Case-studies exploring STPA in digitalization and autonomy

Børge Rokseth
Borge.Rokseth@ntnu.no

Department of Marine Technology, NTNU

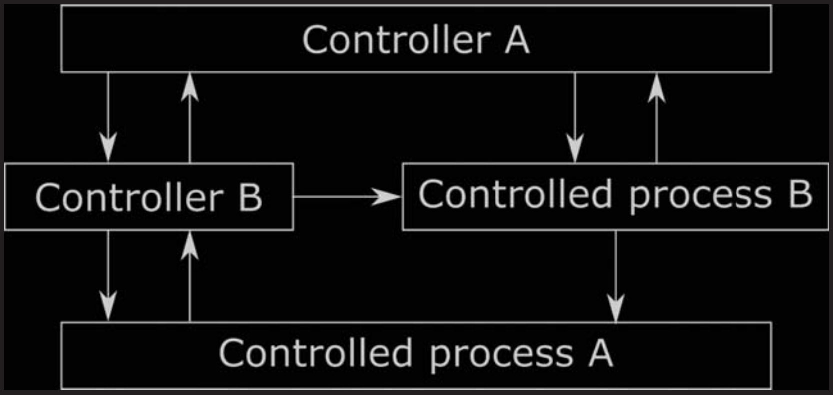
STPA

Case studies: Power management aboard a DP vessel

Discussion

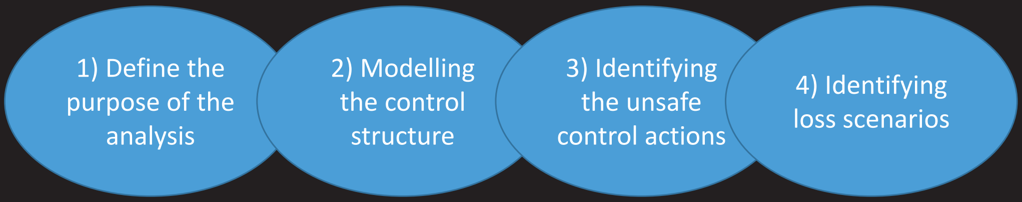
STPA

STPA



Accidents are caused by inadequate control

STPA in four steps



1) Define the purpose of the analysis

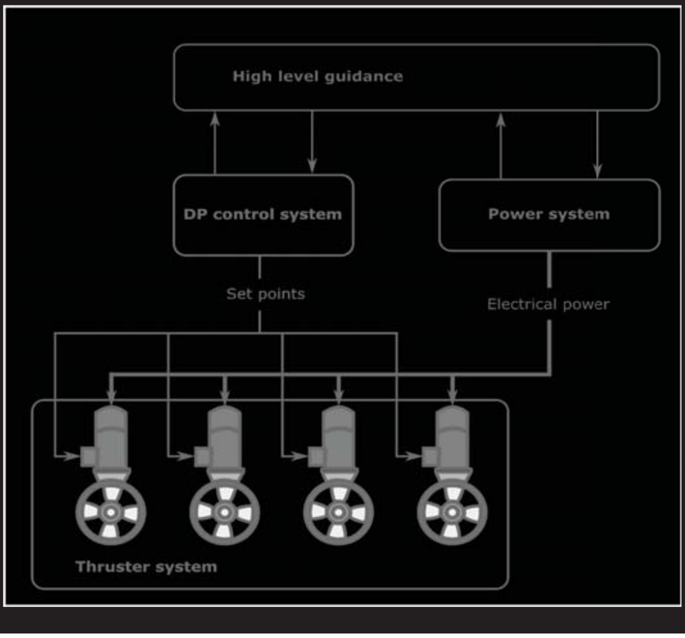
2) Modelling the control structure

3) Identifying the unsafe control actions

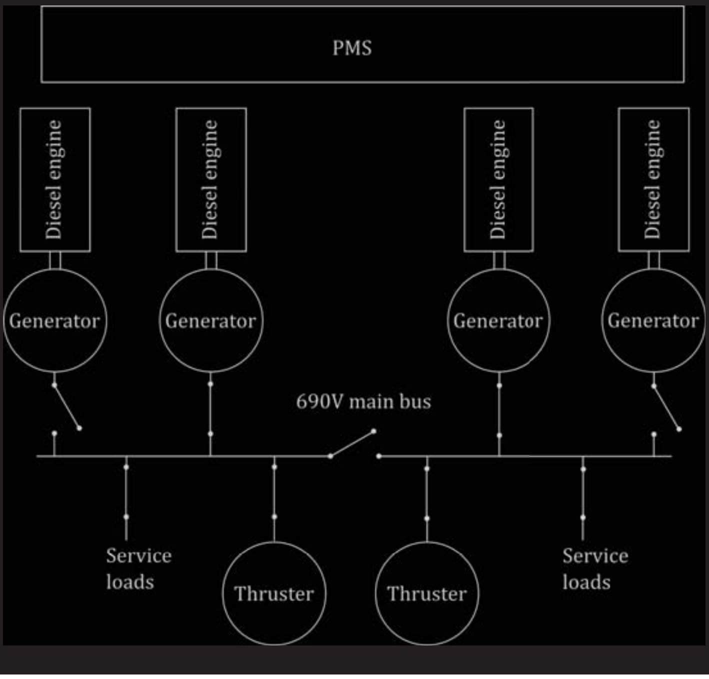
4) Identifying loss scenarios

Case studies

Background: Dynamic positioning



Background: Diesel-electric propulsion



Case Study 1

A generic DP-vessel with a DPO on the bridge

https://c1.staticflickr.com

