Safety management systems

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
11. 17.5 Future challenges and new directions of safety management (TIME!)
12. 25.5 Recap and Q&A
    - Deadline for returning the paper 31.5.2023

Learning logs

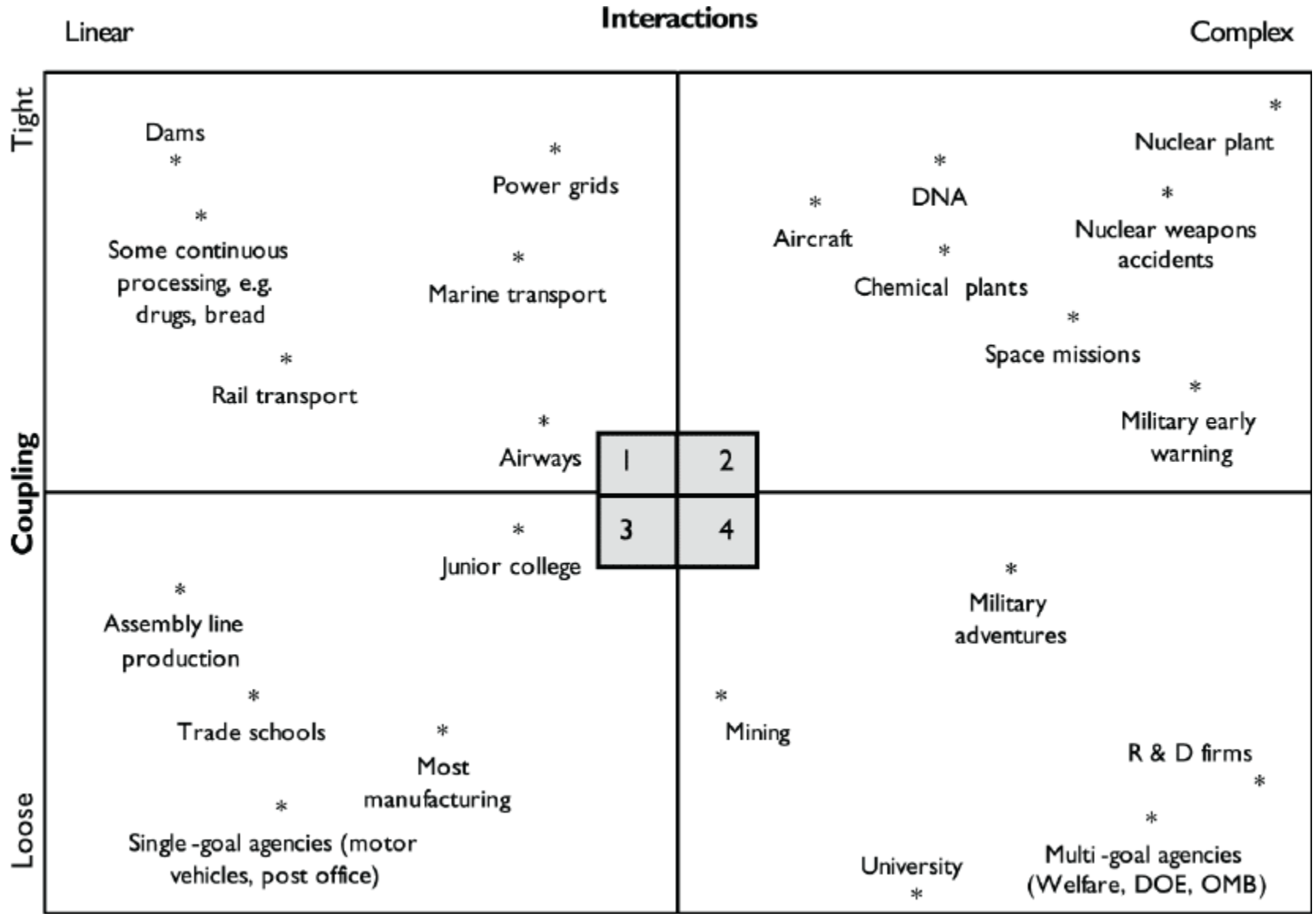
- Many had difficulties in grasping the key message of the previous lecture – especially the introduction of CAS
- Some liked the holistic perspective though!

- “sociotechnical imaginaries”, a concept used in the science and technology studies (STS)

- Questions about the added value of complexity theory and how to balance the various principles in practice, how to know what to do and when

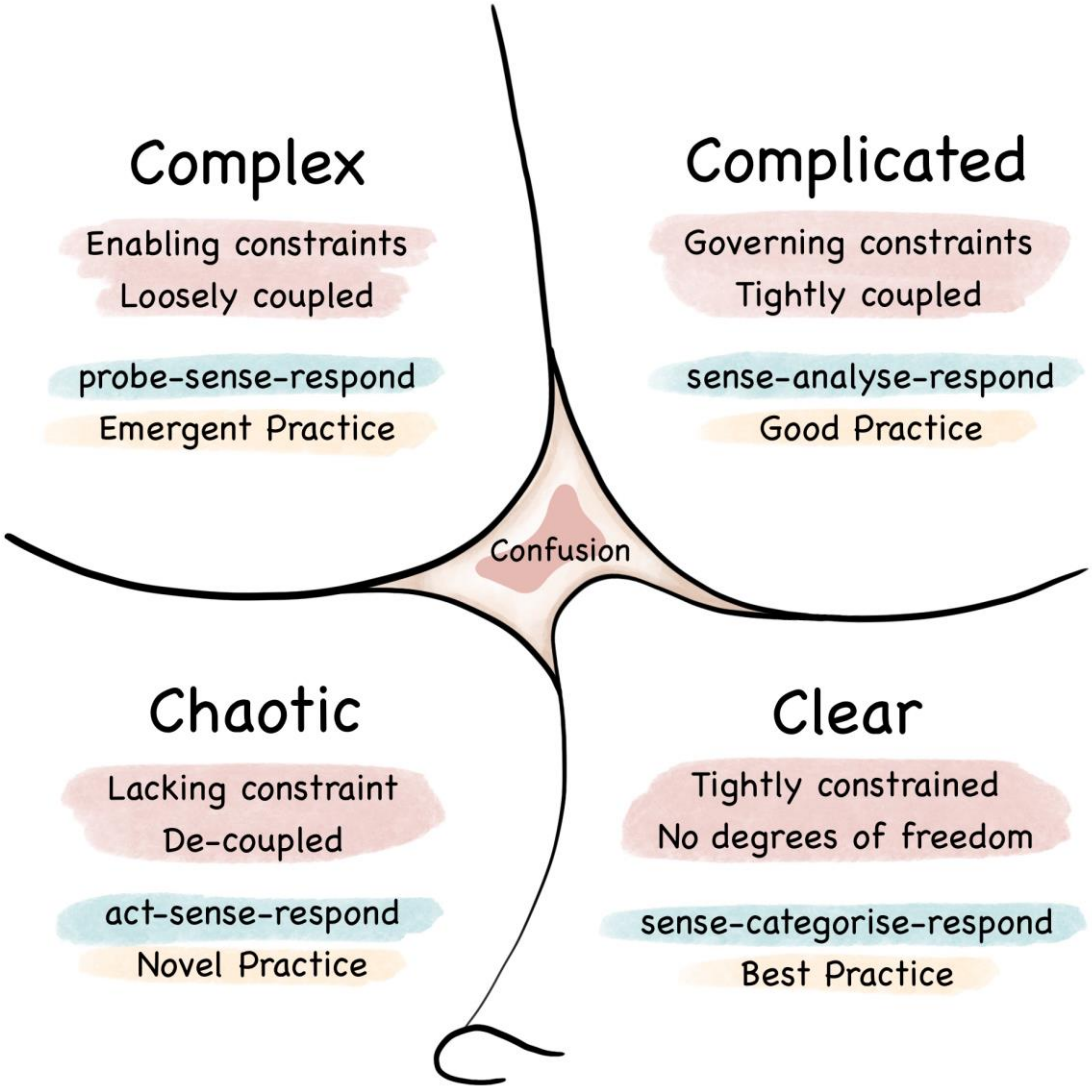
- Are there non-complex systems?

