

Resilience in risk analysis

S.O. Johnsen, T.Skramstad
Norwegian University of Science and Technology (NTNU)
Trondheim, Norway

Definition of Resilience

“The ability of a system to react and recover from disturbances at an early stage, with minimal effect on the dynamic stability.”

In addition “the ability to cope with ongoing trouble and the ability to recover after an incident” – Hollnagel (2006).

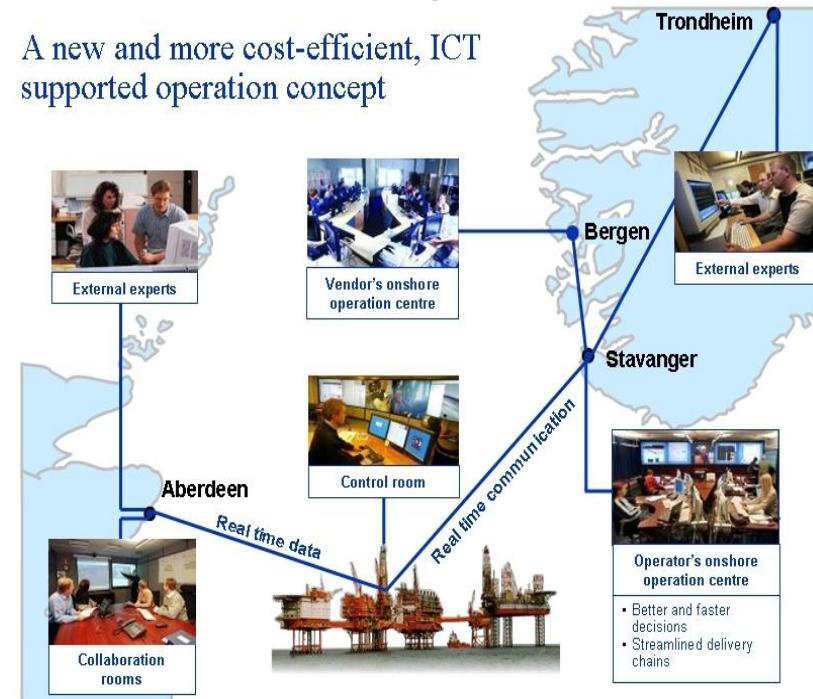
(Both safety and security)

Agenda

1. Background
2. Approach
3. Result
4. Suggested use and reflections

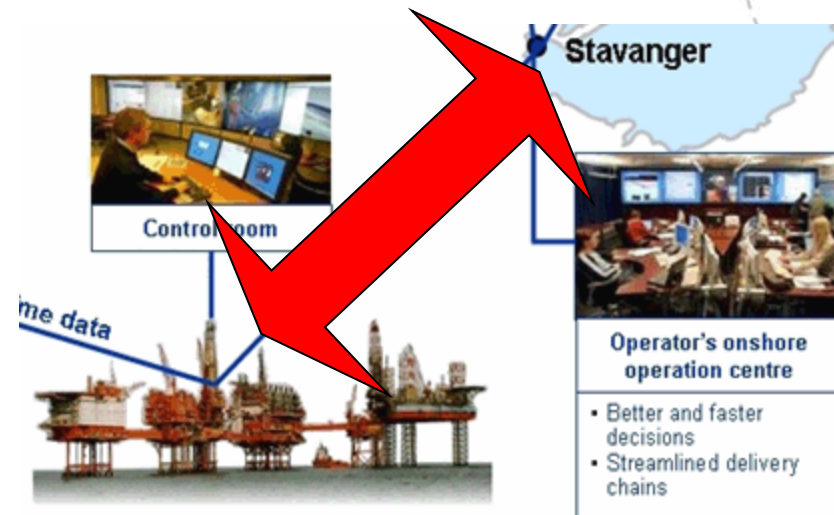
Context: Remote operation – Oil and Gas

- Increased collaboration between onshore and offshore and remote support of manned installations
- Focus on optimization of production and efficiency of operations
- Increased connectivity between systems – SCADA/PCS and ICT



Challenges

1. Complex system (tight couplings, remote collaboration) of ICT/ SCADA, organizations and actors with specialized knowledge
2. Normal variability of operations (Many organizations, new technology, different actors)
3. Consequences serious



“Attack can halt Norwegian oil and gas production” R.Røisli



SCADA

June 10/6, 1999, a 16" Olympic Pipeline Company pipeline ruptured and released 237,000 gallons of gas into a creek in Bellingham, Washington.



How to mitigate challenges

- | | |
|-------------------------|--|
| 1. Complex systems | 1. Model complexity and perform extended risk analysis |
| 2. Normal variability | 2. Must learn both from accidents and successful recoveries |
| 3. Consequences serious | 3. Must detect and recover at an early stage i.e. be resilient: <i>“The ability to react and recover from disturbances at an early stage, ...”</i> |

Agenda

1. Background
2. Approach
3. Result
4. Suggested use and reflections

Approach

Resilience seen as a useful perspective of safety management.

