The Research Council of Norway

DNV·GL

KONGSBERG

AMOS

NTNU – Trondheim
Norwegian University of Science and Technology

A Systems-Theoretic Approach to Verification of Maritime Engineering Systems

Børge Rokseth
Dept. of Marine Technology

Outline

- Dynamic Positioning systems – Short introduction
- Current State of Regulations and Verification - Challenges
- Outline of a new approach for verification
- Case-Study: Finding Generic Verification Objectives for DP-systems using STPA
- Case-Study: Vessel-Specific DP system Verification Program
- Conclusions

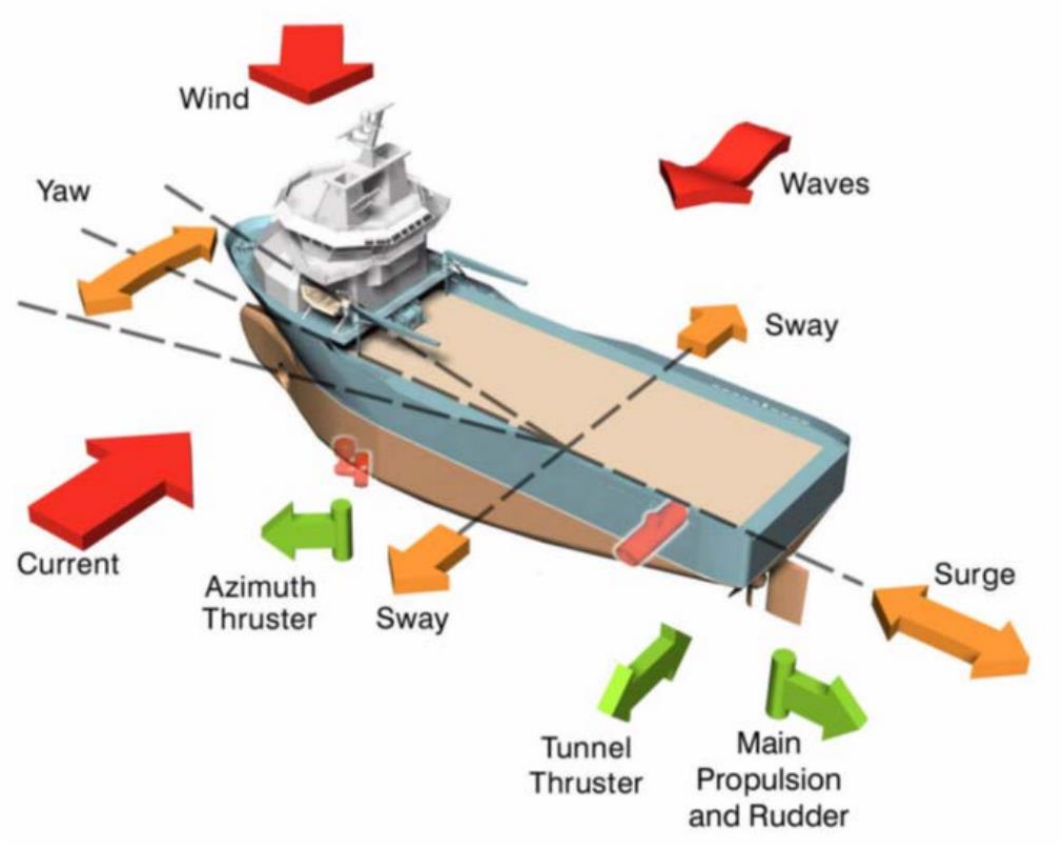
The Research Council of Norway

DNV·GL

KONGSBERG

AMOS

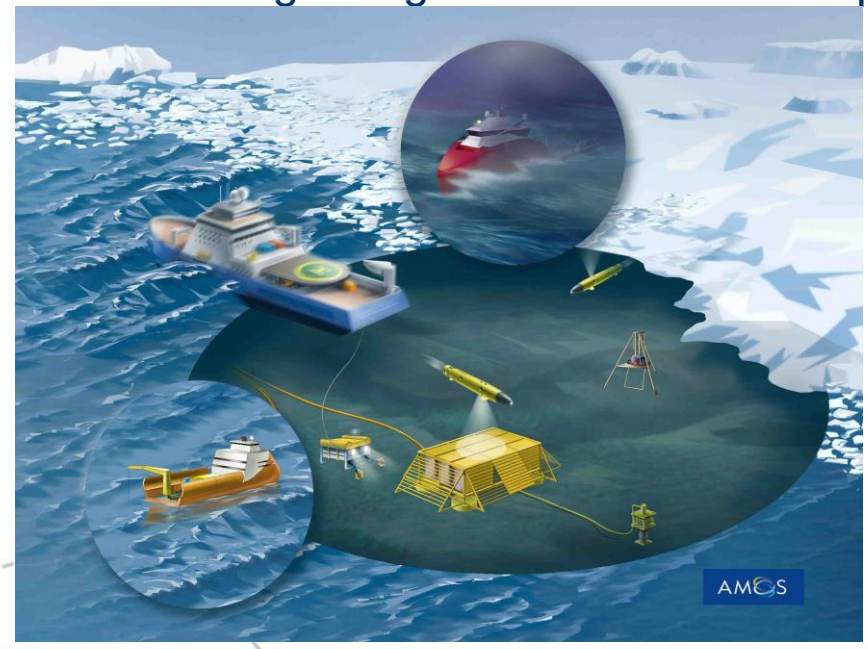
Introduction to Dynamic Positioning Systems



NTNU – Trondheim
Norwegian University of Science and Technology

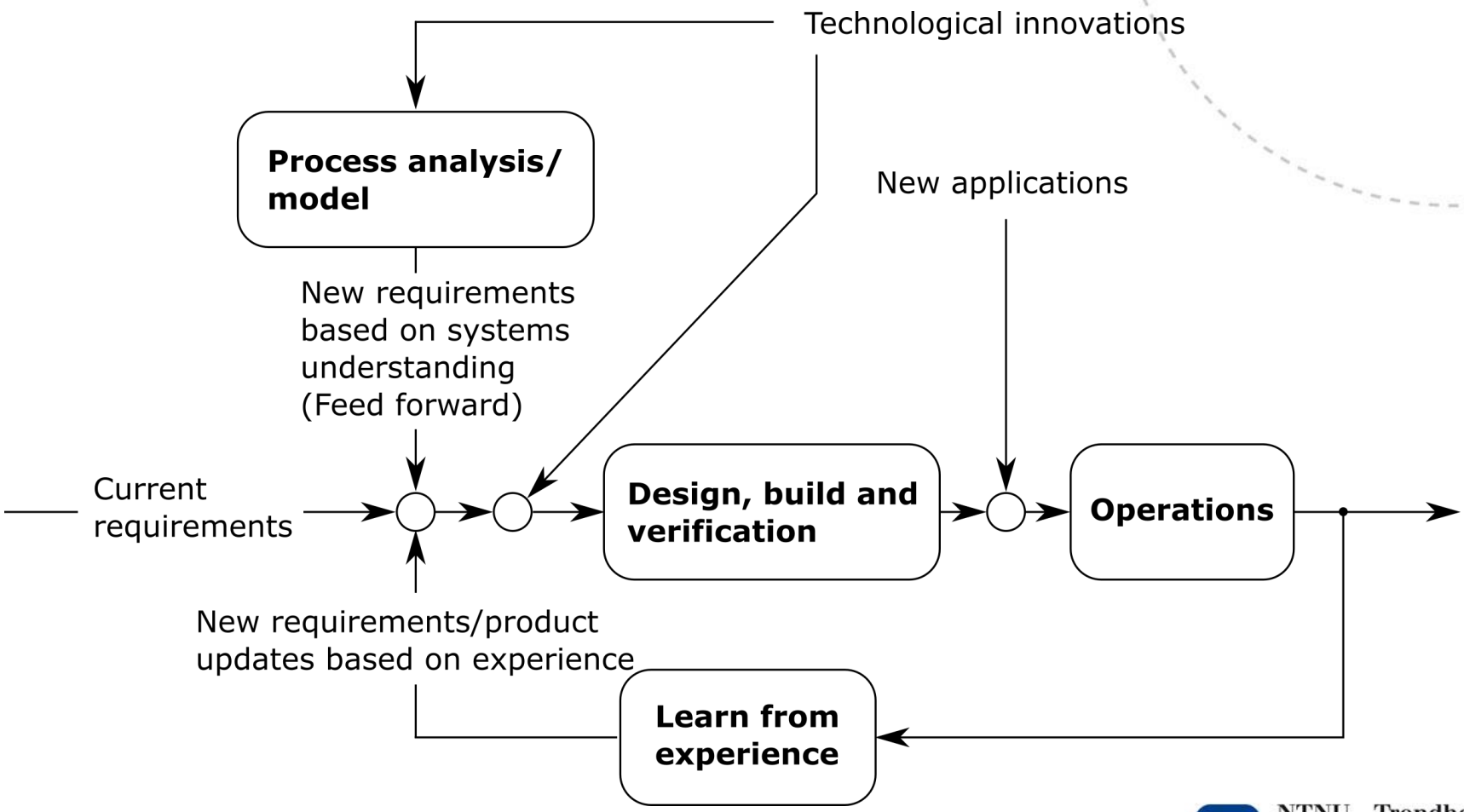
Current State of Regulations and Verification - Challenges