Perrow's model of interactions and couplings



The Cynefin Framework by Snowden (1999)

It is a tool that guides professionals when making decisions by analyzing the context in which that decisions are made.



Benefits of using complexity theory to understand organizations

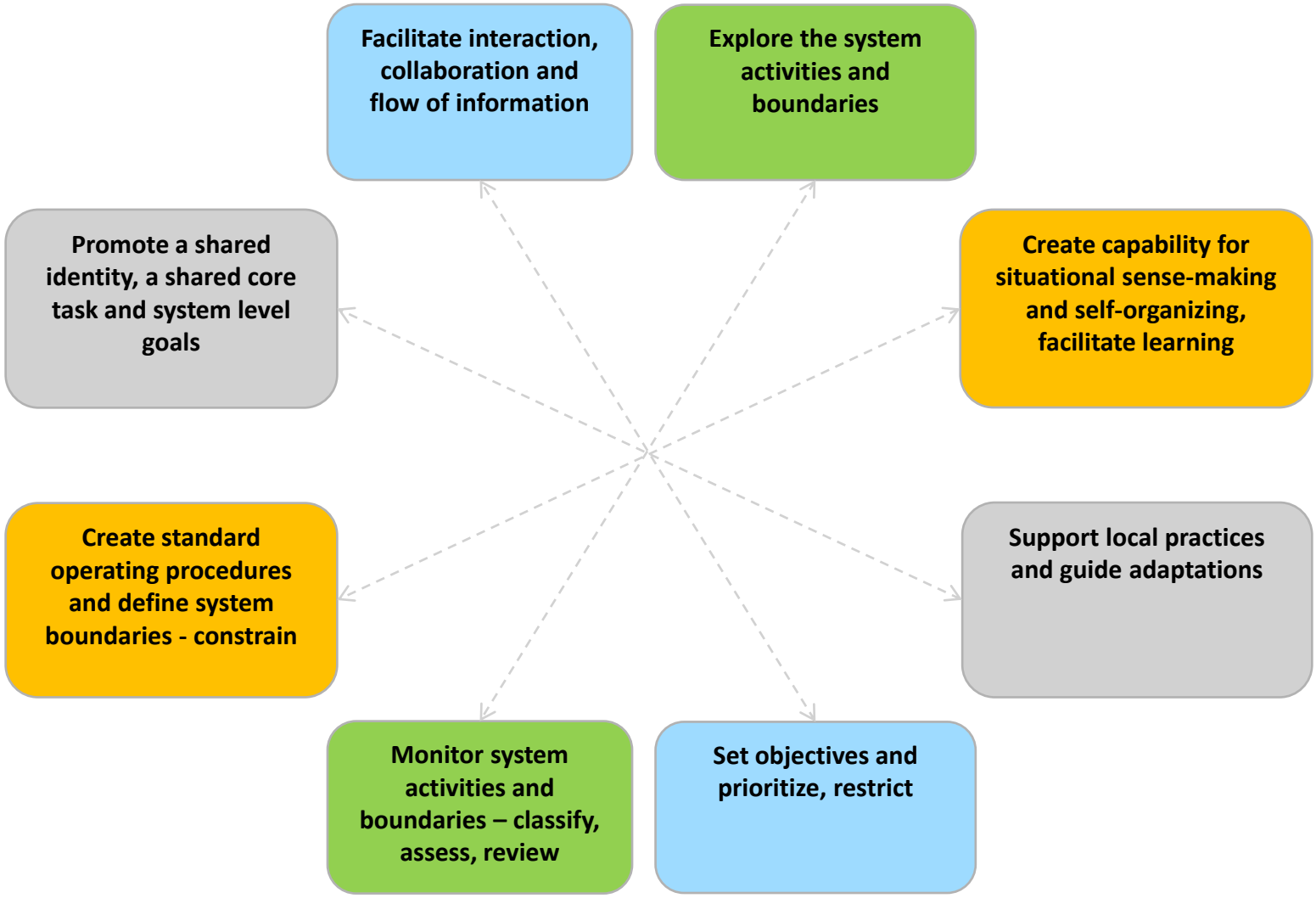
- It reminds us that to understand a system, we need both a microscope and a "macroscope"
  - It reminds us to pay attention to interactions and feedback loops
  - It reminds us to look at the whole – reductionist approaches do not work with complex systems
- It reminds that all things are interconnected, we always need to choose the level of analysis: where to draw the system boundaries, what to leave out
- It challenges the idea of modelling and predicting system behavior and shows how all models are incomplete
  - Safety culture overemphasizes unity, leadership overemphasizes individual's contribution & linear causality, human error approach overemphasized individual accountability & decision making, management systems overemphasize structural aspects and determinism
  - Control not only by constraining but by creating potential to the system, as prediction is impossible

