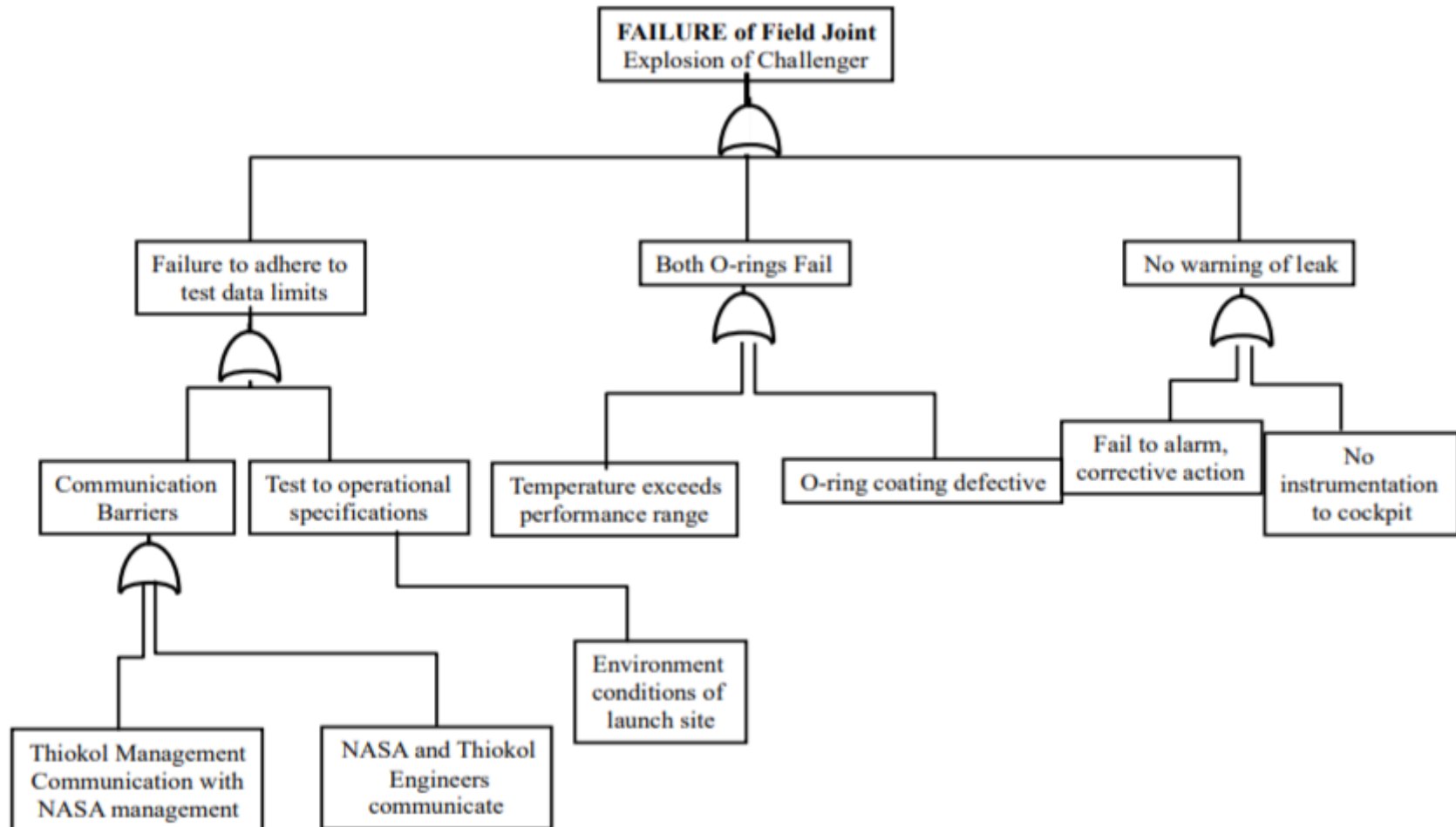
- First developed to evaluate the Minuteman I Intercontinental Ballistic Missile Launch Control System in the 60s
- Boeing started utilizing FTA to civil aviation in the late 60s
- Nuclear adopted the method after the Three Mile Island accident
- NASA adopted the method after Challenger accident
  - NASA used qualitative FMEA before, since first FTAs done during the Apollo mission led to too low probabilities for mission success
- Nowadays used in many industries, including software development



