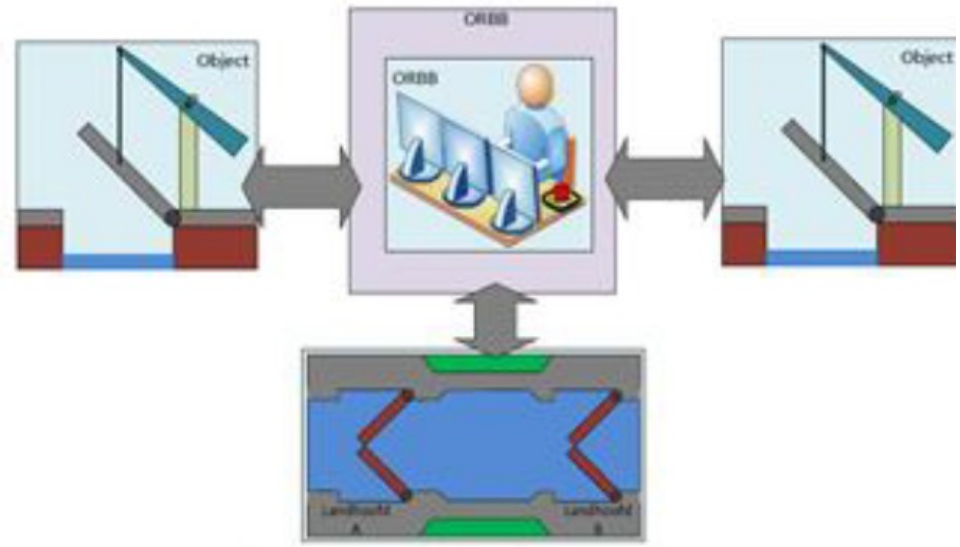


Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

Risk Assessment for a Uniform Workstation for Control and Supervision of a Shipping Lock

Martijn Flinterman
Anne van der Heiden

Contents

- Introduction of Rijkswaterstaat
- The Delden and Hengelo Locks
- STPA: Findings and usefulness
- Comparison with other used risk assessment methods
- Conclusion

Rijkswaterstaat

- Founded 1798
- Dutch government agency
- 8800 staff
- Regionally oriented and nationally controlled
- Responsible for Dutch main infrastructure:
  - design
  - construction
  - management
  - maintenance

Dutch main road network

- Highways (3102 km)
- Driveways, exits and connecting roads (1259 km)
- Overpasses, ecoducts (2540)
- *Fixed and movable bridges (715)*
- *Road tunnels (15)*


CineMec

Dutch main watersystems and waterways network

- fresh water (5000 km²)
- salt water (59000 km²) with
  - dikes, dams and dunes
  - 4 *storm surge barriers*
- 100 objects for water level management:
  - *Locks*
  - *Pump houses*
- canals and rivers
  (1686 km)
- navigable channels
  (6165 km)
- *422 bridges*

Storm surge barriers

Movable bridges

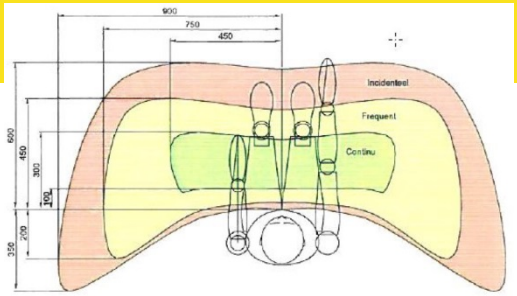
System goals of the Delden & Hengelo Locks

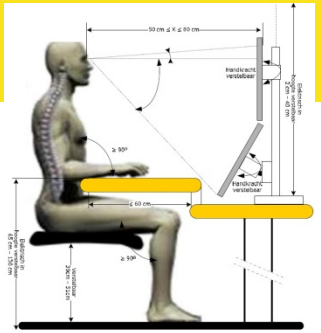
- Passage of professional shipping and pleasure craft, across Twente Canal (Eastern Netherlands);
- Regulation of water by draining the lock.