Safety management in complex sociotechnical systems

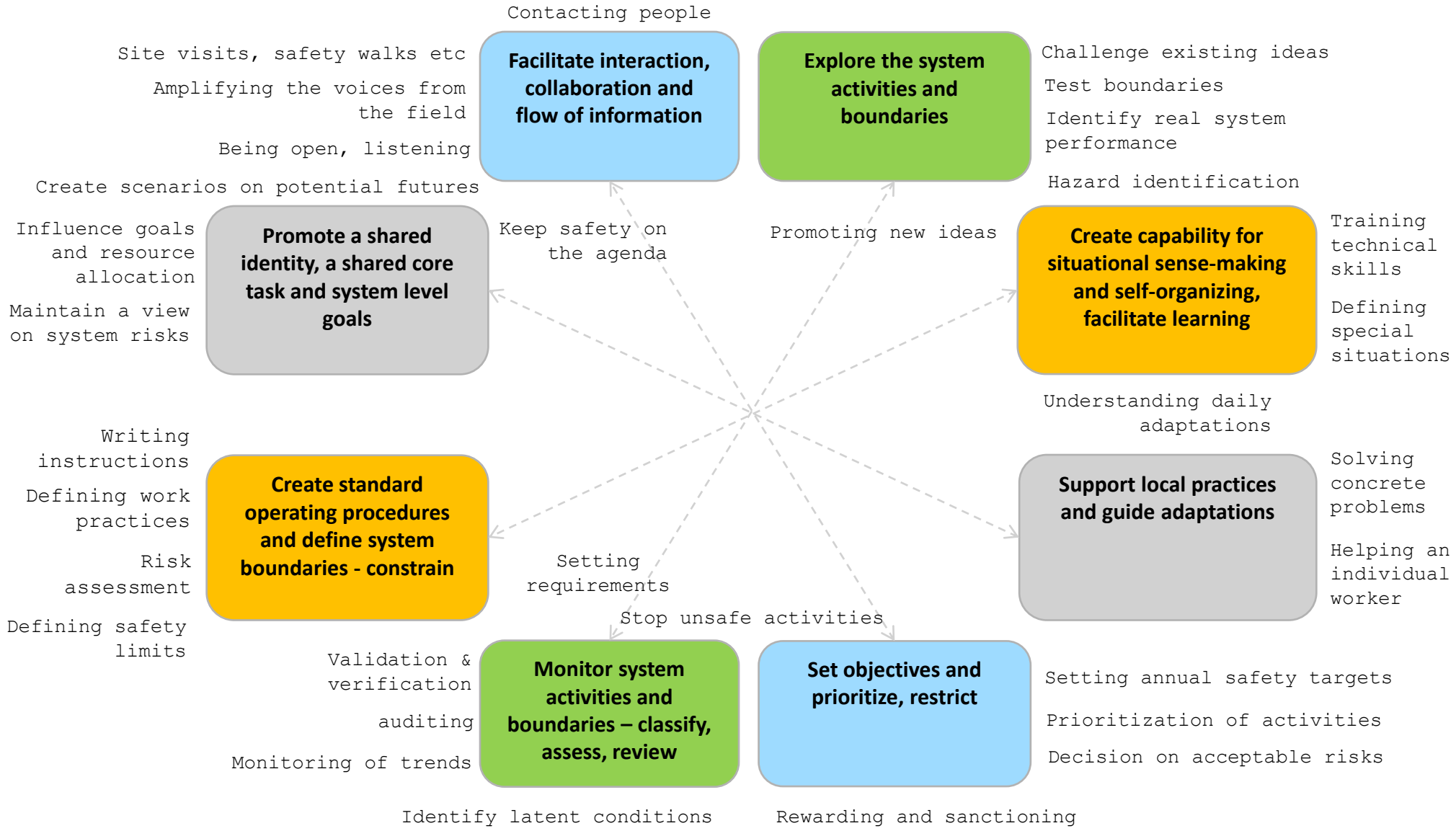
- In order to assure safety, we need to better understand
  - What is *safety* => prevention of errors, control of hazards, AND presence of organizational capabilities
  - What is to be managed => *complex sociotechnical systems*
  - What it means to *manage* => the eight basic principles of safety management
  - How to manage safety in complex sociotechnical systems => safety management systems and tools of safety management, implemented in line with the basic principles

Recap: organizations as complex adaptive systems as a starting point for safety management

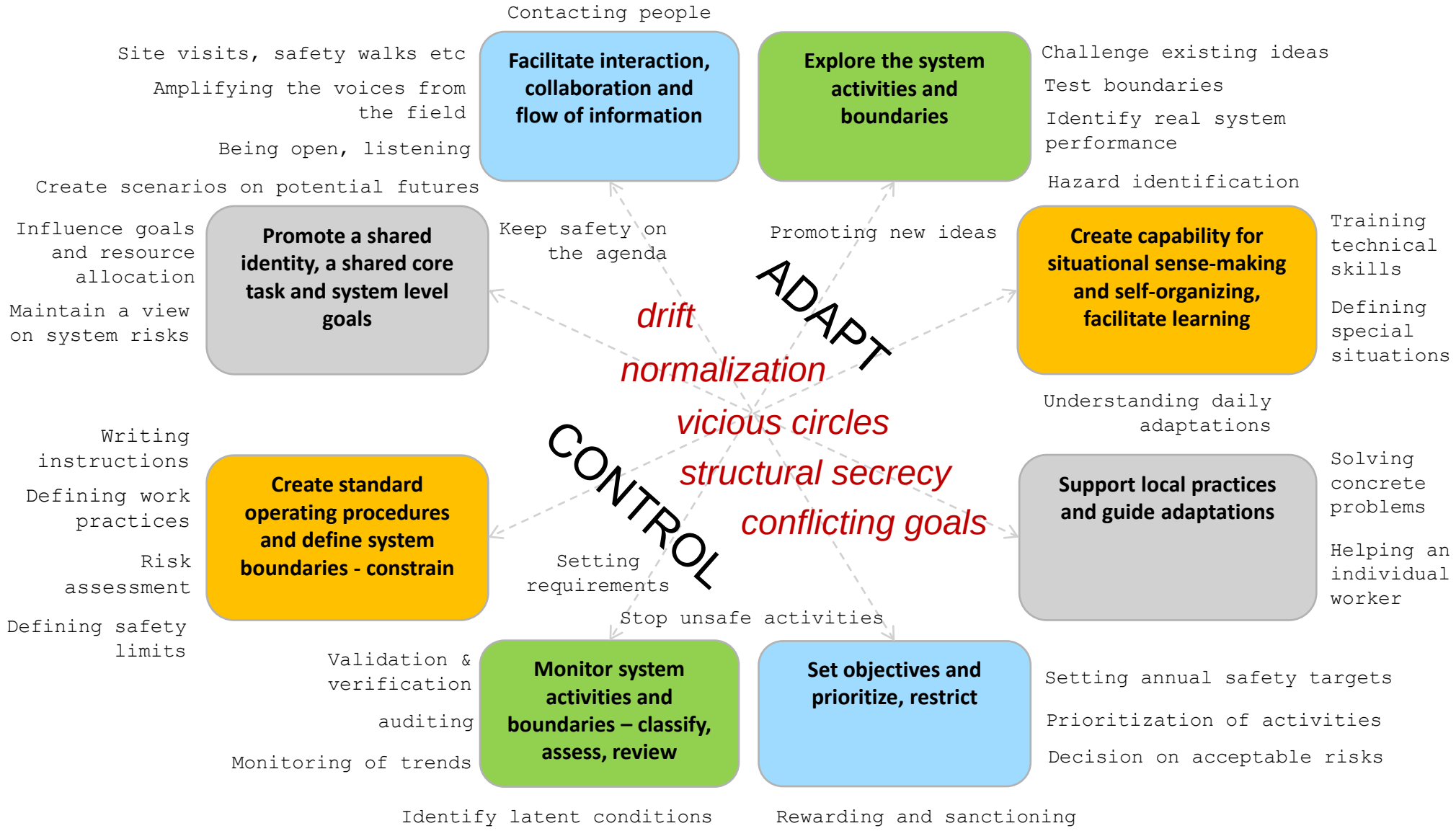
Model of safety management principles (revised from Reiman et al. 2015, Provan et al. 2020)



