SITUATION ASSESSMENT - AN ESSENTIAL FUNCTIONALITY FOR RESILIENT NAVIGATION SYSTEMS

Michael Baldauf[2]
Paweł Banyś[1.1]
Evelin Engler[1.1,1.2]
Maciej Gucma[3]
Frank Heymann[1.1]
Frank Sill Torres[1.2]

German Aerospace Center
[1.1] Institute for Communications and Navigation
[1.2] Institute for the Protection of maritime Infrastructures

[2] University of Applied Sciences: Technology, Business and Design
[3] Maritime University of Szczecin

Topics

1. Introduction
   - Resilience as challenge
   - Resilience principles
   - Situation awareness

2. Ships‘ Navigation System
   - Carriage Requirements
   - System for Detection and Indication of Threats
   - Threat Management

3. Case Studies
   - Resilience by additional capacities
   - Resilience by tolerance
   - Resilience by flexibility

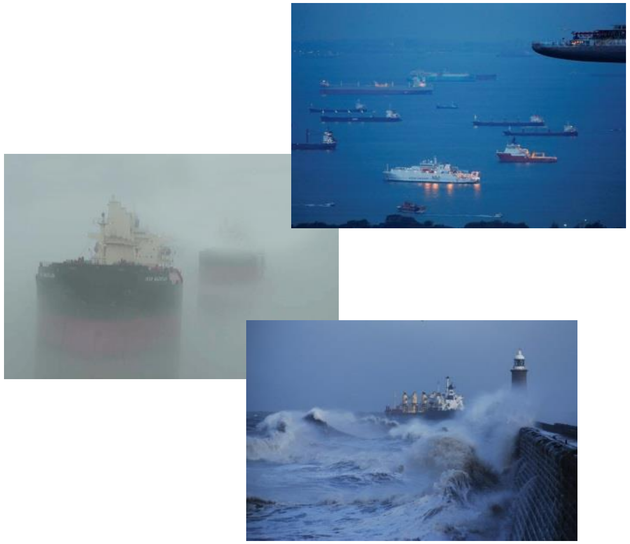
4. Summary

DLR

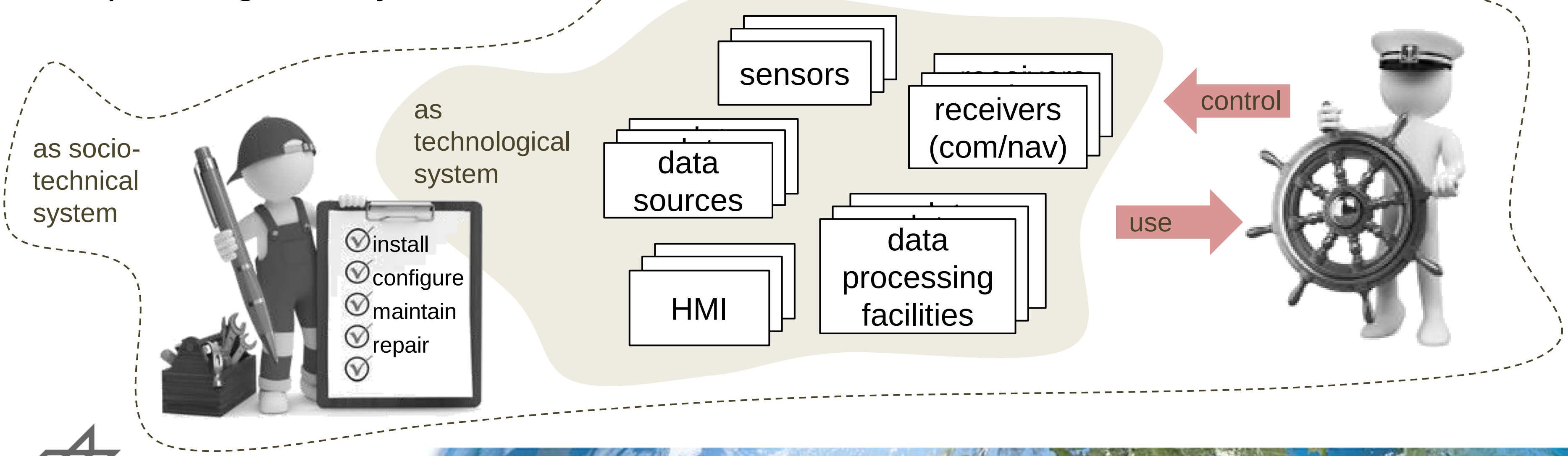
Resilience as Challenge

Resilience of engineered systems reflects the required system ability

- to well-function with the needed performance
- to adapt the operation to changing conditions
- to withstand interfering influences
- to rebound from disruptive & destructive effects