Key issues to be explored:

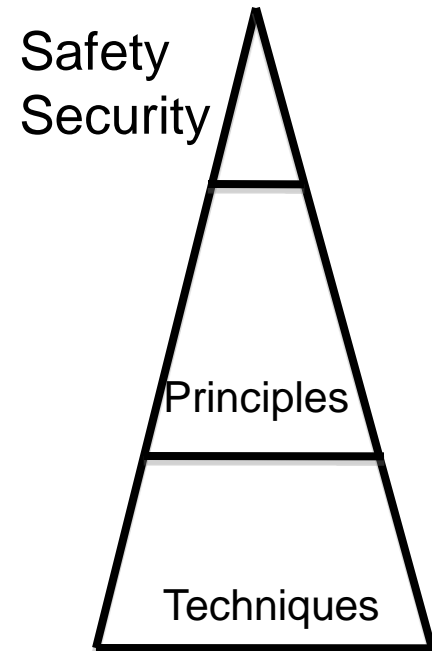
- How can we specify resilience to use the concept?
- How can resilience increase safety and security?

Performed a literature review of resilience and analysis of accident reports. Have described resilience and how resilience can be explored. Tested approach in workshops with the oil and gas industry.

What is resilience

Resilience as a strategy to improve safety and security in complex systems - described by:

- Resilient (functional) principles – such as the ability to manage margins.
- Resilient techniques – principles implemented through organizational, technological and human factors



Resilience – learning from +/-

+Positive	Recovery <i>HRO, Culture</i>	Variability <i>Resilience Engineering to avoid incidents</i>
-Negative	Accidents <i>Non linear, Complex, Simple linear</i>	Threats <i>Mitigating threats and risks</i>
	Past	Future

Model of root causes both +/-

Constraints

3. Root causes: management systems, culture, policies.

Conditions

2. Condition or lack of conditions

Mechanisms

1. Chain of events

Ref Leveson

Resilient principles to avoid root cause

Principle
(Constraint)

Constraints

Conditions

Mechanisms

3. "Root causes:"
Management of
margins

2. Condition or lack of
conditions

1. Chain of events

Agenda

1. Background
2. Approach
3. Result
4. Suggested use and reflections

■ Survey of practice to identify principles

- Survey of brittle practice and resilient practice
- Identify root cause
- Suggest a set of **resilient principles**

- Brittle practice

- NASA – during pressure to be faster, better, cheaper eroded the sources of resilience. IOM (Institute of Medicine) – balancing conflicting goals in healthcare against safety and not succeeding. (Ref Hollnagel)
- Suggested root cause: Disability to balance many conflicting goals.
- Suggested resilient principle: **Ability to manage margins (at boundaries).**

+ Resilient practice

- Even though there is distributed operations in HRO, there is good collaboration and a high level of safety and safety is in focus.
- Suggested “root cause”: In HRO there is a focus on top/down resolution of goal conflicts related to safety. There is focus on both “slow drift” (i.e. erosion of margins/goals) and actual “sacrificial decisions”.
- Suggested resilient principle: **Ability to manage margins** (at boundaries).