Model of safety management principles (revised from Reiman et al. 2015, Provan et al. 2020)



Model of safety management principles (revised from Reiman et al. 2015, Provan et al. 2020)



Both control and adaptation are needed to manage the system – the system phenomena cannot be completely controlled, but by understanding them the organization can safely adapt

Main tool of safety management is the Safety Management System (SMS)

Safety management systems (SMS) are based on the idea of quality management systems

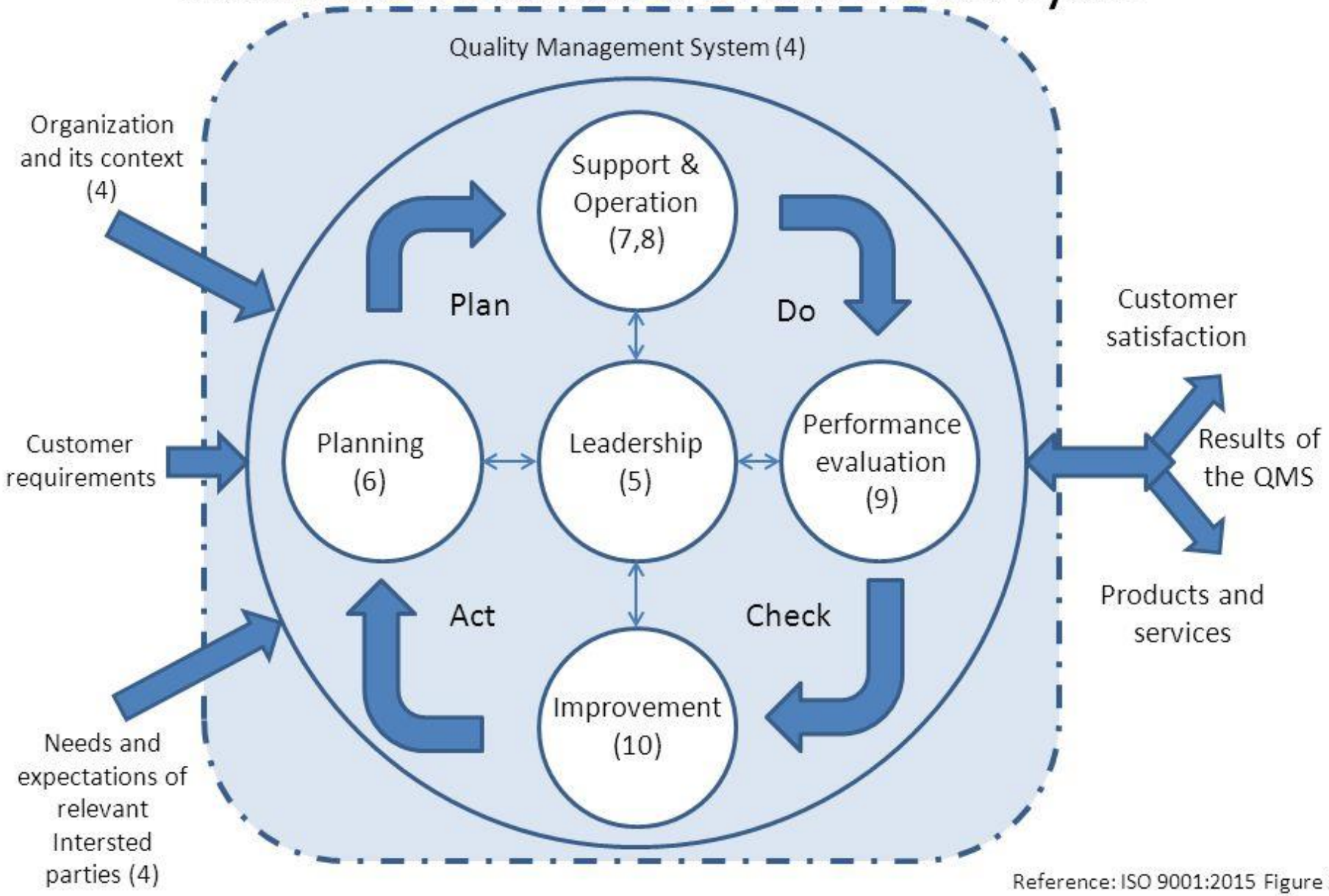
- Quality management systems were taken into use during the 80s and 90s (during the Management Systems Age mentioned in Lecture 1), thus the early SMS were quite similar to quality management systems
- SMS is a planned, documented and verifiable method of managing hazards and associated risks – systematic and continuously improving
  - A formal approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.
- Safety management systems became mandatory during the late 1990s and early 2000s in many safety critical domains (e.g. aviation, marine and rail industries) – however, organizational practices associated with SMS have been developed since the 1970s
  - The 1976 Seveso disaster led to the Seveso II directive (1996), which mandated systematic management systems across facilities in Europe that handled dangerous substances
  - Fire at the Piper Alpha offshore platform in 1988 led to a similar requirement in the petrochemical industry
  - For maritime, the watershed moment was the capsizing of the Herald of Free Enterprise in 1987