Ships navigation system



Resilience Principles and Concepts (Theory)

Principles

- In the last decades the resilience community identified more than 40 principles
- Jackson identified 14 top level principles in an abstract manner

	Principle	Capability	Attribute
1	absorption	to absorb the magnitude of disruption	capacity
2	physical redundancy	to overbridge single failures by redundant layout	
3	functional redundancy	to provide different ways to perform critical tasks	
4	layered defence	to apply two or more independent principles	
5	human in the loop	to use humans' better dealing with unprecedented threats	flexibility
6	reduction of complexity	to limit the complexity to the necessary degree	
7	reorganization	to adjust structure and functioning to current situation	
8	reparability	to be prepared for recovery of origin functionality and performance	
9	loose coupling	to limit error propagation in complex, networked systems	
10	localized capacity	to perform the functionality using distributed resources	tolerance
11	drift correction	to mitigate risks by adjustment to changes	
12	neutral state	to ensure true situation awareness for right decisions	
13	inter-node interaction	to ensure communication, cooperation, collaboration between nodes for a coordinated use of resources	cohesion
14	reduce hidden interactions	to avoid harmful interactions between nodes	

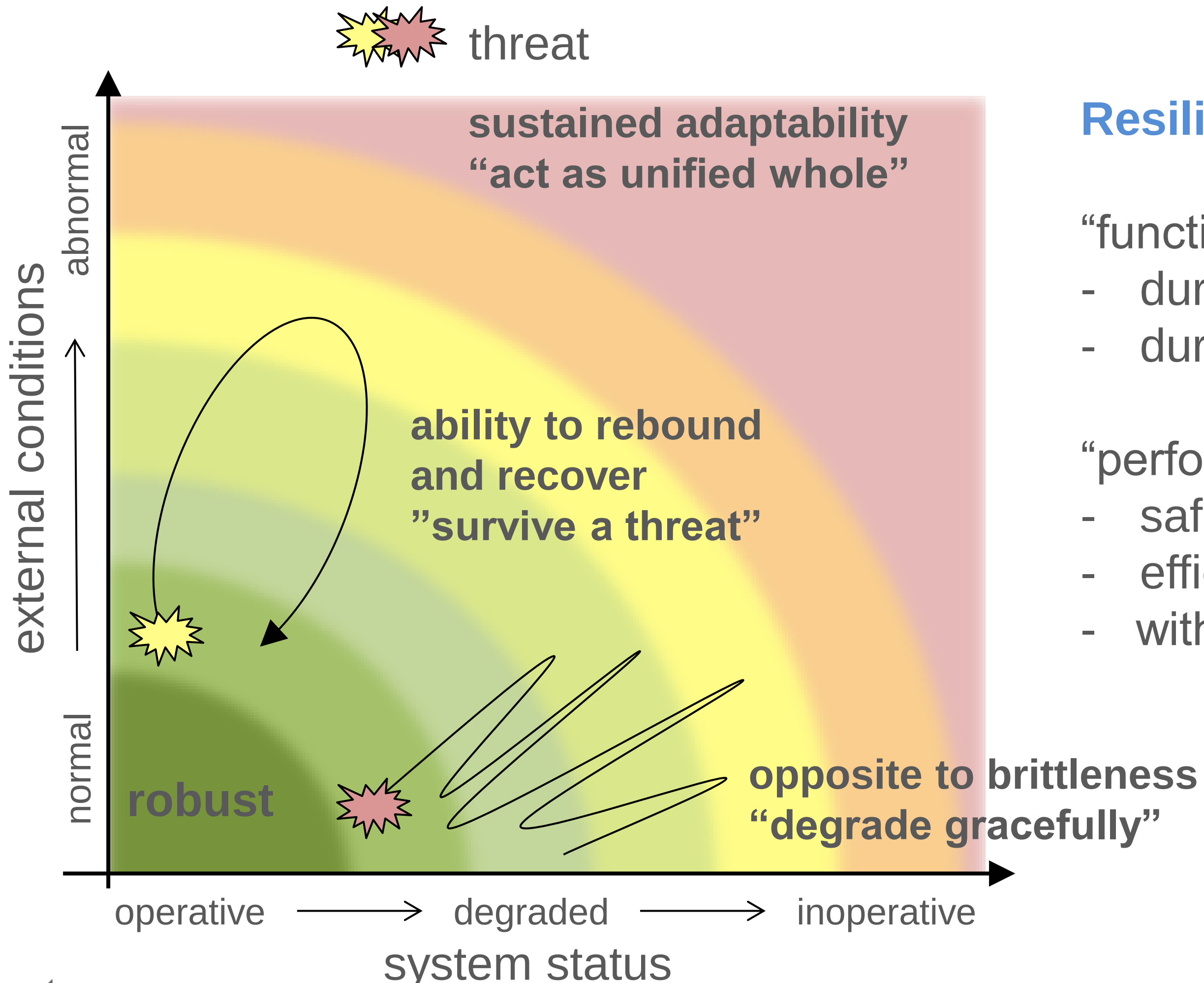
Resilience targets [Jackson]