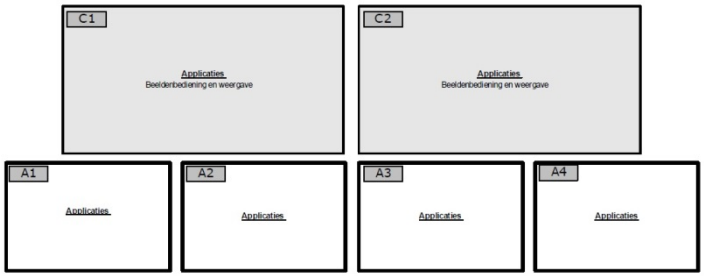
“ORBB”: Central operating stations

- Rijkswaterstaat increasingly uses *central operating stations*.
- Uniform workstations: component, used for:
  - road tunnel operation;
  - bridge and lock operation.
- Uniform interface between workstation and object.
- All operating applications accessible at one desk, through process manager software.

Operator’s workplace





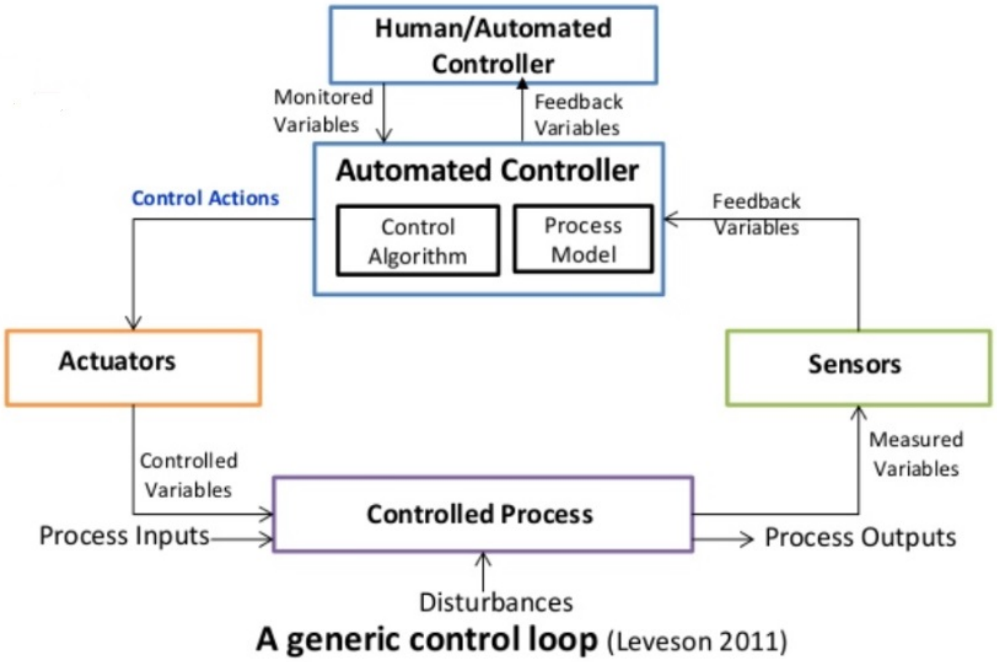


- Furniture (desk & chair)
- Monitors
- Means of communication with skippers
  - Microphone, headset, foot pedal (activates microphone), telephone, speaker (marine VHF radio, intercom, Scada signals)

multifunctional touch panel

- Process controls
  - Mouse, keyboard, joystick (turns and zooms camera), cardreader
- Safety controls
  - Routable Emergency Stop: routed when the operator switches to another object to operate.

ORBB Risk analysis



A generic control loop (Leveson 2011)

- Movable bridges and locks are machines.
- Operators adapt and "complete the design"; feedback loops exist

  Inspect – Operate – Monitor – [repeated]
- We used STPA to study the process flow together with *the actual field experts*.
- The project team initially assessed the risks of the workstation through:
  - using worst-case scenarios (EN-ISO12100).
  - FMECA: possible defects considered and assessed for each component.

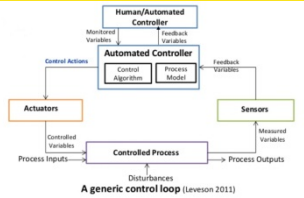
Why use STPA within our organisation?

"The control algorithm is created by a human using a process model of what he or she thinks will be the operating states of the controlled process. Unsafe automated control algorithms may result if the designer of that algorithm has an incorrect understanding (process model) of the required behavior of the automated controller."