NASA 2002



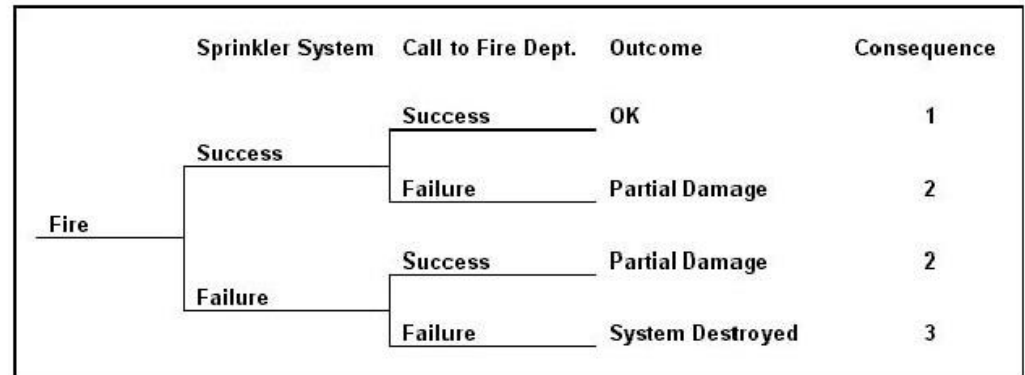
# FTA of SRB failure in Challenger (Jenab and Moslehpour 2016)



# Event tree analysis

- Analysis **starts with a particular event** and then defines the possible consequences that may occur
- Explores responses through a single initiating event and lays a path for assessing probabilities of the outcomes and overall system analysis
- Each branching point on the tree indicates a controlling point, where a success or failure leads to specific scenarios
- Can be used to estimate the probabilities of different outcomes associated with the particular event
- Developed in the nuclear industry in the 70s to complement the fault tree analysis

## Event tree analysis of a fire



# Example (from [www.unitingaviation.com](http://www.unitingaviation.com)) of risk matrix for deciding the risk score

## RISK MATRIX EXAMPLE-INCHEON AIRPORT

### Severity table-Incheon Airport

Number	Severity	Loss	Meaning
5	Very High	Human Loss	Casualties are more than 10 people
		Hardware Loss	More than 10 million dollars
		Operational Loss	Airport Close or airport operation suspension
4	High	Human Loss	Casualties are 1 to 9 people
		Hardware Loss	More than 1 million and less than 10 million dollars
		Operational Loss	Runway close: more than 24 H, taxiway and apron close: more than 72 h
3	Moderate	Human Loss	Serious Injuries to be hospitalized
		Hardware Loss	More than 100,000 and less than 1 million dollars
		Operational Loss	Runway close: more than 12 H, taxiway and apron close: less than 72 h
2	Low	Human Loss	Light injuries more than 4 weeks medical treatment
		Hardware Loss	More than 10,000 and less than 100,000 dollars
		Operational Loss	Aircraft Operational Delay 3 H or Aircraft operation cancel
1	Very Low	Human Loss	Light injuries less than 4 weeks medical treatment
		Hardware Loss	less than 10,000 dollars
		Operational Loss	No effect airport operation

### Probability table- Incheon Airport

Number	Probability	Meaning
5	Very High	It is expected to happen in a month
4	High	It is expected to happen in a year
3	Moderate	It is expected to happen in 5 years
2	Low	It is expected to happen in 20 years
1	Very Low	It is expected don't happen in 20 years