- to survive a threat (capacity)
- to adapt to a threat (flexibility)
- to degrade gracefully in the face of threat (tolerance)
- to act as unified whole in the face of threat (cohesion)

Resilience concepts [Wood]

1) robustness
2) ability to rebound and recover
3) as opposite to brittleness (during operation near or beyond its capacity limits)
4) sustained adaptability of functioning and operation in a changing and networked world

Resilience Principles and Concepts (Practice)



Resilience criteria

"functionality" = ship navigation

- during voyage
- during life cycle

"performance"

- safe
- efficient
- with negligible emissions….

Situation Awareness

[Lundberg]

- is a human concept driven by increased requirements for human (more complex tasks/systems; changes, new/unexpected threats)
- reflects the human need to be aware of certain aspects of the world to make critical (and right) decisions

Spatial & temporal frame of SA	Current/emerging situation
Objects of interests	Nautical Tasks
Implication to be assessed	Applications

- is a dynamic process triggered by the current situation awareness (new findings) and applications requesting/using these new findings

Digitalization and automatization of ships' navigation system

True situation awareness
(resilience, safety, security)
=
machine-made functions
+ human-made activities

Topics

1. Introduction	▪ Resilience as challenge ▪ Resilience principles ▪ Situation awareness
2. Ships' Navigation System	▪ Carriage Requirements ▪ System for Detection and Indication of Threats ▪ Threat Management
3. Case Studies	▪ Resilience by additional capacities ▪ Resilience by tolerance ▪ Resilience by flexibility
4. Summary	

DLR

Ships‘ Navigation System

Carriage requirements, threat detection, threat management….

Carriage requirements (SOLAS V R.19) and backup recommendations

- ECDIS (Electronic Chart Display and Information System): up to date paper charts or a secondary independent ECDIS device,
- magnetic compass: a spare magnetic compass independent of any power supply,
- X-Band radar: S-Band radar
- ARPA: a second automatic tracking aid to plot automatically the range and bearing of other targets

Threats to safety of navigation

- nature-related: heavy weather, storms, waves etc.
- traffic-related: collisions, grounding
- societal: piracy, cyber terror

Dealing with threats

- Robustness of equipment
- Backup solutions
- Provision of special services e.g. ice control, weather, VTS, (FOC) to improve navigation ….

Need of enhancement

- different threat detection strategies
- design/acting as whole (system approach)

OOW = Officer on Watch, VTS = Vessel Traffic Service, FOC = Fleet Operation Center

Topics

1. Introduction
   - Resilience as challenge
   - Resilience principles
   - Situation awareness
2. Ships‘ Navigation System
   - Carriage Requirements
   - System for Detection and Indication of Threats
   - Threat Management
3. Case Studies
   - Resilience by additional capacities
   - Resilience by tolerance
   - Resilience by flexibility
4. Summary

DLR

Resilience by additional capacities (1)

Principles

- **absorption**
  to absorb the magnitude of disruption
- **physical redundancy**
  to overbridge single failures by redundant layout
- **functional redundancy**
  to provide different ways to perform critical tasks
- **layered defence**
  to apply two or more independent principles

Case study

(a) physical redundancy

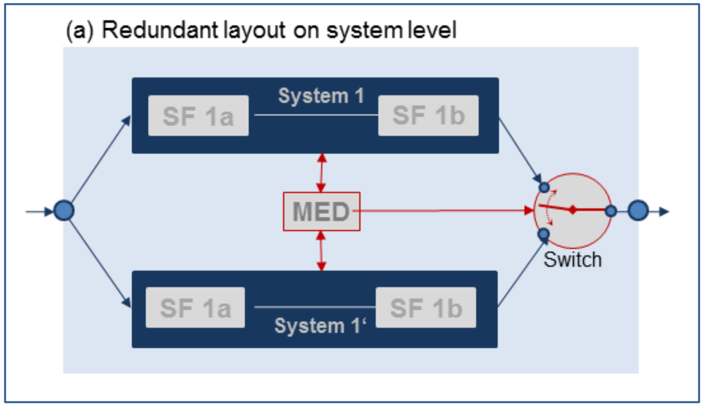
use of same technologies for the redundant system branches:

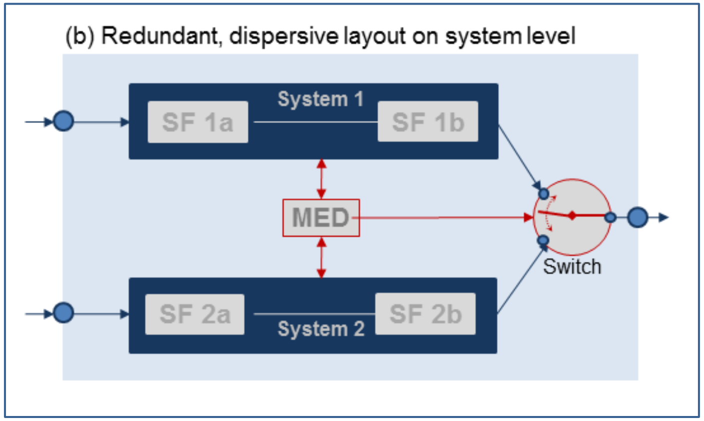
- equal dependencies on errors and threats
- correlated behaviour in the face of threats

(b) functional redundancy

use of different technologies for the redundant system branches:

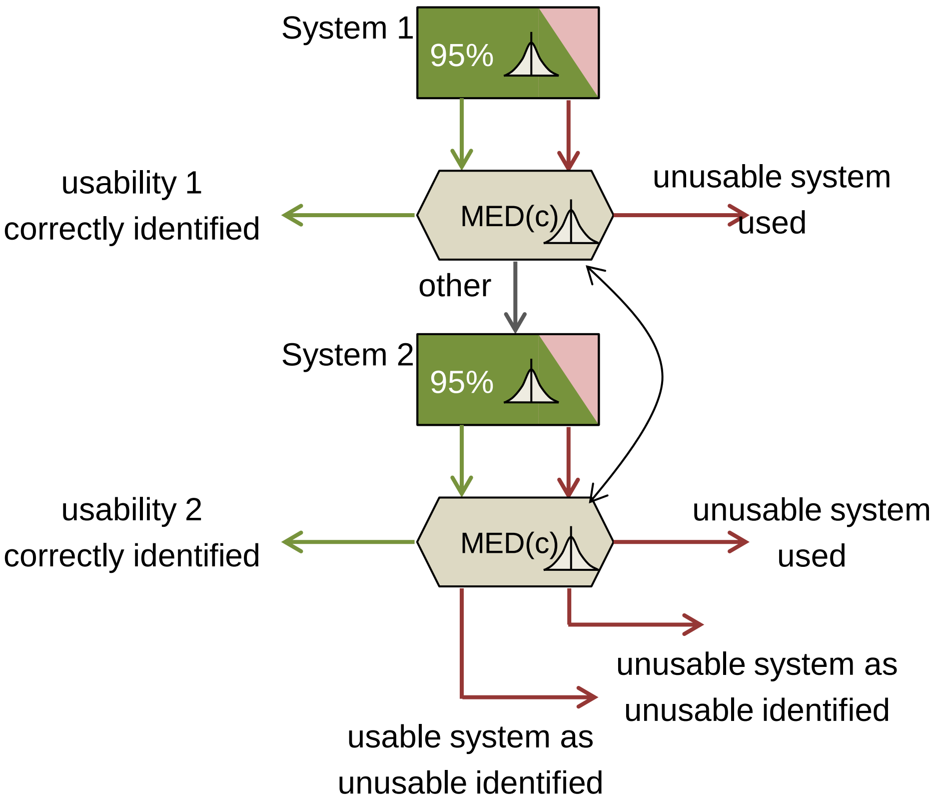
- non-correlated dependencies on errors and threats
- individual behaviour in the face of threats





Resilience by additional capacities (2)