– Leveson: An STPA Primer

- A meta-analysis of accident investigations (Rijkswaterstaat, 2017) has pointed out that:
  - *'A bridge or lock (door) is closed too soon'* is a dominant unsafe control action;
  - In 75% of accidents an incorrect process model was the most significant contributing factor, e.g.:
    - Illogical camera images;
    - Lack of cohesion between images; other factors/interactions?

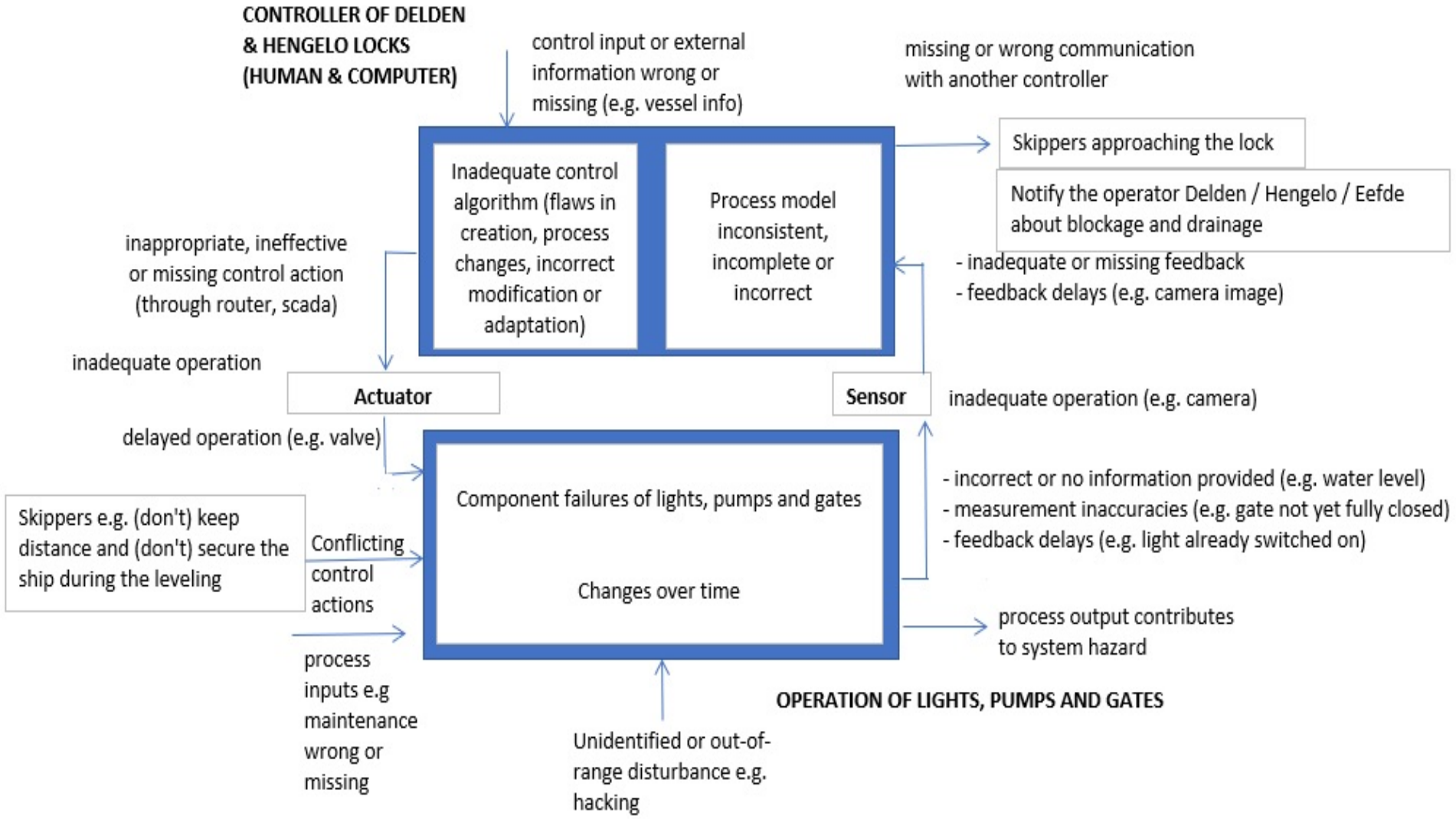
STPA preparation steps



A generic control loop (Leveson 2011)