ISO 9001 elements

1. Context of the organization (needs and expectations of interested parties, processes, relevant internal issues)
2. Leadership (leadership and commitment, policy, roles, responsibilities, authorities
3. Planning (including risks and opportunities, quality objectives and changes)
4. Support (including resources, competence, documents, communication, and awareness)
5. Operation (including product control, inspection, operational planning etc)
6. Performance evaluation (including monitoring, measurement, auditing and management review)
7. Improvement (including non-conformity handling, corrective actions and continual improvement)

https://compassqs.com/iso-9001-certification-process/

Representation of the structure of ISO 9001:2015 Standard in the PDCA cycle



Reference: ISO 9001:2015 Figure 2

Safety Management Systems

- Management system provides a framework and a process for managing the organization
  - SMS should be integrated into the business processes of the organisation => should not become a paper-based system specifically developed for demonstrating compliance with the regulatory framework.
  - However, the SMS is a good place to gather all requirements for managing the organization, and define how these requirements are to be met
- The SMS should be a living set of arrangements, which grows in maturity and develops as the organisation, which it serves, does so.
  - It needs to be systematic => when things are done in a systematic manner, they can also be developed in a systematic manner
- Constructing an SMS requires an organisation to understand the hazards, and the risks it must control, the legal framework in which it is operating and to have a clear idea of what ‘good’ performance looks like.
- SMS should be proactive and integrated into all operations of the company

Culture and leadership is embedded in safety management systems

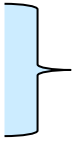
Edgar Schein (2010) has proposed the following mechanisms by which leaders embed organizational culture

- **Primary embedding mechanisms**
  - What leaders pay attention to, measure, and control on a regular basis
  - How leaders react to critical incidents and organizational crises
  - How leaders allocate resources
  - Deliberate role modelling, teaching, and coaching
  - How leaders allocate rewards and status
  - How leaders recruit, select, promote, and excommunicate
- **Secondary articulation and reinforcement mechanisms**
  - Organizational design and structure
  - Organizational systems and procedures
  - Rites and rituals of the organization
  - Design of physical space, facades, and buildings
  - Stories about important events and people
  - Formal statements of organizational philosophy, creeds, and charters

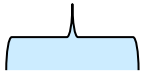
Culture and leadership is embedded in safety management systems

Edgar Schein (2010) has proposed the following mechanisms by which leaders embed organizational culture

- **Primary embedding mechanisms**
  - What leaders pay attention to, measure, and control on a regular basis
  - How leaders react to critical incidents and organizational crises
  - How leaders allocate resources
  - Deliberate role modelling, teaching, and coaching
  - How leaders allocate rewards and status
  - How leaders recruit, select, promote, and excommunicate
- **Secondary articulation and reinforcement mechanisms**
  - Organizational design and structure
  - Organizational systems and procedures
  - Rites and rituals of the organization
  - Design of physical space, facades, and buildings
  - Stories about important events and people
  - Formal statements of organizational philosophy, creeds, and charters



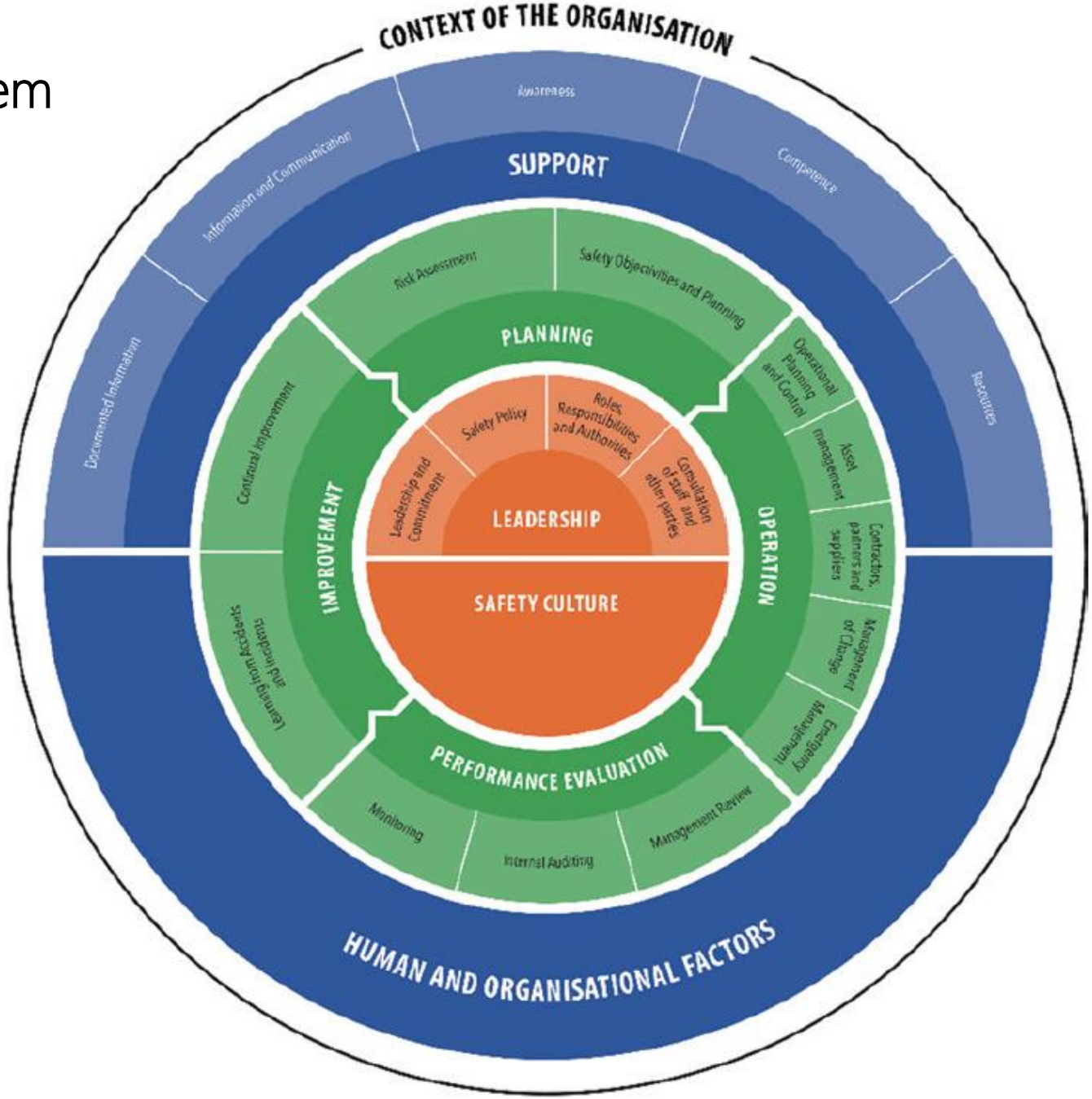
SMS typically covers only these mechanisms. Leadership and creation of appropriate culture in key role (again)



Safety management system requirements for safety certification or safety authorisation by ERA

ERA SMS requirements are built around two principles: PDCA cycle (Plan, Do, Check, Act) and International Standardization Organization's (ISO) Standard ISO 9001 Quality management systems – Requirements.