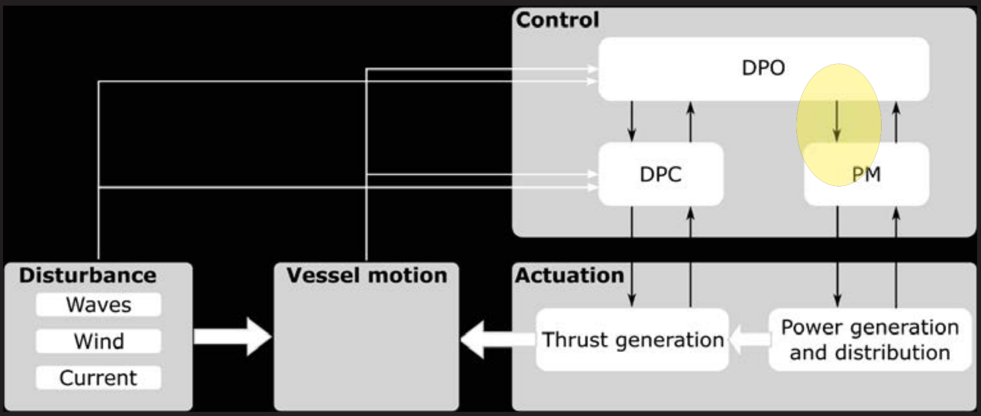
http://www.shipspotting.com/

Rokseth, B., Utne, I. B., & Vinnem, J. E. (2017). A systems approach to risk analysis of maritime operations. *Journal of Risk and Reliability*, *231*(1), 53–68. https://doi.org/10.1177/1748006X16682606

Case Study 1: Defining the purpose

- **Losses:**
  - Loss of life, damage to property or the environment, or loss of mission due to unsuitable motion of the vessel
- **System-level hazards:**
  - Vessel motion is not controlled according to motion-control objectives
    - Adequate amounts of power are not available for the thrusters
- **System safety constraints:**
  - Adequate amounts of power must be made available for producing the required thrust force

Case Study 1: Modelling the control structure



Control actions (DPO):