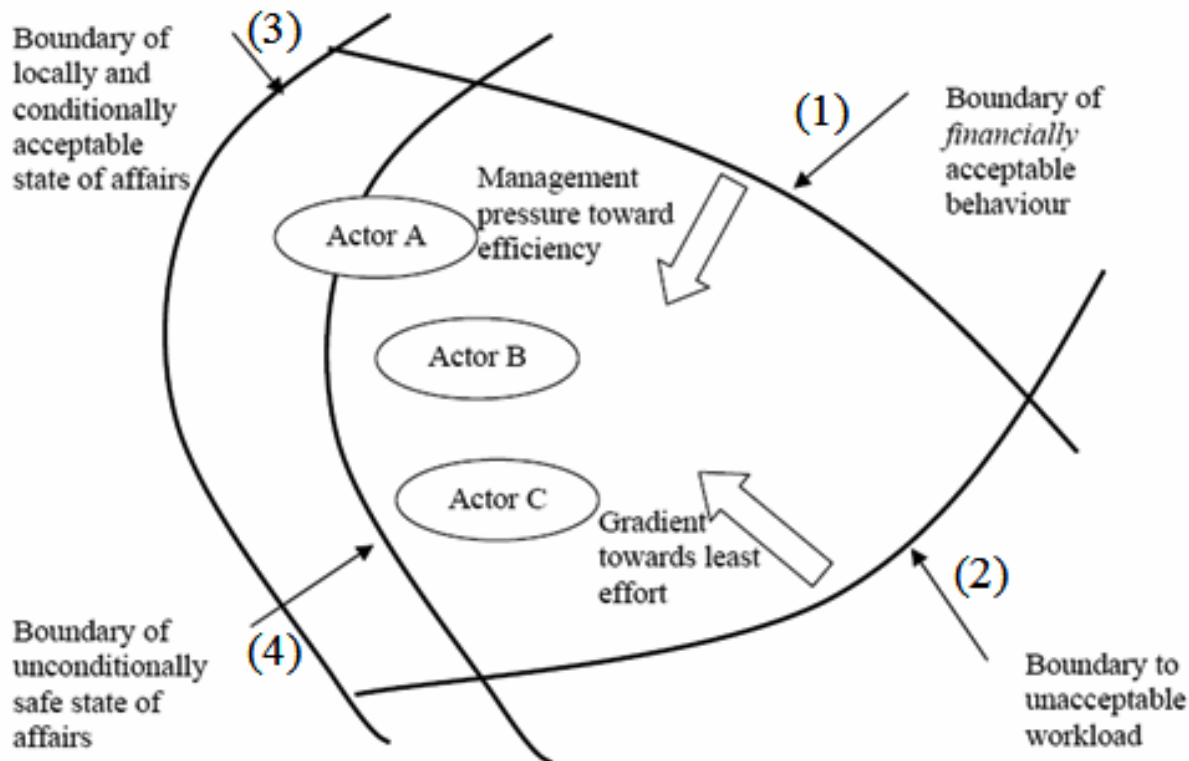
Identified seven resilient principles

- 1- Redundancy – having several alternate ways of performing a function. Implemented by spares, or concurrent use of multiple devices
- 2- Ability to graceful and controlled degradation (2A) and the ability to “rebound or recover” and achieve normal operation from degraded system (2B)
- 3- Flexibility in systems and organizations
- 4- Ability to manage margins (at boundaries)

Resilience

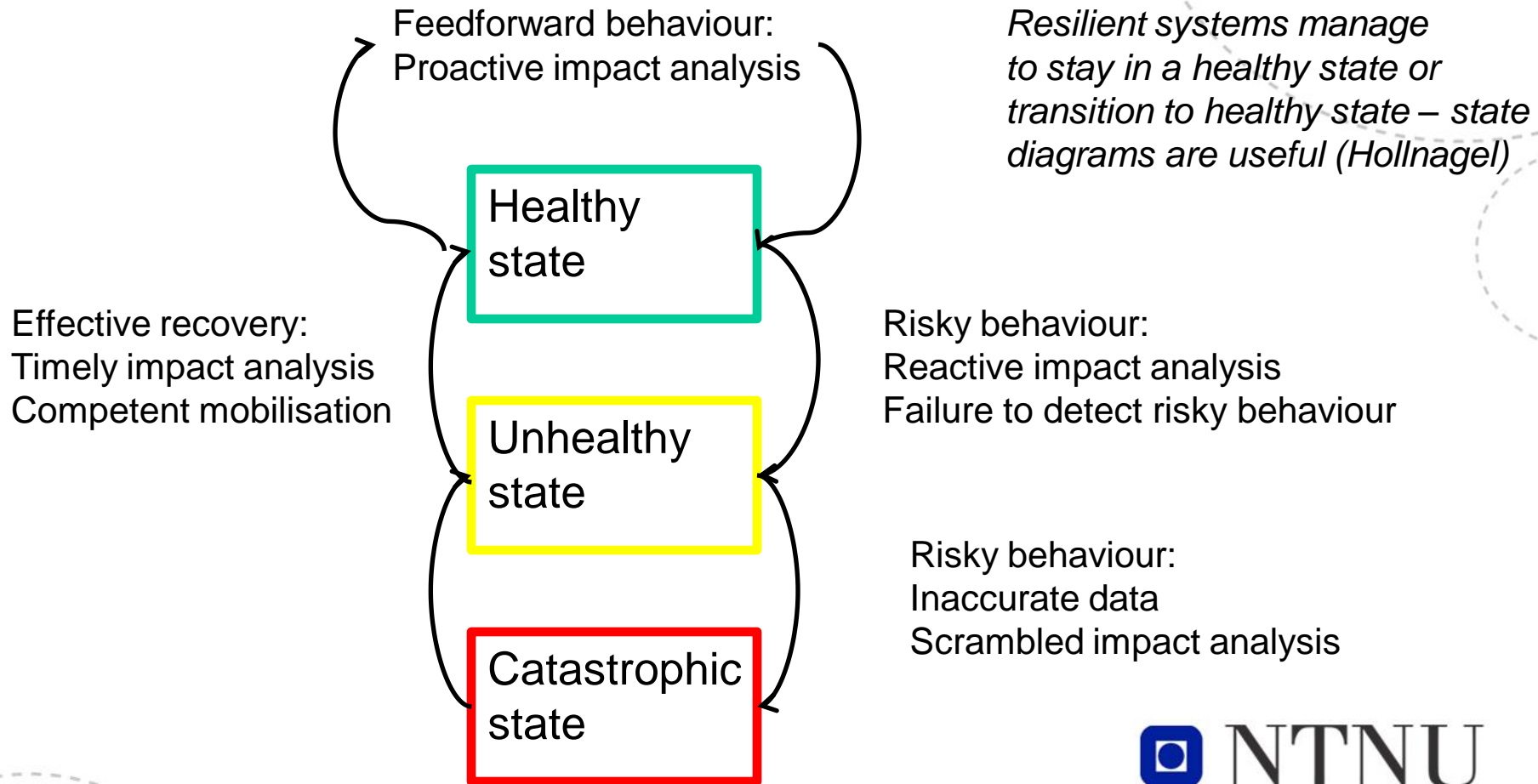
- 5- Use of common mental models across organisations that are collaborating
- 6- Reduce complexity by going from complex to linear interactions (as described by Perrow.)
- 7- Reduce couplings by going from tight to loose (as described by Perrow.)