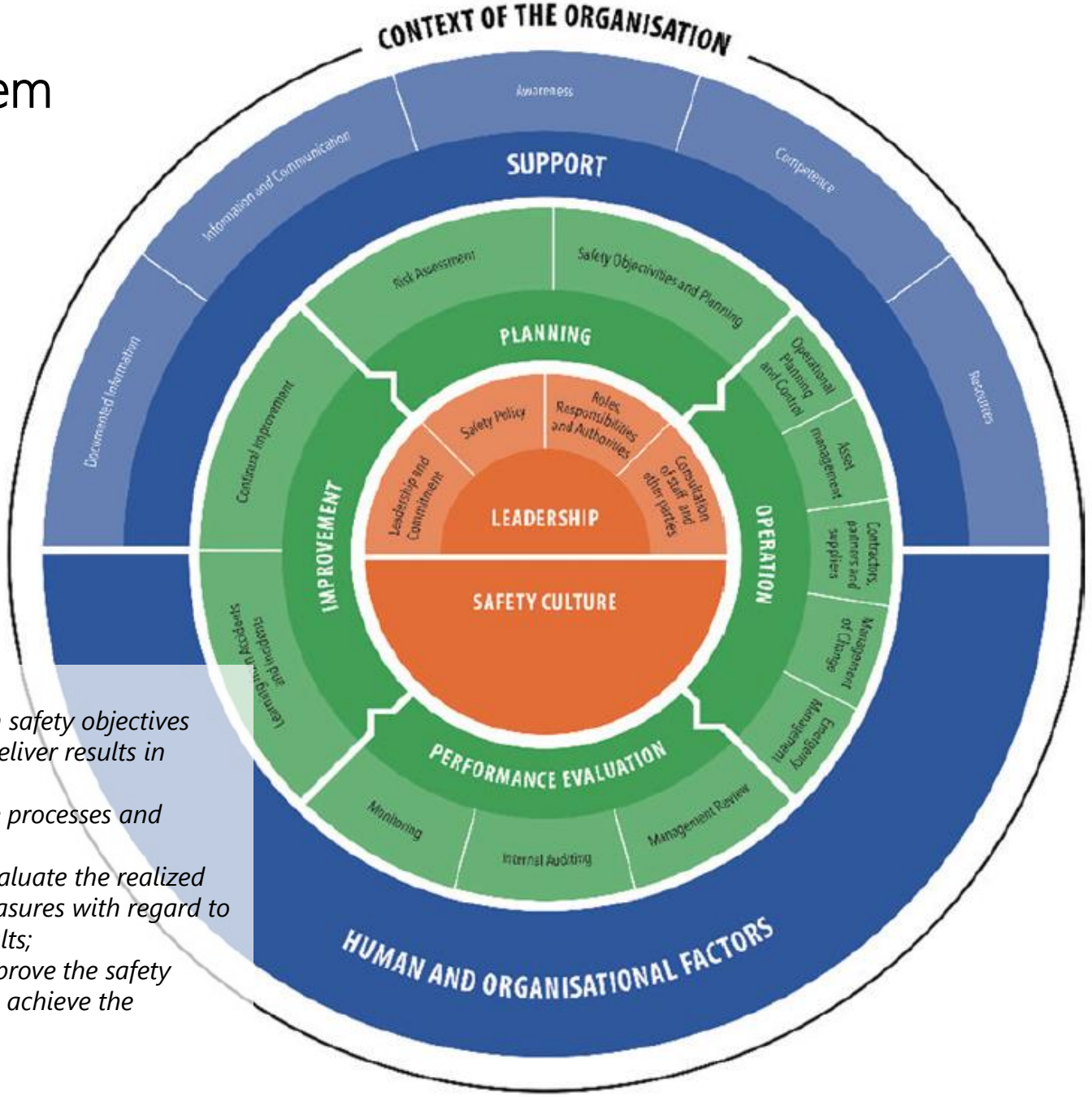
Figure 2: Railway safety management system



Safety management system requirements for safety certification or safety authorisation by ERA

ERA SMS requirements are built around two principles: PDCA cycle (Plan, Do, Check, Act) and International Standardization Organization's (ISO) Standard ISO 9001 Quality management systems – Requirements.

Figure 2: Railway safety management system



***Planning**: identify risks and opportunities, establish safety objectives and identify processes and measures necessary to deliver results in accordance with the organization's safety policy;*
***Operation (Do)**: develop, implement and apply the processes and measures as planned;*
***Performance evaluation (Check)**: monitor and evaluate the realized performance of the implemented processes and measures with regard to the objectives and the planning, and report the results;*
***Improvement (Act)**: take actions to continually improve the safety management system and the safety performance to achieve the intended outcomes.*

Elements of the ERA safety management system are on the top level identical to ISO 9001, but lower levels are safety-focused

1. Context of the organization
2. Leadership
   - I. Leadership and commitment
   - II. Safety policy
   - III. Organisational roles, responsibilities, accountabilities and authorities
   - IV. Consultation of staff and other parties
3. Planning
   - I. Actions to address risk
   - II. Safety objectives
4. Support
   - I. Resources
   - 1. Competence
   - 2. Awareness
   - 3. Information and communication
   - 4. Documented information
   - 5. Integration of human and organisational factors
5. Operation
   - I. Operational planning and control
   - II. Asset management
   - III. Contractors, partners and suppliers
   - IV. Management of change
   - V. Emergency management
6. Performance evaluation
   - I. Monitoring
   - II. Internal auditing
   - III. Management review
7. Improvement
   - I. Learning from accident and incidents
   - II. Continual improvement

Four components and twelve elements of Aviation Safety Management System (ICAO 2018)

1. **Safety policy and objectives**
   - 1.1 Management commitment and responsibility
   - 1.2 Safety accountabilities and responsibilities
   - 1.3 Appointment of key safety personnel
   - 1.4 Coordination of emergency response planning
   - 1.5 SMS documentation
2. **Safety risk management**
   - 2.1 Hazard identification
   - 2.2 Safety risk assessment and mitigation
3. **Safety assurance**
   - 3.1 Safety performance monitoring and measurement
   - 3.2 The management of change
   - 3.3 Continuous improvement of the SMS
4. **Safety promotion**
   - 4.1 Training and education
   - 4.2 Safety communication.