### Risk Matrix-Incheon Airport

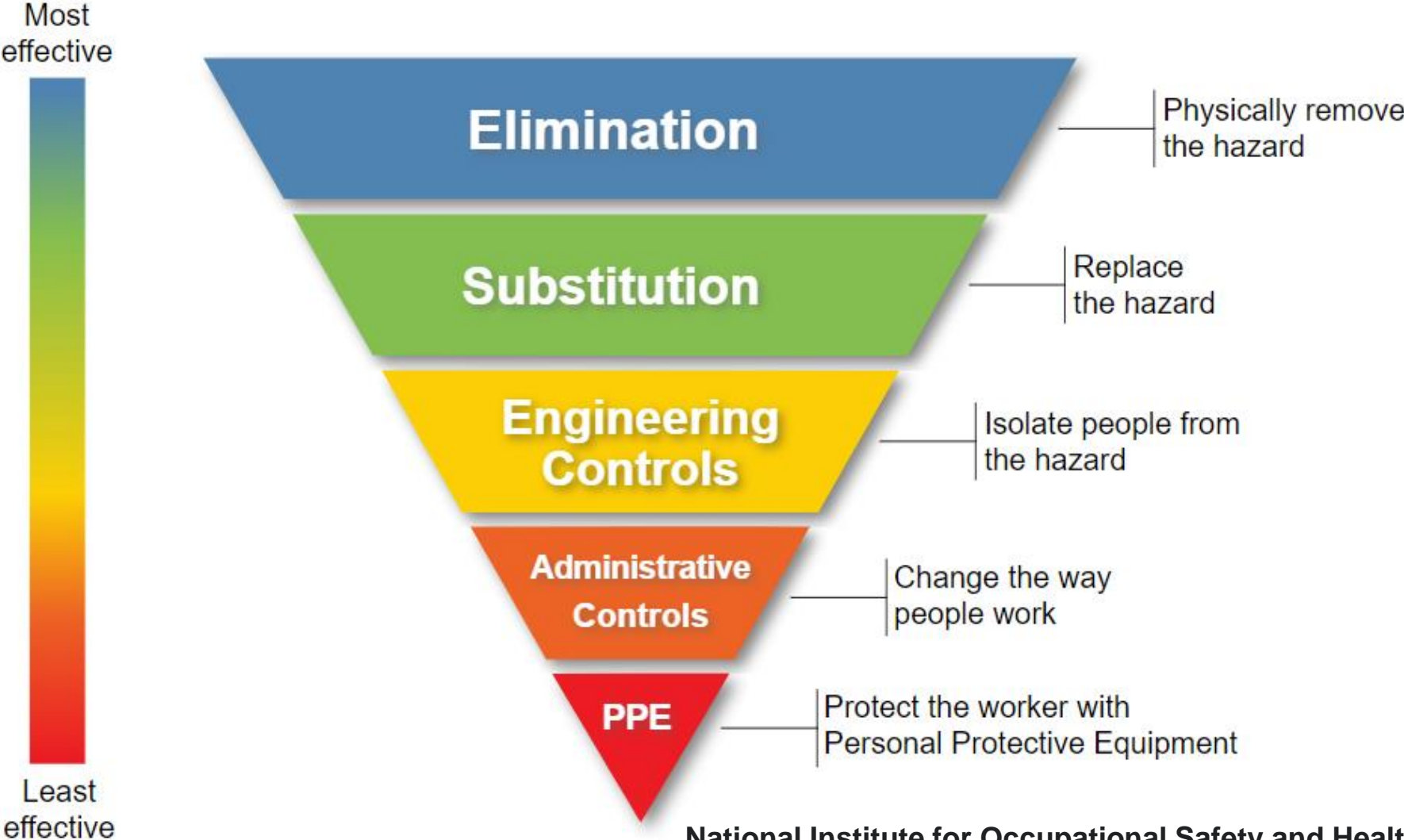
Severity \ Probability	Very High 5	High 4	Moderate 3	Low 2	Very Low 1
Very High 5	Very High (25)	Very High (20)	High (15)	High (10)	Moderate (5)
High 4	Very High (20)	Very High (16)	High (12)	Moderate (8)	Moderate (4)
Moderate 3	High (15)	High (12)	High (9)	Moderate (6)	Low (3)
Low 2	High (10)	Moderate (8)	Moderate (6)	Moderate (4)	Low (2)
Very Low 1	Moderate (1)	Moderate (5)	Low (3)	Low (2)	Low (1)

### Criteria table-Incheon Airport

Level of risk		Acceptability of risk	Criteria for management
16~25	Very high	Intolerable	It is required to be eliminated or reduced to be less than middle risk
9~15	High	Tolerable	It is required to be eliminated or reduced to be less than middle risk
4~8	Middle		It is acceptable, but further action is required
1~3	Low	Acceptable	no further action is required