- System accidents:
  - Damage to lock chamber / gate
  - Damage to the ship and / or injury of people on board
  - Grounding of ships
- System hazards:
  - Ship collides with front lock gate
  - Lock gate (entrance) closes while a ship is sailing in
  - Ships collide while entering the lock chamber
  - Ship collides with lock chamber
  - Water level is too low or too high
- System constraints
  - Ship keeps distance from the front lock gate
  - Back gate closes when all ships are inside the lock chamber
  - Ships keep distance from each other
  - Secure the ship at several bollards
  - Maintain water level

STPA control structure



Unsafe control action

- Yaughts sail too close to front gate. Yaughts sail up too early, because of fear of not being able to join in.
- Operator gives the door close command before ships are in lock chamber.
- Yaughts moor only at one mooring point, while the bollards are too far apart.
- Operator does not maintain water level if he sees two conflicting data in water management and lock operating system.
- Operator does not maintain water level correctly if lock is opened too often.

Individual constraint

- Operator instructs by VHF and, where necessary, per public address system, if ships enter too early.
- Administrator presents camera images in a logical manner including a time display and identification code showing that the correct lock is being operated.
- Manager provides bollards every ten meters.
- Administrator unifies the source for the water level in systems.
- Operator adjusts number of lock operations to required water level.

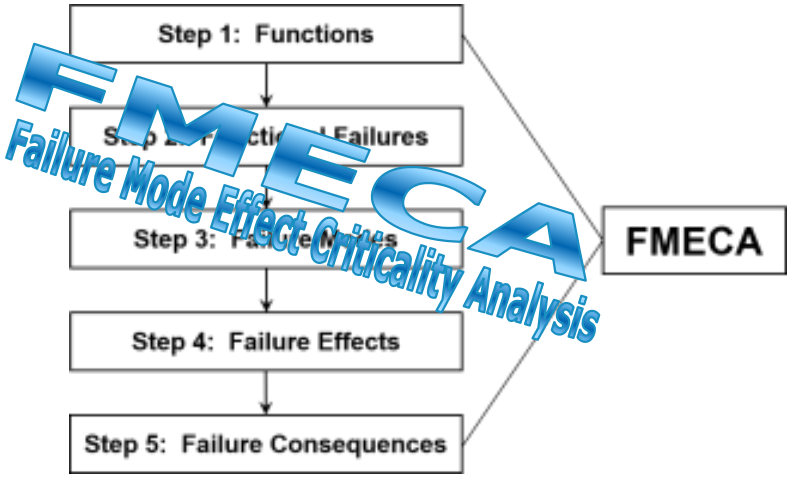
Assumptions & Leading indicators for the SMS

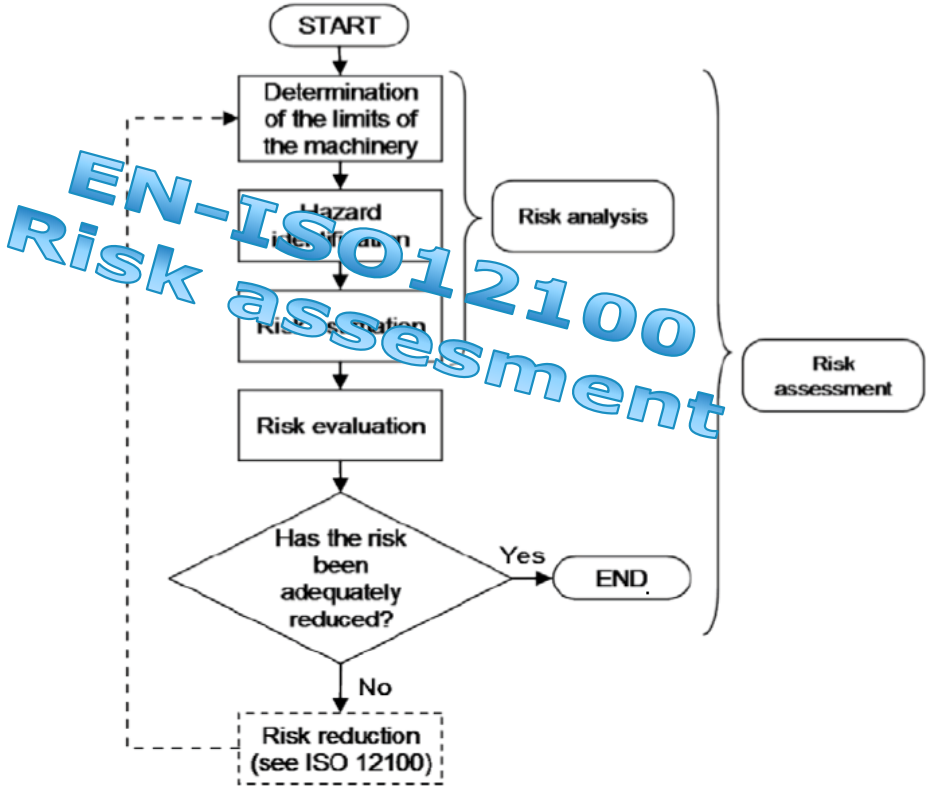
- The current prescribed method of operating more than one lock or bridge per operator does not lead to unsafe control actions.
- Questions from (maintenance) personnel and visitors, and VHF calls for other locks and bridges in the neighborhood do not hinder control actions.
- There are no notable workarounds that are not included in the object-specific operating instructions.