Resilience as a boundary discussion



The boundaries of acceptable safety performance
Rasmussen (1997)

Graceful degradation and recovery

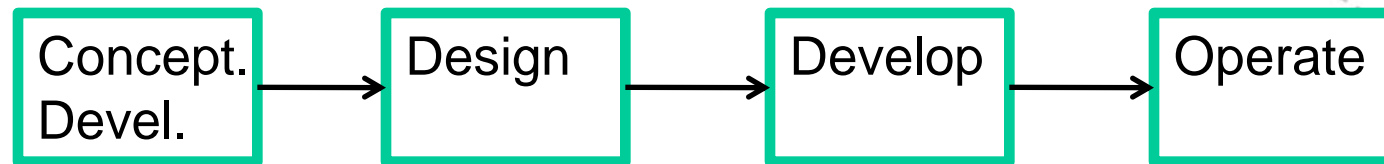


Agenda

1. Background
2. Approach
3. Result
4. Suggested use and reflections

Resilience in development and operations

- Based on a standard development lifecycle model.



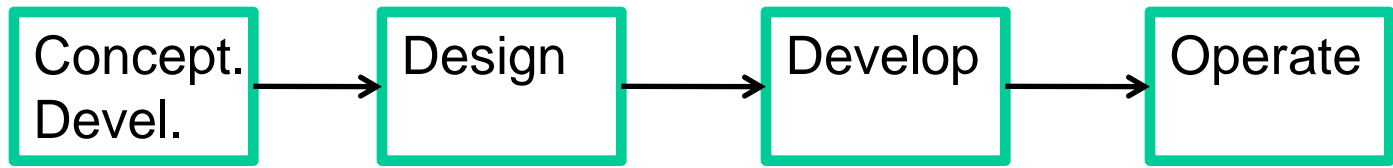
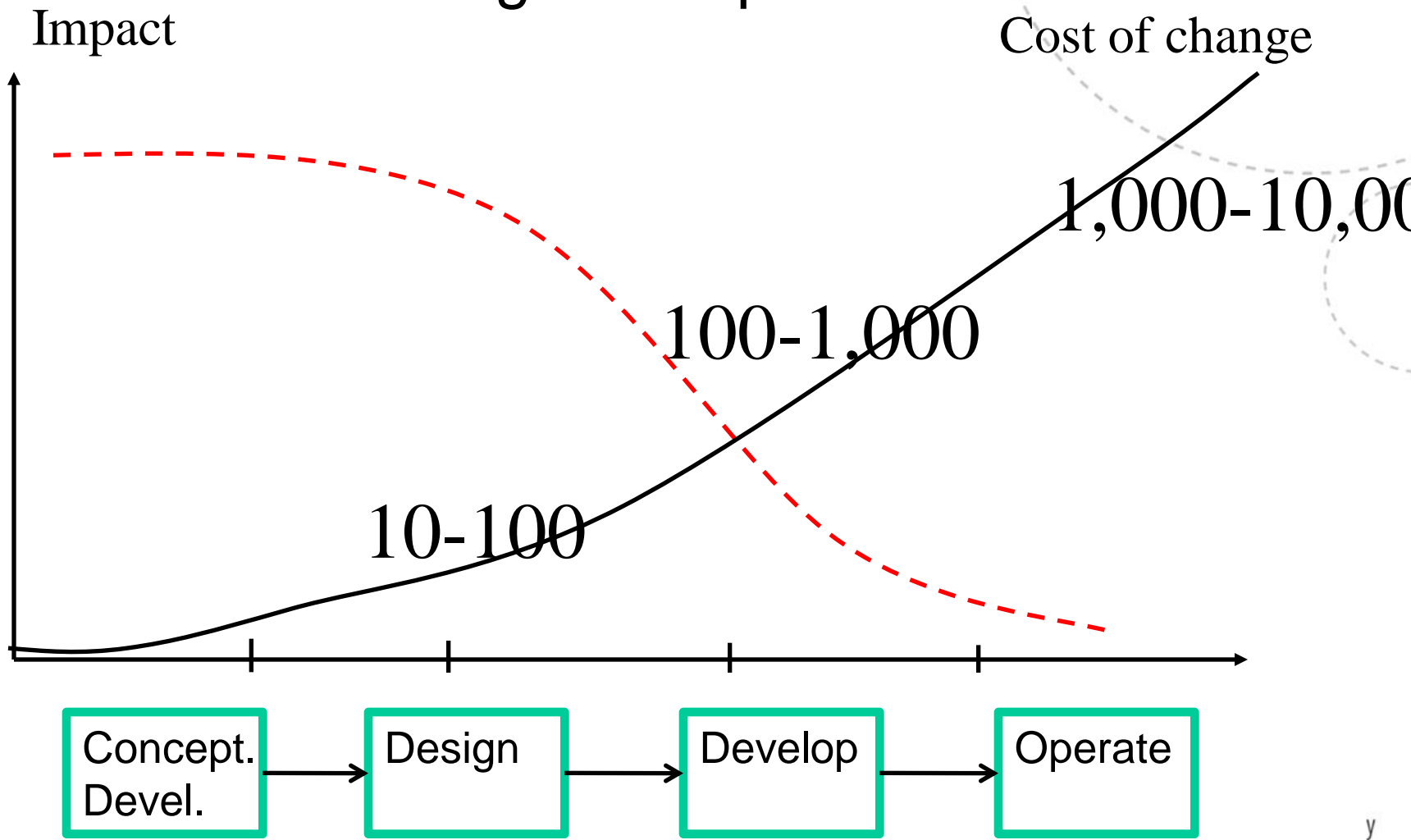
Conceptual: Resilient principles and hazards in PHA.