- DP regulations, class-rules and international standards confuse reliability for safety
  - Almost a singular focus on redundancy
- Not sufficient (although important)
- Less sufficient in the future
  - E.g. integrated autonomous operations



- DP system verification process:
  - Verify hardware redundancy using FMEA
  - Perform sea-trials, while failing various sensors etc.
  - HIL-tests (voluntary)

Current State of Regulations and Verification - Challenges



An Outline for a New Approach for DP System Verification

1. Generic study

- Analyze a generic DP-system and find safety constraints and requirements
  - High level of abstraction
  - Use STPA
- Derive high-level verification objectives based on the high-level safety constraints and requirements

2. Vessel-specific study

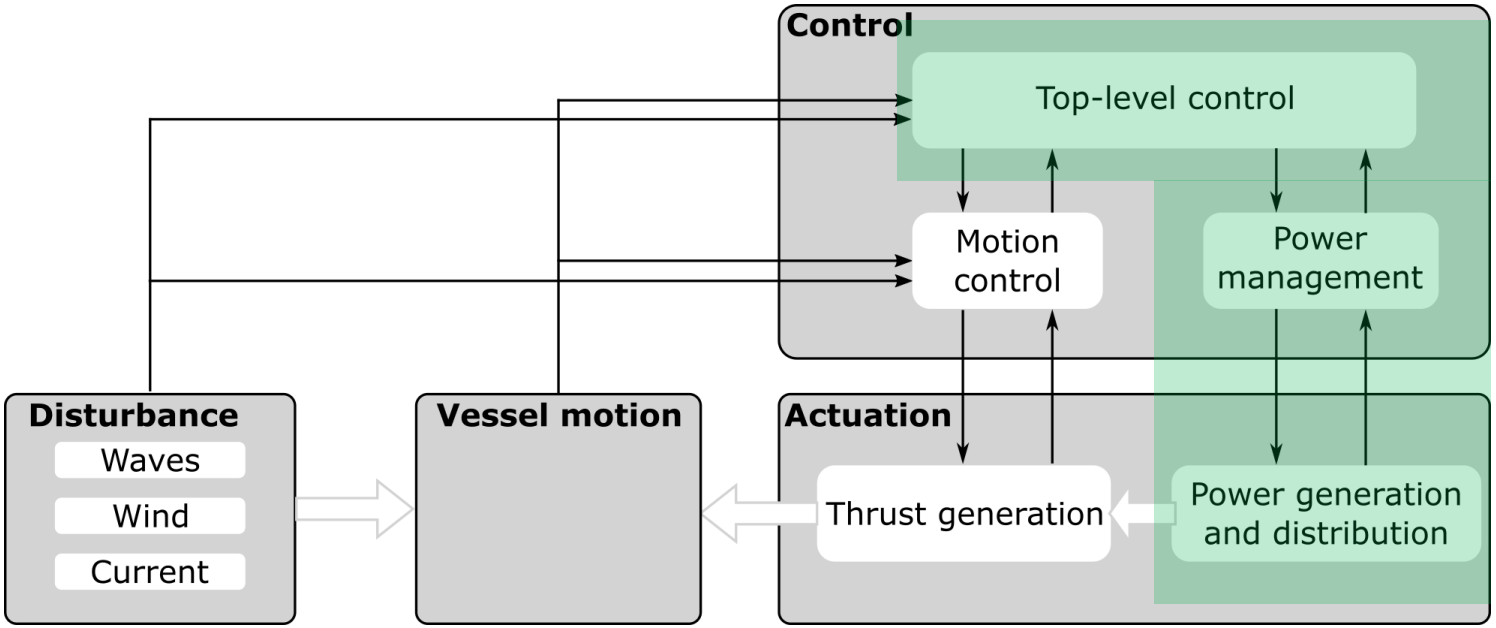
- Then, for each new vessel, derive system hazards from the high-level verification objectives, and use STPA to figure out how to avoid them
- This will produce a number of safety constraints and safety requirements to ensure that the system hazards are avoided.
- From these constraints and requirements, a vessel-specific verification/testing program can be developed

Why Use STPA

- It seems uniquely suitable for handling systems at an abstract and generic level
  - Safety constraints seems to come out at the same level of detail and abstraction as the level of detail of the information going into the analysis
  - Therefore enables us to find abstract safety constraints rather than specific rules
- A number of authors (including myself) reports more thorough hazard identification of complex software intensive and socio-technical systems, than traditional methods
- A study (Sørensen and Skjetne, 2004) found that *the interaction between hardware, software and human operators,* often cause DP accidents