Note that the severity criteria as well as acceptability criteria are decided by the organization => depends also on what risk is considered, e.g. often in occupational safety analyses very high severity equals 1 fatality

# Hierarchy of controls (NIOSH)



# **Safety performance indicators**

# Leading and lagging indicators of safety performance

- Lagging indicators
  - Reactive, includes (typically) negative outcomes that have already occurred
  - Lagging indicators include incidents and accidents statistics, environmental releases, number of fatalities, frequency of injuries (per work hours), sick leaves, etc.
  - Lost Time Incident Frequency Rate (LTIF) most typical indicator in most industries – allows comparison with other companies
- Leading indicators
  - Proactive in nature, includes (positive) issues that can be observed and recorded (prior to adverse events)
  - Goal is to prevent adverse events before they happen – events that are measured by lagging indicators
  - Examples include training, conducting audits, near misses, risk assessments, safety initiatives

# Challenges with indicators (see e.g. Hopkins 2009, Reiman & Pietikäinen 2012)

- What safety are we measuring? Process safety versus personal safety?
- Are near misses leading or lagging indicators? How about findings in a safety audit (e.g. non-conformities that have not yet caused incidents)?
- The problem of data: the safer the system less data there is to indicate safety (at least in lagging terms)
  - How about safety in e.g. design, construction etc. where the hazards actualize years or even decades later?
- Misuse of the safety pyramid (Heinrich)
  - 300 near-misses – 30 minor incidents – 1 fatality rule does not always apply, and even if it applies in frequency the causal influencing factors may differ
- Reliability of indicator data – e.g. what counts as a minor injury
  - You get what you measure: means also underreporting if the management is only interested in the measure
- Differentiating indicator from the measured phenomena => indicators *tell* something about safety, but they are not safety
- Do all indicators need to be quantitative?
  - Qualitative indicators are often perceived by management to be too vague, when in fact they can be more valid



# Some good safety performance indicators

- Number of safe days – positive indicator telling how many days (per year) the organization has avoided any major incidents (also Productive Days % indicator can be used)
  - Challenge with lost time indicators is that they often restart when something happens (e.g. "number of days without an accident"), potentially hindering reporting
- Number of near-misses reported per hours worked
  - Tells more about openness than about the actual number of near-misses happening
- Backlog of corrective actions / maintenance
  - Tells about organizational priorities and ability of the organization to correct issues on time
  - Also, average closing time of identified issues can be used
- Number of audits, inspections, assessments etc conducted, no of non-conformities identified, backlog of corrective actions
  - Tells about organizational willingness to develop
- Employee turnover
  - Tells about the overall culture and wellbeing of personnel
- Amount of training days per employee
  - Priorities, is the competence of employees kept up
- Employee surveys, e.g. annually
  - Job satisfaction, feedback on performance, relation with immediate supervisor, collaboration, trust in management, perception of management safety commitment psychological safety



## SMART indicators

- **Specific** – It must be clear what exactly the KPI measures
- **Measurable** – The KPI has to be measured according to a defined standard so that the actual value can be compared to normal standard values
- **Achievable** – Every KPI has to target a realistic and feasible goal (nothing is more discouraging than striving for an outcome that will never be obtained)
- **Relevant** – The KPI must give insight into the organization's safety performance
- **Time phased** – A KPI only has a meaning if we know the time dimension in which it realized