Design: FMECA, HAZOP, STAMP - exploring risks and resilience (focus on boundary discussions/ degradation)

Develop: Mitigate and control major hazards through indicators, safety/security cases.

Operate: Proactive hazard control, explore safety cases.

Suggested activities placed based on cost of change vs impact

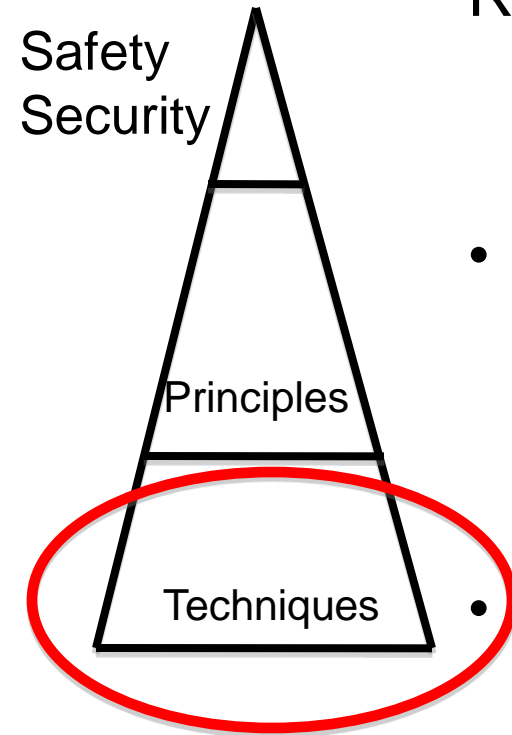


Resilience – example

Resilience as a strategy to improve safety and security in complex systems :

- Resilient (functional) principle – **managing margins**

- Resilient techniques – principles implemented through organizational, technological and human factors



Principle - Managing margins

Man: Knowledge of boundary conditions, i.e. knowing what may go wrong (risk analysis), getting the right information, knowing what to do (emergency training) and having ability to perform necessary actions (prioritizing/sacrifice safety vs. production).

Tech: Identify critical boundary conditions – design in margins and establish ability to report at boundary – proactive indicators and reactive (to manage, learn and react).

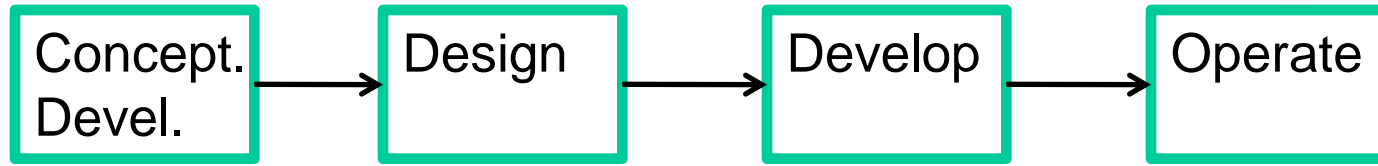
Organization: Clarity in responsibility at boundaries – overlap, interfaces.