  - STPA seems to be well suited for studying interactions between controllers at different levels and components

Case-Study: Finding Generic Verification Objectives for DP-systems

- Purpose: Find generic verification objectives for DP systems
- Limited to marine power systems control



The Research Council of Norway

DNV·GL

KONGSBERG

AMOS

System Accidents, Hazards and Safety Constraints for Generic System

System Accident	System Hazards	System Safety Constraints
A-1: Loss of life, damage to property or the environment, or loss of mission, due to unsuitable motion of the vessel	**H-1:** Thrusters are not controlled in a manner that satisfies the control objectives	**SC-1:** Thrusters must be controlled so that the resultant thruster forces induce vessel motion according to objectives
	H-2: Adequate amounts of power are not available for thrusters	**SC-2:** Adequate amounts of power must be made available for producing the required thrust force
	H-3: The motion control objectives are not in line with the operational function of the vessel	**SC-3:** Motion control objectives must be in line with the operational function of the vessel

Control Structure Information

- Top level control (TLC)
  - High level strategic control responsibilities such as
    - Select position and yaw set-points
    - Select and configure position reference systems
    - Configure power production and power distribution
      - Activate and deactivate power sources as needed
  - Relevant process model variables
    - Level of available power (the power that could be delivered if all active sources produced a maximum rating)
    - Adequacy of available power
    - Power consumption and load distribution
    - Behavioral state of power sources
    - Capacity of each power source
    - Standby power sources