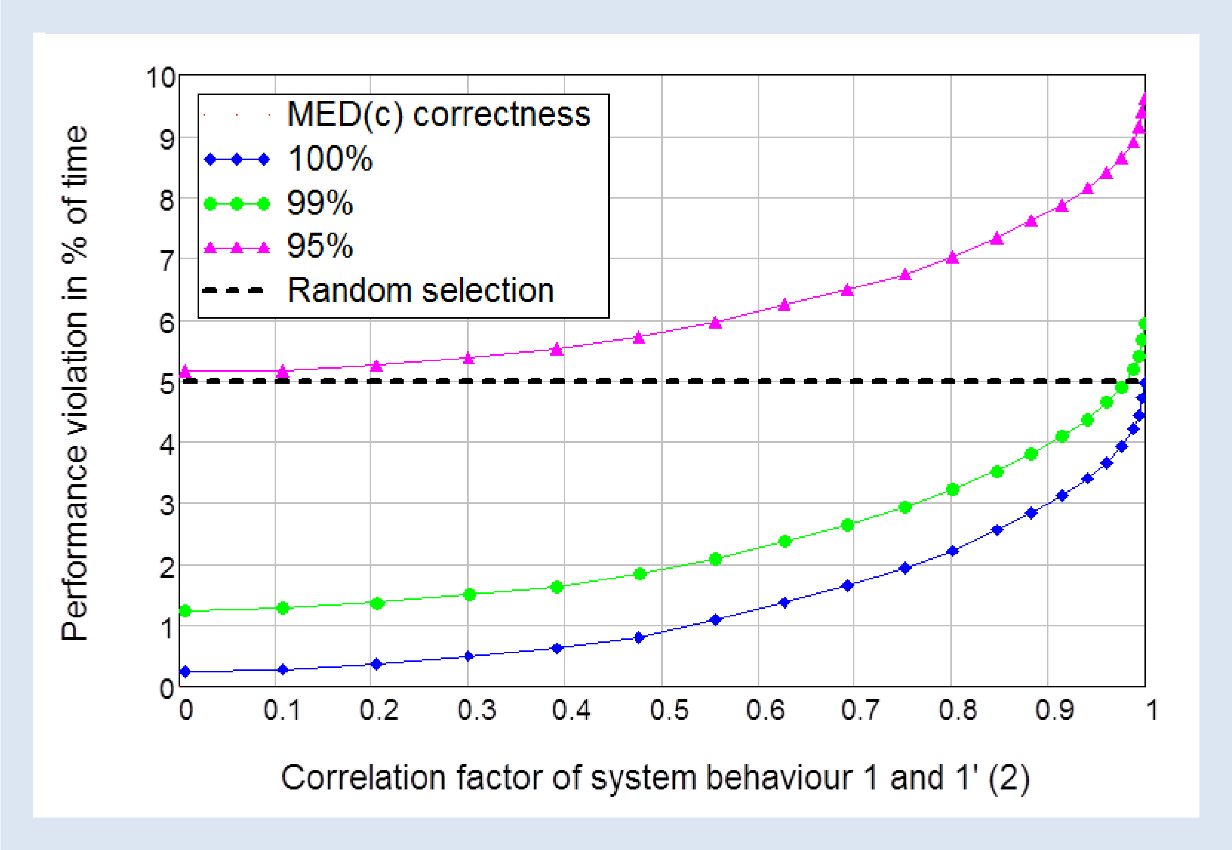
Simulation Setup (N=100.000 epochs)



- Generated random numbers used as criteria of usability or unusability (outside 95% value range)
- Random numbers follow the normal distribution
- Nominal distribution of system 1 and 1'/2 is correlated (CF 0…1)
- MED(c) is considered as one function, correctness is determined based on random numbers of normal distribution

Resilience by additional capacities (3)

(c) Influence of MED(c) and correlation factor on performance violation of the redundant system



- most benefit, if redundant system branches are uncorrelated in relation to threats (blue,CF=0: R=99,75%)
- the benefit is lost,
  - if redundant branches are fully correlated (blue,CF=1: R=95%)
  - if MED(c) makes a random selection of used branch (black dashed line) or
- MED(c) is effectively an extension of the system and influences the reliability of the whole system
  - a high correctness of MED(c) is necessary to achieve any improvement of reliability (green curve vs. pink curve)

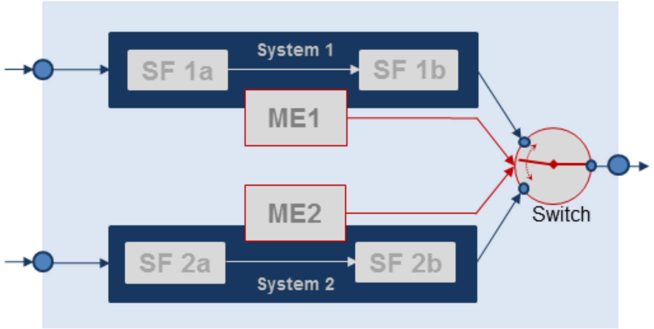
CF = Correlation Factor, R = Reliability