Generic elements of a safety management system

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

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

1. Management commitment

- Management commitment includes the formal setting of objectives and allocation of resources, as well as the less formal leadership of safety
  - Commitment should manifest in both behaviour and structures (resources, safety policy)
  - Management is in a key role in building safety culture via its leadership actions
- Typically management formalizes its commitment by creating and signing a safety policy
  - Including statement about the priority of safety, acceptable and non-acceptable behavior, and commitment to continuous improvement of safety and no-blame culture / just culture
  - Policy needs to be communicated to personnel and periodically reviewed

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

2. Employee involvement

- Organization needs to actively involve their own staff (or their representatives) as well as external interested parties in using and developing the safety management system to control risks over time
- No single person has the information needed to manage safety – collaboration and sharing of information are required in complex sociotechnical systems
- Safety committees are one way of involving personnel – mandatory in companies over 20 persons
- However, the involvement should be more daily than a committee participation
  - System for promoting employees to speak up, voice concerns, suggest developments – also anonymous concern system for significant safety issues
  - Active involvement in e.g. risk analyses, work development, change planning etc.

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

3. Organizing

- SMS needs to provide a clear picture of the structure of the organisation and how roles and responsibilities are allocated and maintained over time from those in front line positions to top management
- Organizing covers also
  - Organizing of the safety function – while retaining the responsibility for safety in the line organization
  - How safety issues are escalated in the organization, and who has a final say in safety related decisions
  - Information flows and reporting structure
  - Decision making practices
  - Process to ensure that individuals can report near misses, incidents and accidents
  - How work is supervised, how quality is assured (QA) and controlled (QC)
  - Interfaces between different functions and units

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

Organizing: Safety department in the organization

- Woods (2006): challenge is how to build a safety organization that would be “independent enough to question the normal organizational decision-making but involved enough to have a finger on the pulse of the organization”.
- His solution: A safety organization based on four principles:
  - Independent (of financial pressures and able to challenge management decisions),
  - Involved (in organizational actions that affect safety, e.g. event investigations, definition and updating of technical standards, readiness reviews),
  - Informed (about how the organization is actually operating and what factors are changing it) and
  - Informative (by providing information about organizational weaknesses and directing interventions).
- The challenge comes from the fact that, as Woods notes, these requirements are in conflict – balancing is needed, there is no one perfect solution

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

4. Hazard identification and risk assessment

- Identification of hazards is a prerequisite for a functioning safety management system
- ***Hazard*** can be defined as a condition / state or an object with the potential to cause harm to people or the environment, damage to equipment, loss of material or reduction of the ability to perform a prescribed function
- ***Risk*** is the projected likelihood and severity of the consequence or outcome from an existing hazard or situation.

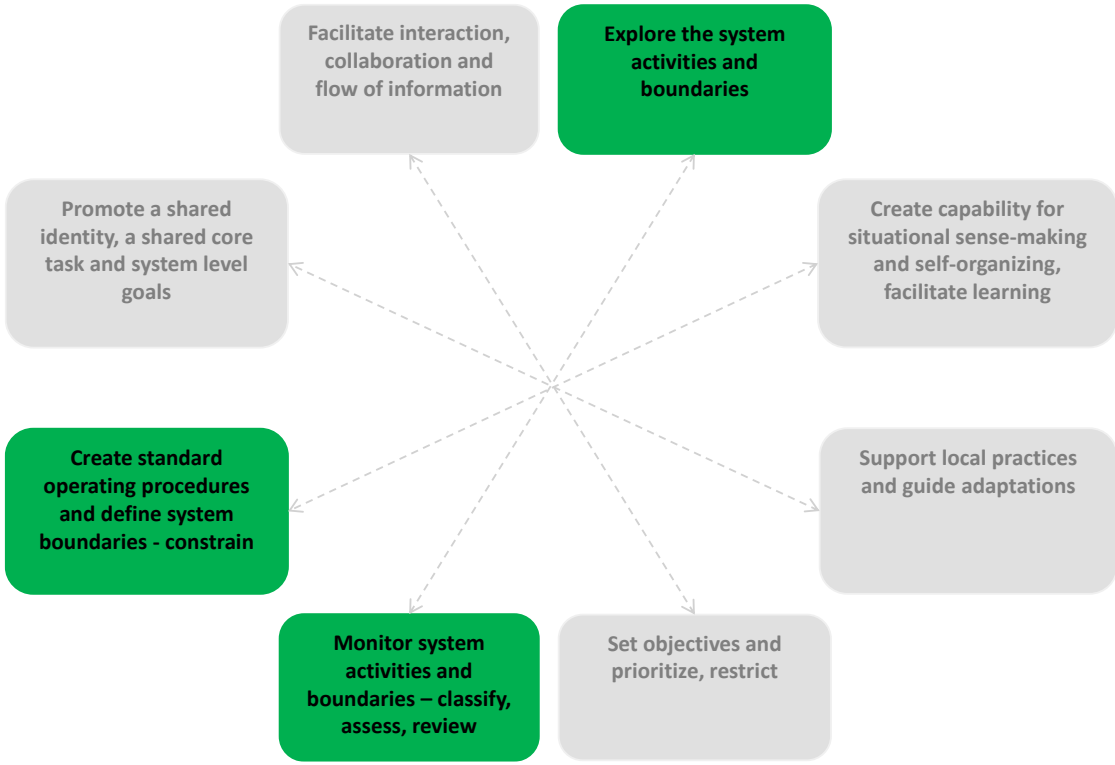
- There are various methods for identifying hazards during the system design and operation
- During operation, hazards can also be identified by various means, such as reporting systems, assessments, audits, inspections, incident investigations
  - Through “learning from experience” and “monitoring and assessment”

- Risk assessment process and some tools to be presented in the next lecture

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

Risk and hazard identification and assessment requires practices based on opposing principles

- Exploring the system boundaries by bringing in new information, identifying previously unknown hazards, identifying weaknesses in existing means of taking care of the hazards
- Monitoring the boundaries by assessing the probabilities and consequences of hazards, taking into account barriers
- Defining the system boundaries to be assessed – what is the risk tolerance of the organization



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

5. Hazard prevention and control

- Hazard prevention and control includes the mitigation of risk from the identified hazards
  - Several methods, including (re)design, human performance tools etc.
- Hazards and best controlled at their source: when designing technology, processes, tools and practices
  - Controlling the hazards later in the chain is more difficult and less effective
  - The idea of “inherently safe design”
- Work has to be designed to fit the human, not the other way around
  - Work planning, shifts, wokload, work practices, tool and the content of the work need to be designed so that a good quality performance is possible
- Technology offers both new solutions to protect against hazards as well as new types of hazards
- The countermeasures against the hazards need to be documented as standard operating procedures and emergency procedures
- As hazards change and unexpected things happen, proactive work needs to be done in the entire organization – vigilance and questioning attitude are needed