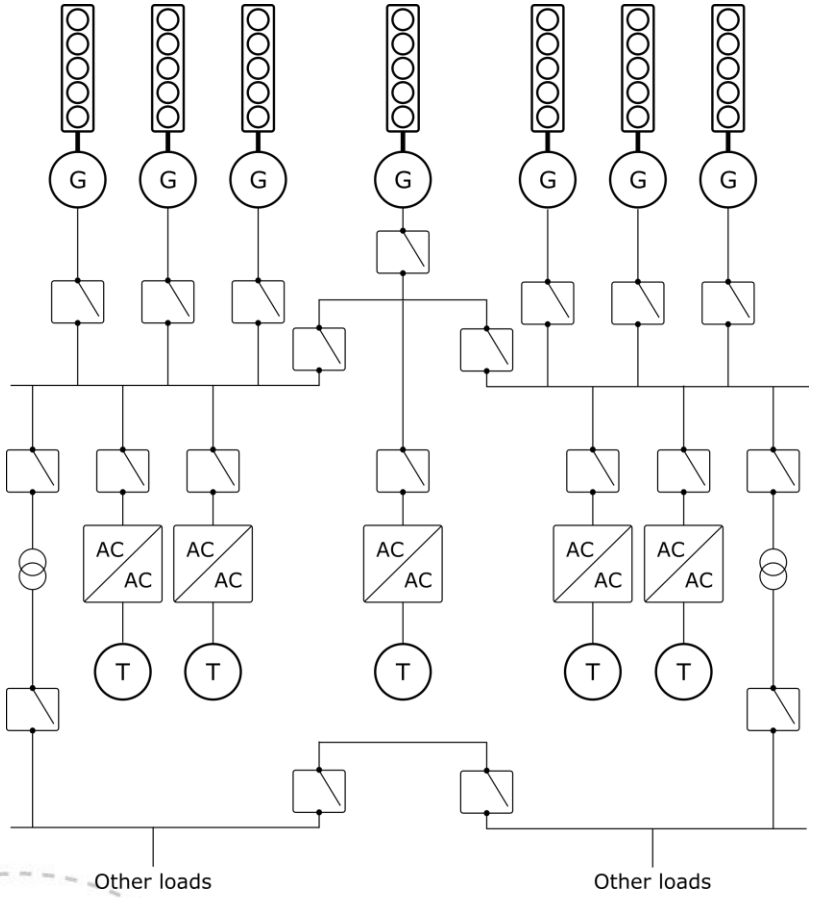
Example of UCA, scenarios and causal factors