Resilience by flexibility (1)

Principles

- **localized capacity**
  to perform the functionality using distributed resources
- **drift correction**
  to mitigate risks by adjustment to changes
- **neutral state**
  to ensure true situation awareness for right decisions

(a) Redundant layout with dispersive ME1/ME2



Case study

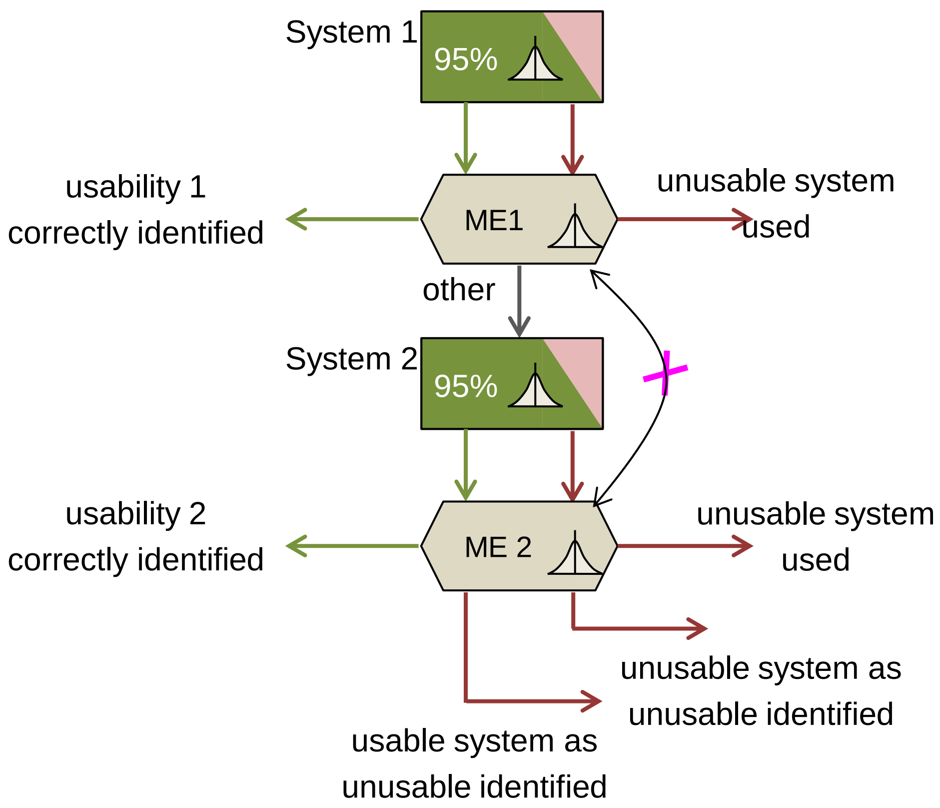
(a) physical with more or less functional redundancy as used in the first case study

(b) Monitoring and evaluation is done separately per each redundant system branch

- non-correlated dependencies on errors and threats
- individual behaviour in the face of threats

Resilience by flexibility (2)