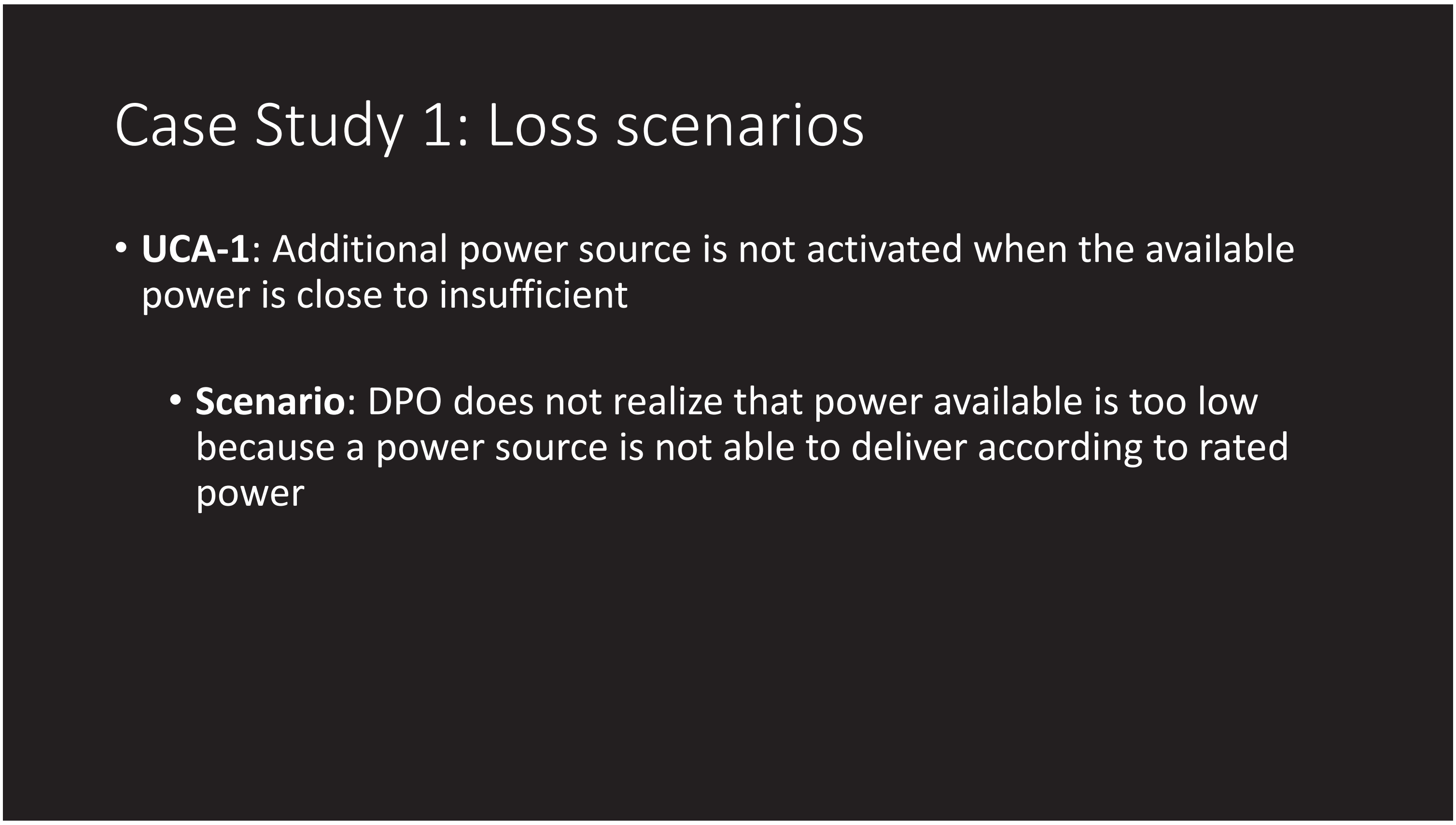
1. Activate power source

Relevant process model variables (DPO):

1. Level of available power
2. Power demand in the near future
3. Active power sources
4. Health state of each power source