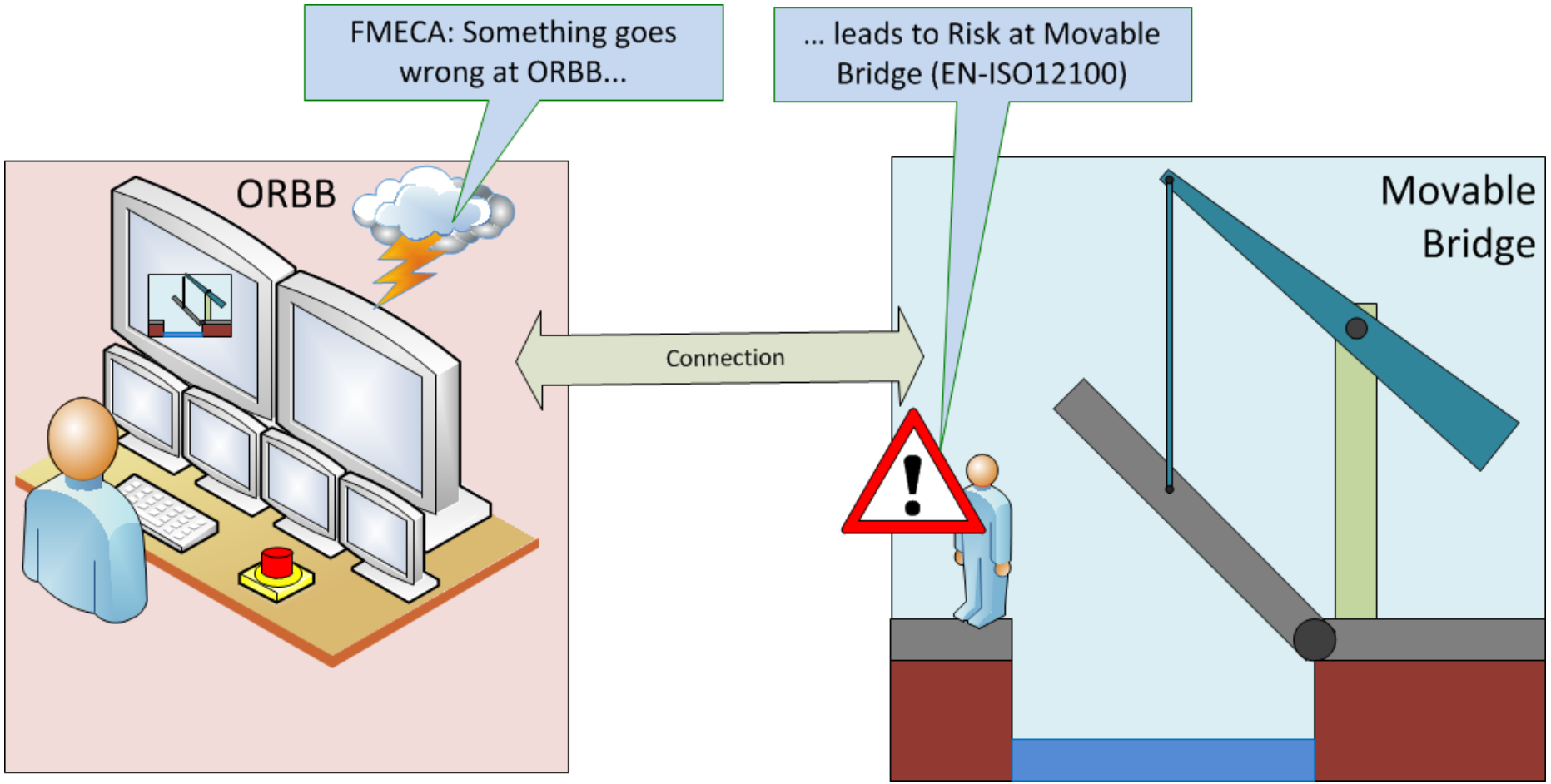
- Sample # of missed / delayed monitoring actions for various combinations of objects.
- [HF task analysis]
- Local rationality research: Ask operators what *requirements and pressures* lead to work-arounds and considerations in favor of efficiency.