Vulnerabilities introduced: New functionality can lead to more complex systems.

Resilient principles in Oil and Gas/ICT

Principle	Oil and Gas - ICT
Redundancy	Adaptive routing
Controlled degradation	Autonomic Computing - self protection or graceful degradation
Reduce complexity, reduce couplings	Service interface “hardening” OS and architecture

Resilience in development and operations



1. **Conceptual**

2. Design

3. Develop

4. Operate

1. Conceptual development

Key issues:

- Establish common “mental models” and identify stakeholders and scope.
- Identify resilient principles to be explored.
- Explore both accidents and successes - perform high level PHA (Preliminary Hazard Analysis) including resilience.

Key results:

- Document objectives of safety, security, control and resilience
- Document accountability – a key issue in complex systems
- Document functions and hazards and possible resilient principles
- Document key boundary conditions – including key states in addition to “normal operation”. (i.e. startup, shutdown).

Key issues

- Useful definition of resilience?
 - Have defined resilience by: Managing margins, Redundancy, Controlled degradation, Flexibility, Common mental models, Reduced complexity, Reduced couplings. – (Traceability?)
- How can resilience increase safety and security?
 - Explore resilient principles through PHA, HAZOP, FMECA and assess effect. Increased focus on proactive indicators. (Research).

Resilience a useful perspective

analyzing past and future

Positive and Negative	Resilient	Design Resilient practice <i>Resilience Engineering –</i>
	<i>Weaknesses Incidents, Accidents</i>	<i>Mitigating Threats and risks</i>
	Past	Future

■ Anything new in resilience?

1. Focus on both recovery(+) and accidents(-)
2. Increased focus on complex systems and boundary conditions, proactive indicators and graceful degradation
3. Broader scope of “risk” analysis – increased quality => safer and more resilient systems?

■ Agenda as presented

1. Background
2. Approach
3. Result
4. Suggested use and reflections



■ Questions?

Observing resilience at work

- Study near misses, successful recoveries and accidents – exploring an expanded accident model including RE
- Perform risk analysis exploring resilience in future systems
- Assess benefits of resilience engineering

2. Design

Key issues:

- Perform PHA including the resilient perspective, to identify focus areas to perform FMECA and HAZOP.
- Perform HAZOP – explore resilience. Use guidewords related to resilience such as “limit”, “flexibility”, “redundant”. Use resilience to discuss how deviations can be prevented or reduced.
- Explore margins and graceful degradation and recovery.

Key results:

- HAZOP among relevant stakeholders – list of major hazards and resilience.
- State diagram – graceful degradation and recovery.
- Test plan (Critical scenarios, graceful degradation, and recovery)
- Documentation of critical margins – mitigating actions and relevant proactive indicators.

3. Development/ Implementation

Key issues:

- Implementation of solutions and resilience
- Systematic testing, and test scenarios to be explored in operations – at margins, and during graceful degradation and recovery
- Common perceptions of hazards and key strengths (resilience)
- Information needs across relevant stakeholders and key indicators to be explored

Key results:

- Test models and scenarios to be explored in operations
- List of hazards and key strengths (resilience) in the system
- Critical margins and relevant proactive indicators

4. Operate

Key issues:

- Management of hazards and resilience – exploration of proactive indicators to detect slow drift or closeness to boundaries of performance
- Common perceptions of hazards and key strengths
- STAMP used to assess complex areas
- Audits of risks, safety and resilience

Key results:

- Updated test models and critical scenarios to be explored in operations (DFU)
- List of hazards and key strengths (resilience) in the system
- Critical margins and relevant proactive indicators
- Subjective assessment of risk and resilience

Redundancy(1)

- In HRO – focus is on redundancy. In brittle organisations there may be one critical component.
- Suggested “root cause”: In HRO there is a focus on safety and redundancy – having alternate ways of performing functions. In brittle organisations there is a lack of resources (Wreathall).
- Suggested resilient principle: Redundancy – having several alternate ways of performing a function.(1)
Implemented by spares, or concurrent use of multiple devices.

Graceful and controlled degradation(2)

- In HRO: In the “MAR-knockout” the nurses identified error in medication – through improvisation a manual system was introduced. In brittle organisations: there is organisational breakdowns and the system or organisation does not function.
- Suggested “root cause”: In HRO there is established routines and praxis. In brittle organisations routines are not established, or not known or trained for.
- Suggested resilient principle: Ability to graceful and controlled degradation (2A) and the ability to “rebound or recover” and achieve normal operation from degraded system (2B).