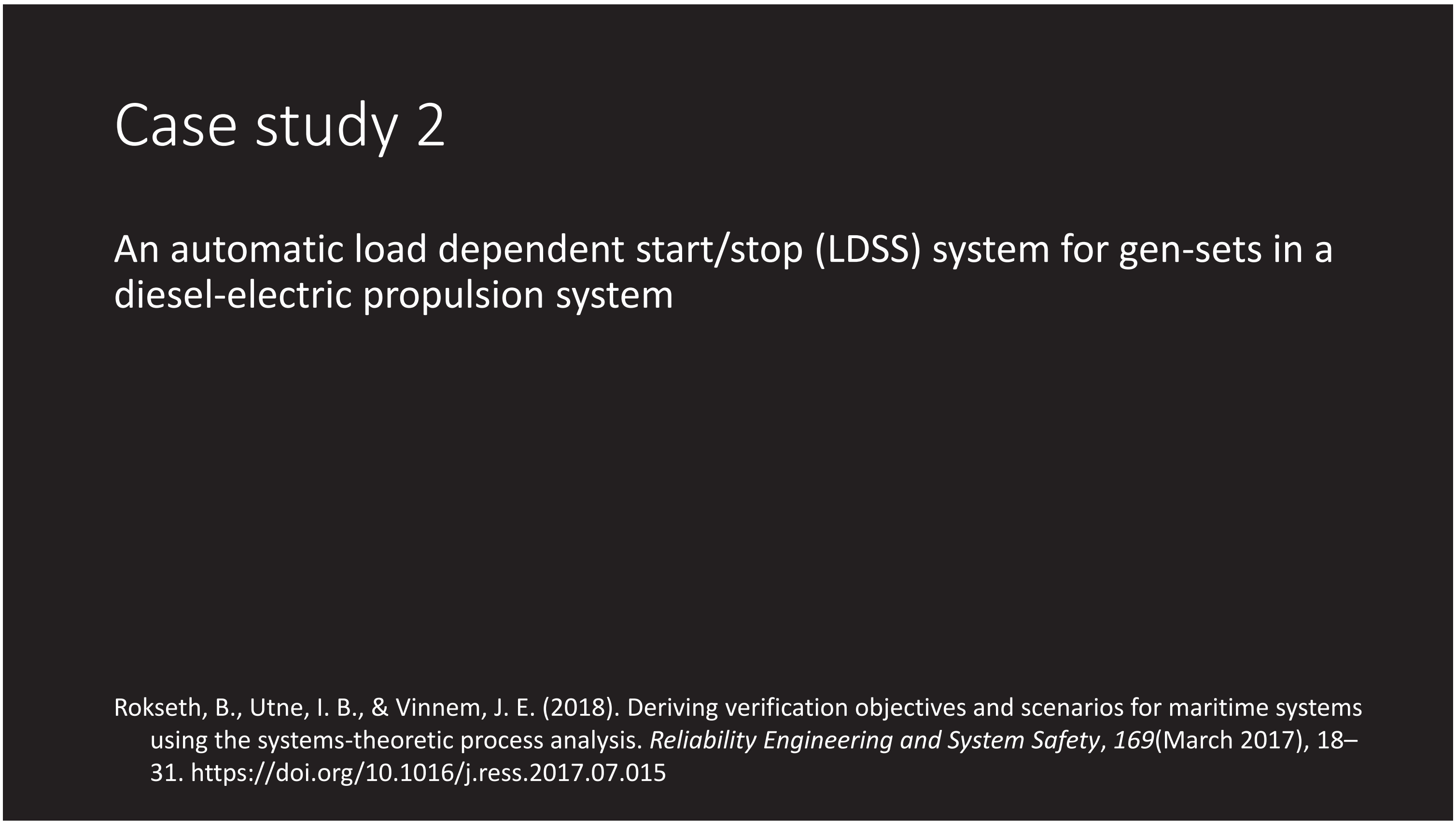
Case Study 1: Unsafe control actions

- **UCA-1**: An additional power source is not activated when available power is close to insufficient
- **UCA-2**: A power source that is not in proper working order is activated
- **UCA-3**: An additional power source is activated too late when the available power is decreasing



Case Study 1: Loss scenarios

- **UCA-1**: Additional power source is not activated when the available power is close to insufficient
  - **Scenario**: DPO does not realize that power available is too low because a power source is not able to deliver according to rated power



Case study 2

An automatic load dependent start/stop (LDSS) system for gen-sets in a diesel-electric propulsion system

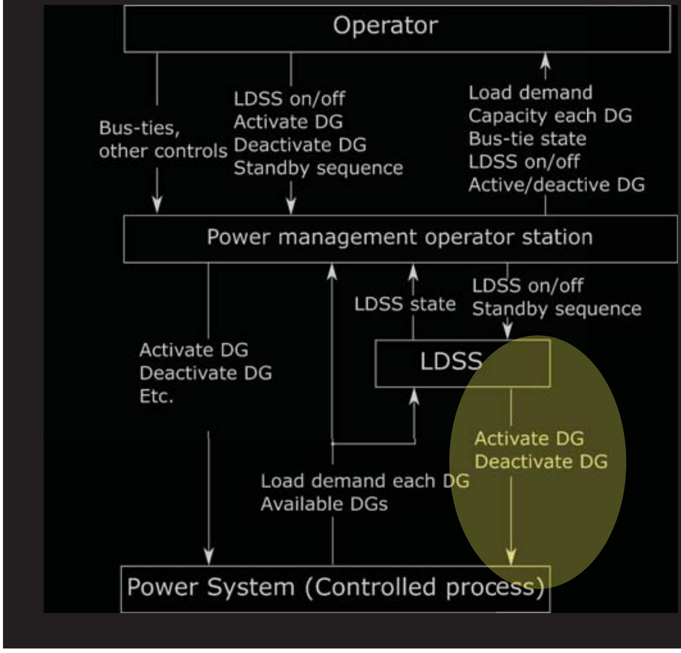
Rokseth, B., Utne, I. B., & Vinnem, J. E. (2018). Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. *Reliability Engineering and System Safety*, *169*(March 2017), 18–31. https://doi.org/10.1016/j.ress.2017.07.015

Case study 2: Defining the purpose

	System accident description
A-1	Power system not able to serve loads *(Loss of motion control)*

	System hazard description
H-1	Available power becomes too low

Case study 2: Modelling the control structure



Control actions (LDSS):

1. Activate gen-set

Relevant process model variables (LDSS):

1. Whether LDSS is on or off
2. The gen-set activation sequence
3. The capacity of each gen-set
4. Level of available power
5. More…

Case study 2: Unsafe control actions

Control action	Control action not provided causes hazard	Control action provided causes hazard
Activate DG (LDSS)	**UCA-9**: Additional gen-set not selected for activation by LDSS when LDSS is active and available power is close to insufficient.	**UCA-10**: Unhealthy gen-set is selected for activation by LDSS.