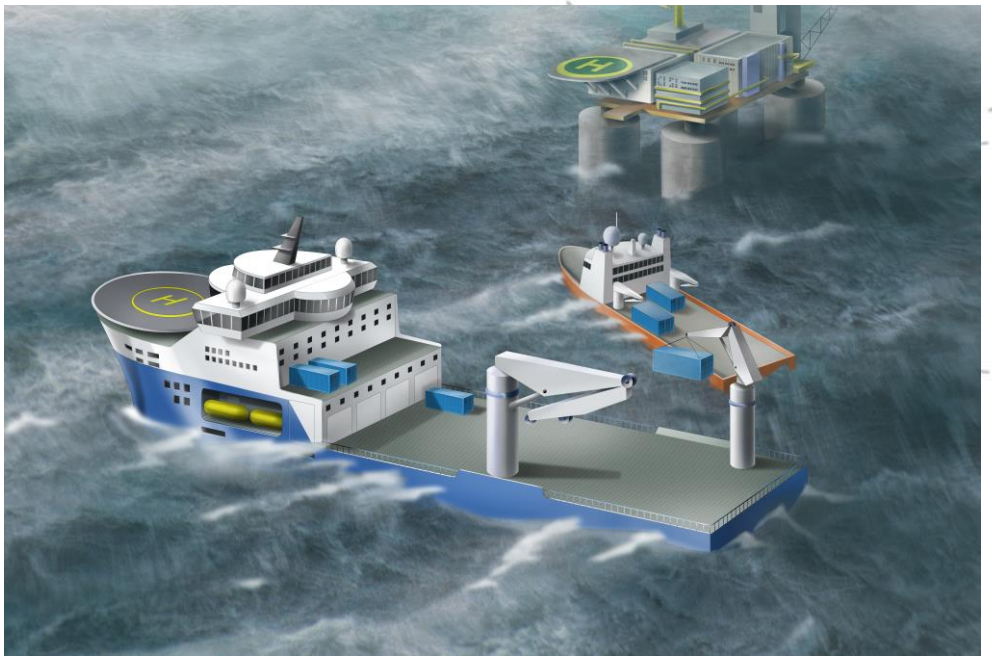
- **UCA-1:** Additional power source is not activated when available power is close to insufficient. *Rationale: If power consumption increase or capacity is reduced rapidly, there may not be enough time available to activate an additional power source.*
  - **S-1:** TLC does not realize that power available is too low
    a) Information about power consumption is missing, delayed or wrong
    b) TLC thinks power capacity is different from what it actually is because a power source is able to deliver less than rated power or because TLC have wrong information about rated power
    c) Production capacity is less than TLC believes because a power source that TLC believes to be active is actually inactive
    d) TLC does not pay attention to available power
  - **S-2:** Load increases so rapidly that it is not time to activate additional power source
    a) Sudden event, such as start-up of hydraulic pump, fault in thruster system (e.g., a thruster failing to full power)
  - **S-3:**Sudden or rapid reduction in power production/supply so that there is not enough time to activate additional power source
    a) Loss, inadvertent deactivation, or suddenly reduced performance of power source
    b) Power suddenly fails to be distributed, or distribution changes
  - **S-4:** TLC tries to activate power source but is not able
    a) There are no additional power sources available
    b) The control algorithm does not succeed in activation

Examples of Safety Constraints Formulated as Verification Objectives

- **VO-1:** Verify that additional power source will be activated before available power becomes too low (**UCA-1, S-1**)
- **VO-2:** Verify that heavy consumers will be interlocked when there is not sufficient amount of available power serve them (**UCA-1, S-2**)
- **VO-3:** Verify that heavy consumers are not able to increase loading at a more rapid rate than the power sources can handle (**UCA-1, S-2**)
- **VO-4:** Ensure that equipment, such as thrusters, that can fail to full power, can be physically separated from the electrical system (**UCA-1, S-2**)
- **VO-5:** Ensure that sudden, rapid, or unexpected reduction in power production cannot occur (**UCA-1, S-3**)