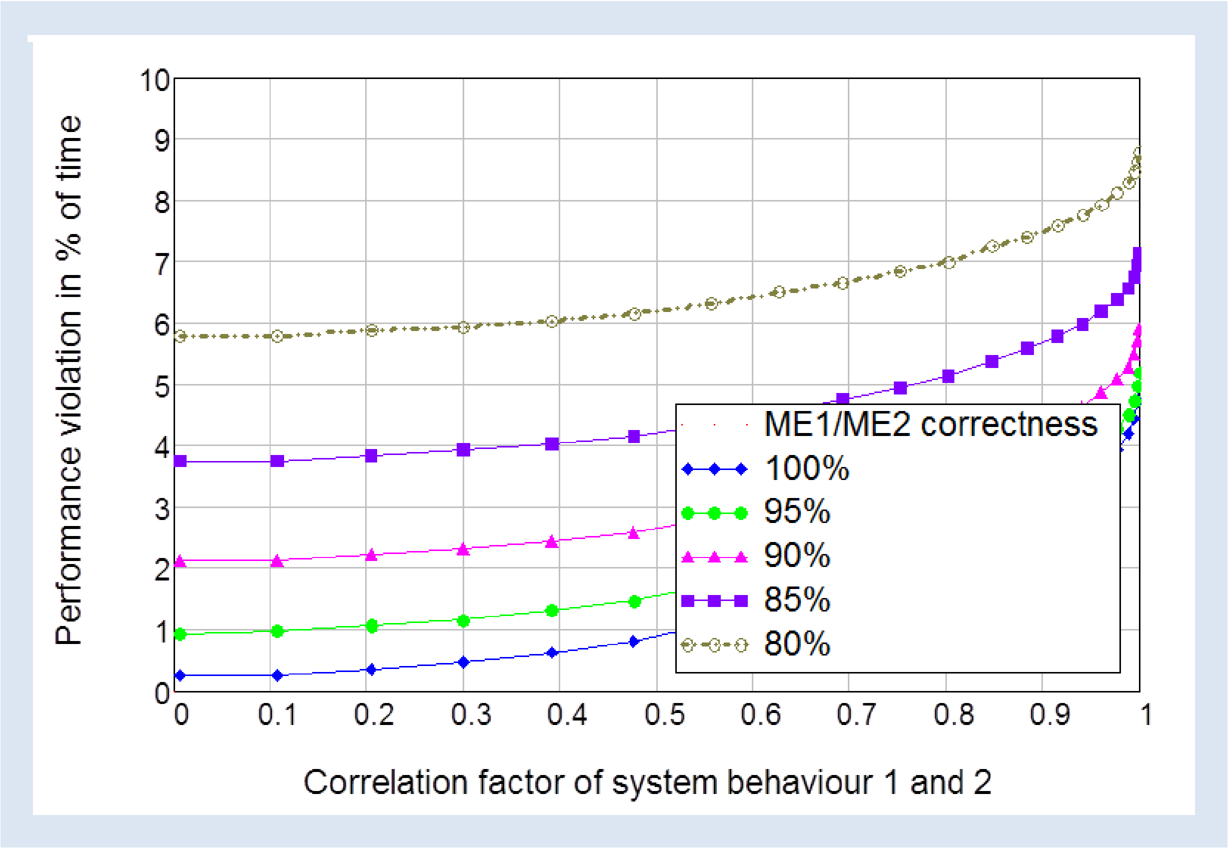
Simulation Setup



- Generated random numbers used as criteria of usability or unusability (outside 95% value range)
- Random numbers follow the normal distribution
- Nominal distribution of system 1 and 1'/2 is correlated (CF 0…1)
- ME1 and ME2 are considered as independent functions, correctness is determined based on random numbers of normal distribution

Resilience by tolerance (2)

(b) Influence of MED(c) and correlation factor on performance violation of the redundant system



- If MED(c) as well as ME1/ME2 operate error-free, the kind of implementation has no influence on reliability. (blue curve)
- The sensitivity against reliability of MED(c) reduces, if it is performed with distributed resources ME1, ME2 and switch.
  (green, pink, and purple curves)
- Also here the benefit is lost,
  - if the correctness of ME1/ME2 sinks below 80% (brown curve)
  - if redundant branches are strongly correlated (CF→1)

CF = Correlation Factor, R = Reliability

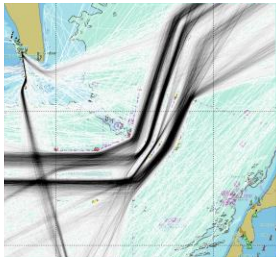
Resilience by tolerance and flexibility (1)

Principles

- **human in the loop**
  to use humans' better dealing with unprecedented threats
- **reduction of complexity**
  to limit the complexity to the necessary degree
- **reorganization**
  to adjust structure and functioning to current situation
- **reparability**
  to be prepared for recovery of origin functionality and performance
- **loose coupling**
  to limit error propagation in complex, networked systems
- **inter-node interaction**
  to ensure communication, cooperation, collaboration between nodes for a coordinated use of resources
- **reduce hidden interactions**
  to avoid harmful interactions between nodes

Case study: Collision Avoidance

AIS based vessel tracks 2003-2008



Pro human in the loop

- as flexible supervisory instance
- skills to detect known and unknown anomalies
- capability to handle unintended surprises

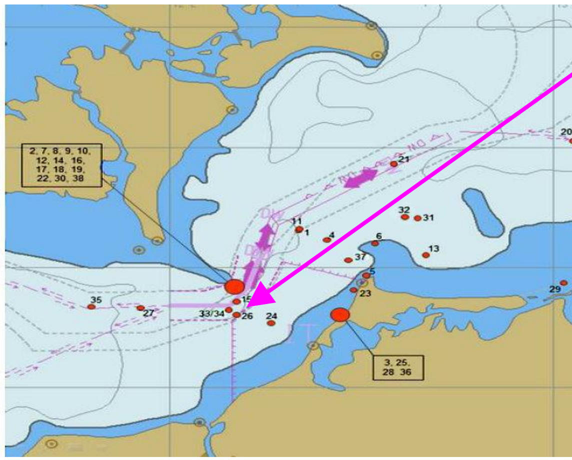
Contra human in the loop

- studies speaks of 50 up to 90% of collisions and groundings caused by human errors
- availability of qualified personnel is getting more difficult
- occupational conditions
- costs…