Case study 2: Loss scenarios

- **SC:** LDSS must activate additional gen-sets when available power is close to insufficient and LDSS is active
  - LDSS is not aware that available power is too low because LDSS perceives the generating capacity as higher than what it actually is
    - **SC:** LDSS must be aware of the actual magnitude of the current generating capacity
      - LDSS may have a wrong belief regarding the capacity of a gen-set because the calibration of a parameter in the LDSS software is incorrect
      - LDSS may have a wrong belief regarding the capacity of a gen-set because its capacity is degraded and the degradation has not been accounted for in relevant parameters in LDSS software

Discussion

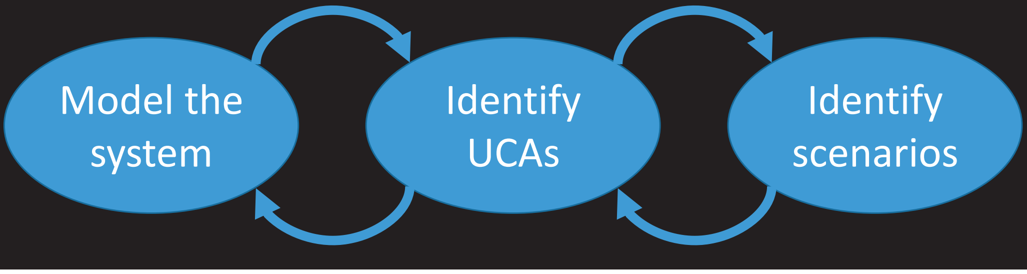
Practical challenges with applying STPA

- Modelling the system:
  - Which level of detail/abstraction?

- My experience: Start at a relatively abstract level and refine as necessary
  - If you are able to formulate unsafe control actions that makes sense, you will be able to get useful information out

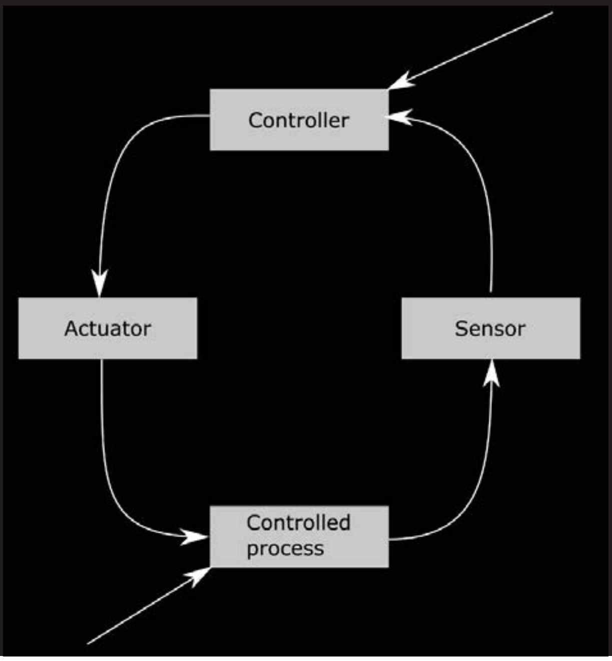
Practical challenges with applying STPA

- Determining relevant process model variables
  - E.g. what must a human operator know in order to satisfy the responsibility of ensuring adequate available power? Not a trivial question!



Practical challenges with applying STPA

- Not much guidance in step 4



Advantages

- Not sensitive to physical implementation
  - Can analyze “black-box” sub-systems. We do not need to understand a subsystem, only its role in the system, to determine appropriate constraints
  - Computer control systems, human operators and organizations are controllers and treated in the same way.
    - → STPA focus on interactions between controllers
- Not so sensitive to how the system is modelled:
  - Consider the two case studies – STPA steps 1 and 2 were solved differently
  - Results points to the same general problems

Advantages

Establishing the system model (control structure hierarchy) is equivalent to e.g. functional/structural decompositions or flow diagrams

- Control loop diagrams are less formal and faster and easier to develop
- Requires less “hard facts” and more “system understanding”

Thank you

Borge.Rokseth@ntnu.no