ORBB projectteam used **combination** of **FMECA** and **EN-ISO12100 Risk assessment** to identify and quantify risks of the uniform workstation:

- FMECA to identify failure's in ORBB components;
- EN-ISO12100 to estimate risks on nautic object due to ORBB failure






FMECA: Something goes wrong at ORBB...
... leads to Risk at Movable Bridge (EN-ISO12100)
ORBB
Connection
Movable Bridge

Failure modes of the automation components (FMECA)

- Failure modes:
  - Broken components:
    - Chair, desk, displays, switches, routers, cables, microphone, speaker, mouse, joystick, keys, touch panel.
  - No power / unsecured plugs
  - No connection to database
  - Configuration / code failure
  - Transmission delays
  - Overload / induction, incorrect EMC filter / failing EMC hardware
  - Freezing / delay of SCADA client/server, control and presentation system, display presentation,
  - No communication between SCADA client/server
  - Shutdown / disconnect by ORBB controller
  - Maintenance by third parties
  - Hacking

Risk Assessment for safe operation following EN-ISO12100

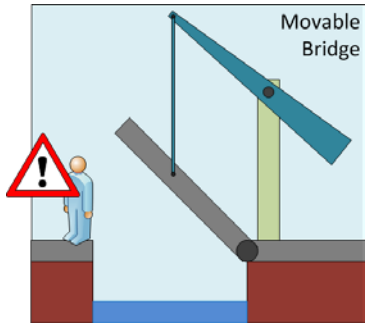
- Operator does not adequately respond to dangerous events or cannot determine if situation is safe.
- *Physiological factors*
- *Conflicting information*
- Distraction by *operating multiple objects* from a control location.
- Dangers due to *transfer of control* (object not in rest, more than one location in use).
- *Excessive workload* resulting from repetitive work due to many operations in relation to passing road / waterway traffic.
- Operator does not view traffic situation before operating.
- “Insufficient operator attention”.
- Low work pressure leads to weakened attention when operating.

Risk Assessment (cont'd)

- Ergonomics and noise.
- Uncertainty about instructions, tasks, responsibilities, competencies.
- Task analysis, training and procedures needed for redesign.
- Operator cannot orientate by overview provided of the entire object.

Identified risks at Movable Bridge / Waterlock: due tot failure ORBB

- Major injury / death by being trapped, crushed, drowned or falling of heights due to moving objects or by startle reaction.
- Estimate risk by parameters:
- - Se (Severity of Harm)
- - Fe (Frequency and duration of exposure)
- - Pr (Probabiltiy of occurrence of a hazardous event)
- - Av (Possibility of Avoiding of limiting harm)



Risk reduction measures prescribed order:

-1 Eliminate source of risk

-2 Add protective measures

-3 Inform user (safety instructions)

1) ***Eliminate source of risk***: most of the times not possible.