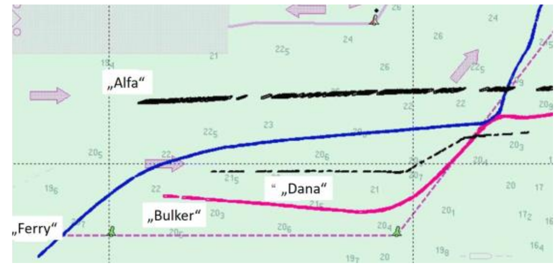
Resilience by tolerance and flexibility (2)

Most serious collisions and grounding (1990-2001)

1. MS Kalliopi (1991)
2. MT Minerva (1994)
3. MS Birkenwald (1994)
4. MS Star Trader / MS Petsamo (1995)
5. MS Kelme (1995)
6. MS Sond / MS Stera (1996)
7. MS Meloi (1996)
8. MS Faworita (1996)
9. MS Christian Paul Palmsalk (1996)
10. MS North Pazifik (1997)
11. MS Aerosmith (1998)
12. MS Francesco (1999)
13. MS Kiaki / MS Ahrenshoop (1999)
14. MT Seajoy (1999)
15. FK Clara / MS Henza (1999)
16. MT Highland Faith (1999)
17. MT Clement (2000)
18. MS Stone Topaz (2000)
19. MS Friendly Ocean (2001)
20. MS Maria / MT Lenaneft2068 (2001)
21. MT Baltic Carrier / MS Tern (2001)
22. MS Nikolaos P (2001)
23. MS Hannes (2003)
24. Schl. Storesund + Barge Aarsleff (2004)
25. MS Lerrix (2005)
26. MS Finnsailor / General Grot-Rowecki (2005)
27. MS Kristina Regina / Pioneer+Barge (2007)
28. MS Ladoga 3 (2007)
29. MS Petri (2009)
30. MS Trust Pioneer (2009)
31. MS Penrhos Bay (2010)
32. Schl. Hans (2011)
33. Schleppzug Westsund / Aarsleff Jack 3 (2011)
34. MS Johanna (2011)
35. MY Da Tiga (2012)
36. MS VYG (2012)
37. Schl. Este (2013)
38. MS Almeria (2013)



AIS tracks of collision scenario 26



- calm weather with good visibility
- ship bridges are properly manned
- ships are equipped in compliance with SOLAS requirements

Causes of collision scenario 26

- collision between “Ferry” and “Bulker” occurred after “Bulker” having initiated a course change to northeast
- technical shortcomings in transmission schemes
- faulty data transmitted

Helpful resilience principles

- 2nd human in the loop (VTS) acting as
  - ➢ independent monitoring instance (loose coupling)
  - ➢ additional capacity to trigger additional demand on coordination and adjustment (reorganization of responsibilities, inter-node interaction)

DLR

Topics

1. Introduction
   - Resilience as challenge
   - Resilience principles
   - Situation awareness

2. Ships‘ Navigation System
   - Carriage Requirements
   - System for Detection and Indication of Threats
   - Threat Management

3. Case Studies
   - Resilience by additional capacities
   - Resilience by tolerance
   - Resilience by flexibility

4. Summary

Summary

- **Safe and efficient ship operation depends on (amongst others):**
  - ✓ reliable provision of nautical data and information
  - ✓ situation assessment and awareness as recurring task
  - ✓ ability to adjust the operation to changes of internal and external conditions (including interfering influences, emerging threats,…)

- **Monitoring is one of the cornerstones of resilience and an essential prerequisite for situation awareness, needed:**
  - ✓ to model behaviour/conditions for the design → to become resilient
  - ✓ to assess states and conditions → to control the
  - ✓ to detect internal/external threats → to protect resilience
  - ✓ to evaluate the effectivity of means managing/protecting the resilience → to maintain resilience

- **Resilience principles**
  - ✓ the application is not new
  - ✓ are recognized as general approaches to ensure resilience
  - ✓ have to be concretized taking into account the specified resilience criteria

….but becomes only effective based on the holistic consideration and coordination of interactions and dependencies on socio-technical level….

DLR