Flexibility(3)

- In HRO: Organisations adapt to situation and work load. In brittle organisations lack of flexibility or adaption are leading to incidents.
- Suggested “root cause”: In HRO abundant resources and ability to be flexible, i.e. having extensive system insight: In brittle organisations there is no flexible response to change or the unexpected.
- Suggested resilient principle: Flexibility in systems and organizations(3)

Common mental models(5)

- In HRO: The ability of inter-element collaboration to support problem solving based on training. In brittle organisations: Poor ability to collaborate and inform across organisation.
- Suggested “root cause”: In HRO: the ability to have extensive system insight. In brittle organisations: Poor common understanding of inter-relationships and dependencies. Poor understanding of risks.
- Suggested resilient principle: Use of common mental models(5)

Reduce complexity (6)

- In HRO: There is extensive system insight and there is an ability to manage complexity. In brittle organisations there is multilayered hierarchies, poor communication and diffuse responsibilities.
- Suggested “root cause”: In HRO there is focus on extensive training, clear responsibility and extensive information to reduce complexity. In brittle organisations there is missing focus on key risks and poor accountability.
- Suggested resilient principle: Reduce complexity (6) by going from complex to linear interactions as described by Perrow.

Reduce couplings (7)

- In HRO: There is focus on mitigating the negative consequences of tight couplings. In brittle organisations there is only one method to achieve goal.
- Suggested “root cause”: In HRO there is focus on flexibility, clarity of responsibility, and substitution is possible. In brittle organisations there is little slack and substitution is limited.
- Suggested resilient principle: Reduce couplings (7) by going from tight to loose as described by Perrow.

Redundancy (1)

Clarify process: Design or operation.

Clarify context: Man (knowledge, perceptions, actions..), technology or organization (responsibility, structure)

Man: May be part of redundant design. Knowledge to perform redundant operation.

Tech: Redundant technology – by spares, concurrent use,...

Organization: Allocation of responsibility and availability of resources to offer redundancy. Establish routines to shift responsibility.

Vulnerabilities: Redundancy may lead to medium complexity. Common failures can mitigate redundancy.

Graceful degradation (2A)

Clarify process: Design or operation.

Clarify context: Man (knowledge, perceptions, actions..), technology or organization (responsibility, structure)

Man: Knowledge to perform and/or assist in graceful degradation.

Tech: Systems designed or operated to do graceful degradation – going to other reduced functional states or safe shutdown.

Organization: Designed and/or trained to operate in degraded state. Key functionality is identified and allocated, with necessary process.

Vulnerabilities: Ability to perform graceful degradation introduces more complexity, and more to be tested and explored. Graceful degradation is assessed as introducing low to medium complexity dependent on design principle.

Ability to rebound (2B)

Clarify process: Design or operation.

Clarify context: Man (knowledge, perceptions, actions..), technology or organization (responsibility, structure)

Man: Knowledge to perform and/or assist in rebound.

Tech: Systems designed or operated to rebound – recovering from reduced functional states or safe shutdown.

Organization: Designed and/or trained to recover from degraded state.

Vulnerabilities: Ability to rebound introduces more complexity, and more to be tested and explored. Ability to rebound is assessed as introducing low to medium complexity dependent on design principle.

Flexibility (3)

Clarify process: Design or operation.

Clarify context: Man (knowledge, perceptions, actions..), technology or organization (responsibility, structure)

Man: System knowledge to be able to be flexible or be able to improvise.

Tech: Systems designed to be flexible, having alternate/ different ways of performing functions. (Systems should be error tolerant – errors should be immediately observable and reversible.)

Organization: Designed and trained to be flexible, switching priorities.

Vulnerabilities: Ability to be flexible introduces more complexity, and more to be tested and explored. Ability to be flexible is assessed as introducing low to medium complexity dependent on design principle.

Common mental models (5)

Clarify process: Design or operation.

Clarify context: Man (knowledge, perceptions, actions..), technology or organization (responsibility, structure)

Man: Having knowledge and understanding of common mental models.

Tech: Supporting common mental models by standardization (design, syntax, semantics) to create common understanding and exploration.

Organization: Interfaces and communication should support establishment and exploration of common mental models.

Vulnerabilities: Introduction and exploration of common mental models introduces more complexity, and more to be tested and explored.

Ability to use common mental models is assessed as introducing low complexity dependent on design principle.

Reduce complexity (6)

Interactions are described as going from linear (expected and familiar sequence) to complex (unfamiliar sequences not planned or unexpected). Complex systems are described as systems characterized by proximity, common-mode connections, interconnected subsystems, limited substitution, feedback loops, multiple and interaction controls, indirect information and limited understanding.

Man: Extensive training and system knowledge.

Tech: Simplification through design aids, design and design principles.

Organization: Clarity in responsibility and interfaces. The need for decentralized organization should be mitigated.