Some examples of leading indicators, provided by the Campbell Institute

Leading Indicator/description	Associated Metrics
<p><b>Risk assessment (S,O)</b></p> <p>Identification of the tasks, hazards, and risks of a job prior to work, and the implementation of protective measures to ensure work is done safely.</p>	<p>Number of assessments conducted per plan</p> <p>Percent of assessments completed per plan</p> <p>Ratio between the levels of risk identified (high, medium, low)</p> <p>Scoring the steps of an operation on severity, exposure, and probability</p> <p>Number of assessments communicated</p> <p>Number of risks mitigated or controlled</p> <p>Number of assessments validated by EHS manager</p> <p>Percent of assessments reevaluated and revalidated</p> <p>Percent of routine tasks identified</p> <p>Percent of tasks identified</p> <p>Percent of risk assessments completed per schedule/plan</p> <p>Number of assessments to evaluate potential severity</p>
<p><b>Hazard identification/recognition (S)</b></p> <p>Evaluations and assessments (not necessarily audits) through management and employee observations to identify potential hazards.</p>	<p>Number of near miss reports</p> <p>Number of unsafe observations (conditions or behaviors)</p> <p>Number of safe observations (conditions or behaviors)</p> <p>Number of unsafe observations per inspection</p> <p>Number of unsafe observations reported per employee per time period</p> <p>Number and percent of previously unknown or uncategorized hazards discovered</p> <p>Inspection count (collection of observations)</p> <p>Ratio of safe to unsafe observations</p> <p>Weighted percent safe observations (using risk matrix)</p> <p>Frequency of 100% safe</p> <p>Number of checklists filled out</p> <p>Number of comments for unsafe observations that clarified nature of the hazard</p> <p>Number of people trained in hazard identification</p> <p>Number of unsafe observations recorded by a trained person</p>

# References

- Accou, B., Reniers, G. (2020). Introducing the Extended Safety Fractal: Reusing the Concept of Safety Management Systems to Organize Resilient Organizations. *International Journal of Environmental Research and Public Health* 17, 5478.
- Amalberti, R. (2013). Navigating safety. Necessary compromises and trade-offs – Theory and practice. Springer.
- Aven, T. (2010). Misconceptions of risk. Wiley.
- Dekker S. (2014). The field guide to understanding ‘human error’. Third edition. Farnham: Ashgate.
- DOE. (2009). Human performance improvement handbook. Volume 2: human performance tools for individuals, work teams, and management. DOE-HDBK-1028-2009.
- ERA (2018). Safety management system requirements for safety certification or safety authorization. European Union Agency for Railways, 2018.
- Hardy, T.L. (2014). The system safety skeptic. Lessons learned in safety management and engineering. Second edition. BookLocker.
- Hollnagel, E. (2014). Safety-I and safety-II: The past and future of safety management. Ashgate.
- Hopkins, A. (2009). Thinking about process safety indicators. *Safety Science* 47, 460-465.
- IAEA (2009). The Management System for Nuclear Installations. IAEA Safety Standards Series No. GS-G-3.5. IAEA, Vienna.
- IAEA (2016). Performing Safety Culture Self-assessments. Safety Reports Series No. 83. IAEA, Vienna.
- Jenab, K. & Moslehpour, S. (2016). Failure Analysis: Case Study Challenger SRB Field Joint. *International Journal of Engineering and Technology*, Vol. 8, No. 6, December 2016
- Manuele FA. (2013). On the practice of safety. Fourth edition. New Jersey: John Wiley & Sons.
- NASA (2002). Fault Tree Handbook with Aerospace Applications. NASA Office of Safety and Mission Assurance, Washington, DC.
- Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27, 183-213.
- Reiman, T., Rollenhagen, C., Pietikäinen, E. & Heikkilä, J. (2015). Principles of adaptive management in complex safety critical organizations. *Safety Science* 71, 80-92.
- Roughton, J. & Crutchfield, N. (2014). Safety culture. An innovative leadership approach. Oxford: Butterworth-Heinemann.
- Snook, S. A. (2000). Friendly fire. The accidental shutdown of U.S. Black Hawks over Northern Iraq. New Jersey: Princeton University Press.
- Sagan, S.D. (1993). The limits of safety. Organizations, accidents, and nuclear weapons. Princeton University Press.
- Schein, E.H. (2010). Organizational culture and leadership. 4<sup>th</sup> Edition. Jossey-Bass: San Francisco.
- Dekker S. (2011). Drift into failure. From hunting broken components to understanding complex systems. Farnham: Ashgate.
- Weick. K.E. (1995). Sensemaking in organizations. Thousand Oaks: Sage.
- Weick. K.E. (1998). Foresights of failure: an appreciation of Barry Turner. *Journal of Contingencies and Crisis Management*, 6, 72-75.
- Weick, K.E. & Sutcliffe, K.M. (2007). Managing the unexpected. Resilient performance in an age of uncertainty. 2nd Edition. San Francisco: Jossey-Bass.
- Woods, D.D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. (2010). Behind human error. Second Edition. Farnham: Ashgate.