2) ***Add protective measures***:

- Choose sound and reliable equipment.
- Connecting PTZ camera to strategic positions.
- Set presets by operator.
- Add *round trips* and *feedback loops* to detect failure in equipment

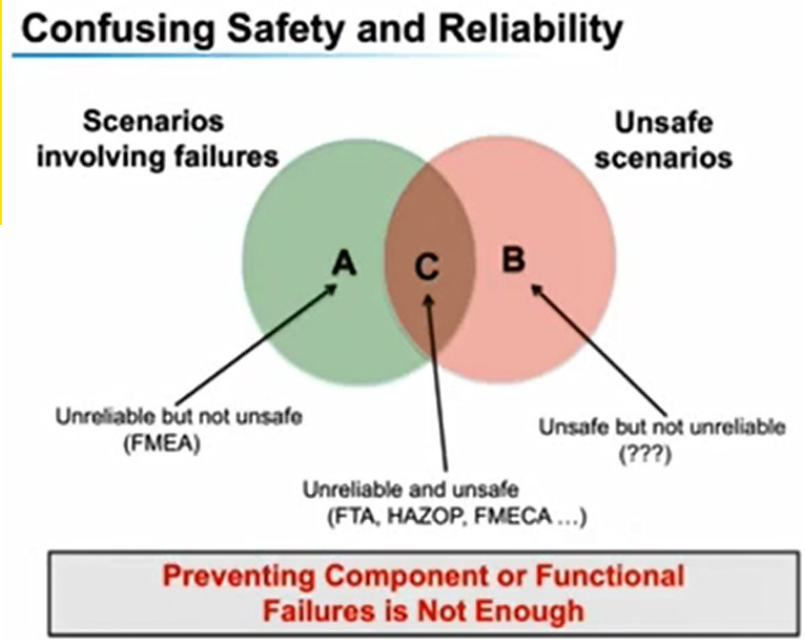
3) ***Inform user (safety instructions)***

- Train operator, to recognize unsafe situations and how to handle
- Perform periodic visual inspections, (diagnostic) tests.
- Visual check:
  - Camera images contain object code that is displayed.
  - Object name is indicated on GUI

3) *Inform User* (Safety instructions) continued

- Personnel and passers-by may not enter or stay in the lock gate during movement.
- Resetting safety devices shall be done by an expert;
- At night, the bridge must be in the 'out of service' position and shut down to prevent unauthorized operation.
- The lock should not be operated when:
- The monitor (s) does not display an image;
- In the evening the lighting is not switched on.
- Personnel and passers-by should not be on or near the pivot points during the movement of the moving parts.
- Operation of the object is only permitted by persons trained and appointed by the administrator.
- Equipment cabinets may only be opened by authorized and designated persons.
- Use of work permit with planned maintenance.

Conclusion



- Risk Assessment cf. EN-ISO12100 (putting up barriers) and FMECA (preventing failure events) work for known failure modes and random failure.
- “STPA does not cancel other methods”, but is additionally needed for potential interactions between components, complex system design and system failures.
  - A lot has gone awry before the controller can make an error.
  - Accidents often happen when the process model is inadequate.
  - A human controller must remain in the loop.
  - Check for your assumptions.

Sources (in alphabetical order)

- Karanikas, N. (2018), Masterclass Risk Assessment Syllabus, HvA
- Krosse, H. (2018), Onderzoek machineveiligheid en functionele veiligheid ORBB, Etten-Leur: D&F Consulting.
- Leveson, N. (2011), *Engineering a Safer World – Systems Thinking Applied to Safety*, Cambridge MA: MIT Press.
- Leveson, N. (2013), *An STPA Primer,* Cambridge MA: MIT.
- Leveson, N. and John P. Thomas, *STPA Handbook*, Cambridge MA: MIT.
- Hollnagel, E. (2011), *Resilience Engineering and Safety Management – presentation for Dutch Contact Group Health and Chemistry.*
- Shorrock, S., J. Leonhardt, T. Licu and C. Peters (2014), *Systems Thinking for Safety: Ten Principles - A White Paper Moving towards Safety-II*, Eurocontrol.

[Reserve dia’s]

ORBB Applications

- Nautical display and operation (mandatory; fixed presentation of images):
  - Display and operation of lock and water pumping station;
  - maintenance control and malfunction display and handling;
  - image control, lighting and signaling;
  - Autorisation and object selection;
  - Displaying and using means of communication;
- Object image display and operation (ditto)
- Radar display and operation
- Information and Tracking System for Shipping
- Office applications display and operation
  - Digital Journal
  - Information Systems: Meteo, Water Regulation, Infrastructure, Automatic Identification.