Vulnerabilities: Redesign of complexity are difficult – and may introduce unforeseen issues – the process must be assessed as having high complexity.

Reduce couplings (7)

A tight coupling has no buffers or slack between two items and what happens in one directly affects what happens in the other. Loose coupling has flexible performance standards and can incorporate failures, delays and changes without destabilization. Tight coupling is described as systems characterized by delays in processing not possible, invariant sequences, only one method to achieve the goal, little slack possible (in supplies, equipment, personnel), buffers and redundancies are designed-in (deliberate) and substitution (of supplies, equipment, personnel) are limited and designed in.

Man: Extensive training and system knowledge.

Tech: System should be designed to allow loose couplings.

Organization: Designed to enable loose couplings. Clarity in responsibility and communication.

Vulnerabilities: Ability to be flexible introduces more complexity, and more to be tested and explored. Ability to be flexible is assessed as introducing low to medium complexity dependent on design principle.

Explore resilience

**Positive
and**

Explore Resilience

Managing margins,
Redundancy,
Controlled degradation,
Flexibility,
Common models,
Reduced complexity,
Reduced couplings.

Implement Resilience

*(based on resilient
principles and risk
analysis)*

Negative

Brittle

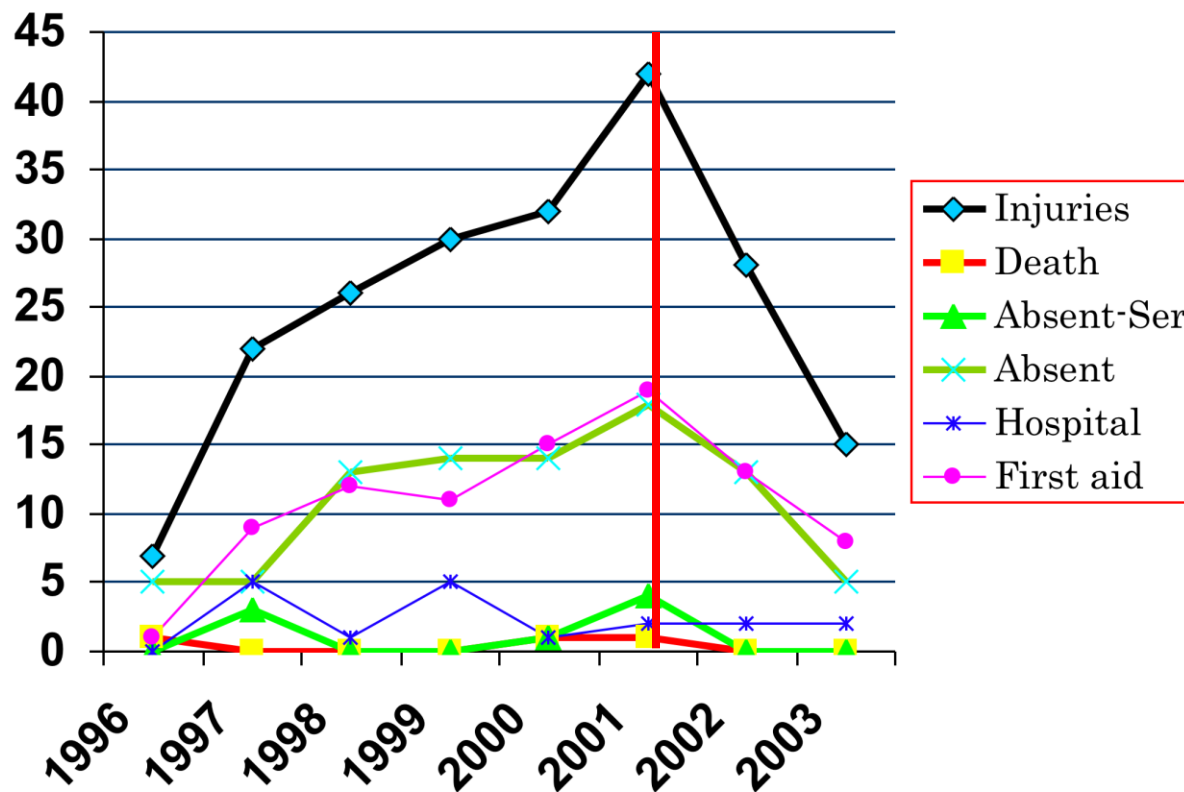
*Goal conflicts, lack
of resources*

Mitigating risks

Past

Future

Process should explore AR



Results

(Antonsen, Ramstad, Kongsvik- 2007)

Robustness criteria

To be robust the events that trigger state change must satisfy the following:

- Every state must have a transition defined for every input
- The logical or of transitions out of any state must form a tautology (logical complete expression)
- Every state must have a transition defined in case of no input

Resilience as ability to manage margin

(Stress-strain curve - Woods and Wreathall 2008)