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

6. Communication

- Organizations need to define adequate communication channels to ensure that safety-related information is exchanged among the different levels of the organisation and with external interested parties including contractors, partners and suppliers.
  - They need to ensure information reaches the people who need it, and that the info is understandable, accurate, consistent, and traceable
  - Organizations need to specify what type of safety-related information needs to be communicated, how they will communicate, to whom and under which conditions this will be initiated and processed
- Communication channels need to be defined and promoted – channels are needed for top-down, bottom-up and horizontal communication
  - Different reporting tools are also one means of communicating bottom-up – important for their functioning is to take care of the feedback top-down
  - However, direct communication between supervisor and subordinate should always be the primary channel
- Communication should also cover information regarding the safety policy, expectations for safe behavior, current safety issues and risks, safety goals and their fulfilment, as well as any changes in the organization, environment or the hazards

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

7. Competence management

- Competence management aims to ensure the adequacy of the knowledge, skills and abilities of the personnel to manage the work and handle risks
  - Especially, the competence management system shall ensure that staff having a role that affects safety are competent in the safety-related tasks for which they are responsible
  - It allows the organization to maintain and develop the necessary knowledge and skills in a systematic manner in the entire organization
- Competence management should include
  - The identification of needed competences
  - Selection criteria for personnel recruitment
  - Initial training for newcomers
  - Ongoing training, specific job-related trainings and refreshment trainings => trainings to include also human and organizational factors related topics
  - Assessment of competence levels
  - Assessment of the effectiveness of training, including improvement
- Competence management should include also contractors, if some of the works have been outsourced
  - Also those competences that cannot be outsourced need to be defined (core competences)

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

8. Monitoring and assessment

- Organization needs a process for monitoring the application and effectiveness of the safety management system
  - Do the processes achieve intended results? Are risks being managed?
  - What opportunities there are for improvement?
- Different ways of monitoring and assessment
  - Management oversight, including supervision and management reviews
  - Independent oversight, including external assessments
  - Self-assessments of the management system, safety culture and leadership
  - Safety performance indicators, data analyses of performance data, surveys
  - Auditing, internal and external – including auditing of processes, performance and products
  - Incident investigations (as part of learning from experience)
  - Operational data (if operations allow such data, e.g. process industries, aviation)

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

9. Learning from experience

- The organization should investigate incidents and accidents to learn and improve risk controls
  - Identification of “root causes” and double-loop learning are required, as well as effective corrective actions
  - Promotion of no-blame / just culture and encouraging the reporting of issues
- There needs to be a process for reporting events, screening events for further investigation, investigating the root causes, and handling of corrective actions
  - Also important external events need to be considered
- Learning from successes needed

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

10. Continuous improvement

- Proactive improvement is needed even without any visible degradation of processes
- Improvement is also needed in terms of e.g. the monitoring and assessment processes – it needs to be acknowledged that they always produce an incomplete picture of the workplace reality and risks
- Continuous improvement is targeted to the creation of a culture that promotes further learning and development
- Safety culture self-assessments can be considered one method on continuous improvement
  - These are periodic assessment of culture made by the personnel themselves (facilitated by safety culture experts) in collaboration with the senior management
- Follow-up of issues identified in other processes – does the organization develop or is there a backlog of non-implemented corrective actions

Other issues of importance that are often incorporated into safety management systems

- Design
- Management of change
- Purchasing and control of the supply chain
- Document management and control of records
- Emergency management
- Asset management
- Operational issues – depending how integrated the management system is

Safety management systems (SMS) aim to make the management of safety systematic and verifiable

- SMS is a planned, documented and verifiable method of managing hazards and associated risks – systematic and continuously improving
  - A formal approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.
- Management system provides a framework and a process for managing the organization
  - SMS should be integrated into the business processes of the organisation => should not become a paper-based system developed for demonstrating compliance to the regulator
- Integrated management system versus safety management system
  - Synergies to be gained by having a similar framework for managing quality, environmental issues, occupational safety and health, process safety etc.
  - Integrated system can bring the various goals of the organization into active discussion and prioritization, but it can also hide goals that are not actively enforced
  - Also, typically not everything is integrated – quality, occupational safety and environmental safety are the most typical
- SMS seeks to formalize safety management
  - However, in a complex sociotechnical system not everything can, or should be, formalized (self-organizing and adaptability)
  - Also, it is important to separate ”work-as-planned” from ”work-as-done” => SMS can create conditions for the work to succeed

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.

Dekker S. (2011). Drift into failure. From hunting broken components to understanding complex systems. Farnham: Ashgate.

Dekker, S. (2018). The Safety Anarchist. Routledge.

ERA (2018). Safety management system requirements for safety certification or safety authorization. European Union Agency for Railways, 2018.

IAEA (2009). The Management System for Nuclear Installations. IAEA Safety Standards Series No. GS-G-3.5. IAEA, Vienna.

IAEA (2016). Leadership and Management for Safety. General Safety Requirements. No. GSR Part 2. IAEA, Vienna.

ICAO. (2013). Safety Management Manual (SMM). Fourth Edition, 2018. Doc 9859. International Civil Aviation Organization.

ISO (2015). Quality management systems. Requirements (ISO 9001:2015). The International Organization for Standardization.

Kurtz, C.F., Snowden, D.J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. IBM SYSTEMS JOURNAL 42, 462-483.

Perrow, C. (1999). Normal Accidents: Living with High Risk Technologies – Updated Edition. Princeton University Press.

Provan, D.J., Woods, D.D., Dekker, S.W.A., Rae, A.J. (2020). Safety II professionals: How resilience engineering can transform safety practice. Reliability Engineering and System Safety 195, 106740.

Reiman, T., Rollenhagen, C., Pietikäinen, E. & Heikkilä, J. (2015). Principles of adaptive management in complex safety critical organizations. Safety Science 71, 80-92.

Schein, E.H. (2010). Organizational culture and leadership. 4th Edition. Jossey-Bass: San Francisco.

Snowden, D. J., Boone, M. E. (2007). A Leader's Framework for Decision Making. Harvard Business Review. 85 (11): 68–76.

Woods, D.D. (2005). Creating Foresight: Lessons for Enhancing Resilience from Columbia. In W.H. Starbuck, M. Farjoun (Ed.), Organization at the Limit. Lessons from the Columbia Disaster. Blackwell Publishing.