Case-Study: Vessel-Specific DP system Verification Program





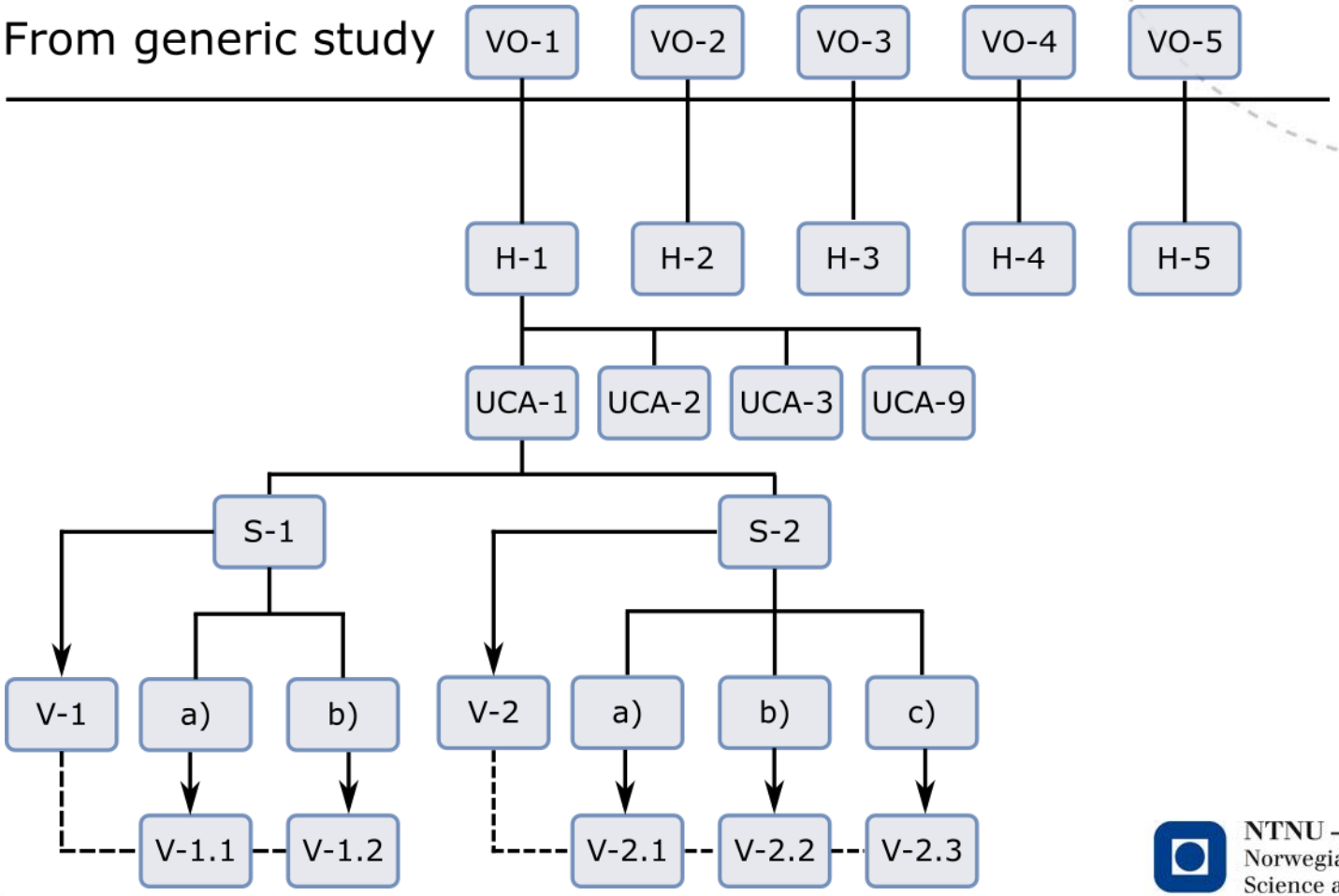
The Research Council of Norway

DNV·GL

KONGSBERG

AMOS

Case-Study: Vessel-Specific DP system Verification Program



NTNU – Trondheim
Norwegian University of Science and Technology

System Accidents, Hazards and Safety Constraints for Specific System

Using verification objectives from generic study to develop system hazards

ID	System hazard	System safety constraint
H-1	Additional power source is not activated, or does not contribute to reduce the available power when available power becomes TBD close to insufficient	Additional power source must be activated when available power becomes TBD close to insufficient
H-2	Heavy consumers are started when there are not sufficient amounts of power available	Heavy consumers must be interlocked when there is not sufficient amounts of available power to operate them
H-3	Heavy consumers increase consumption at a rate so rapid that the generators cannot keep pace	Heavy consumers must not be allowed to increase consumption at higher rate than TBD
H-4	Heavy consumers suddenly fail to full power and overload the power sources	Heavy consumers must be possible to physically separate from the electrical system
H-5	Sudden, rapid or unexpected reduction in power production occurs	Sudden, rapid reduction in power production cannot occur

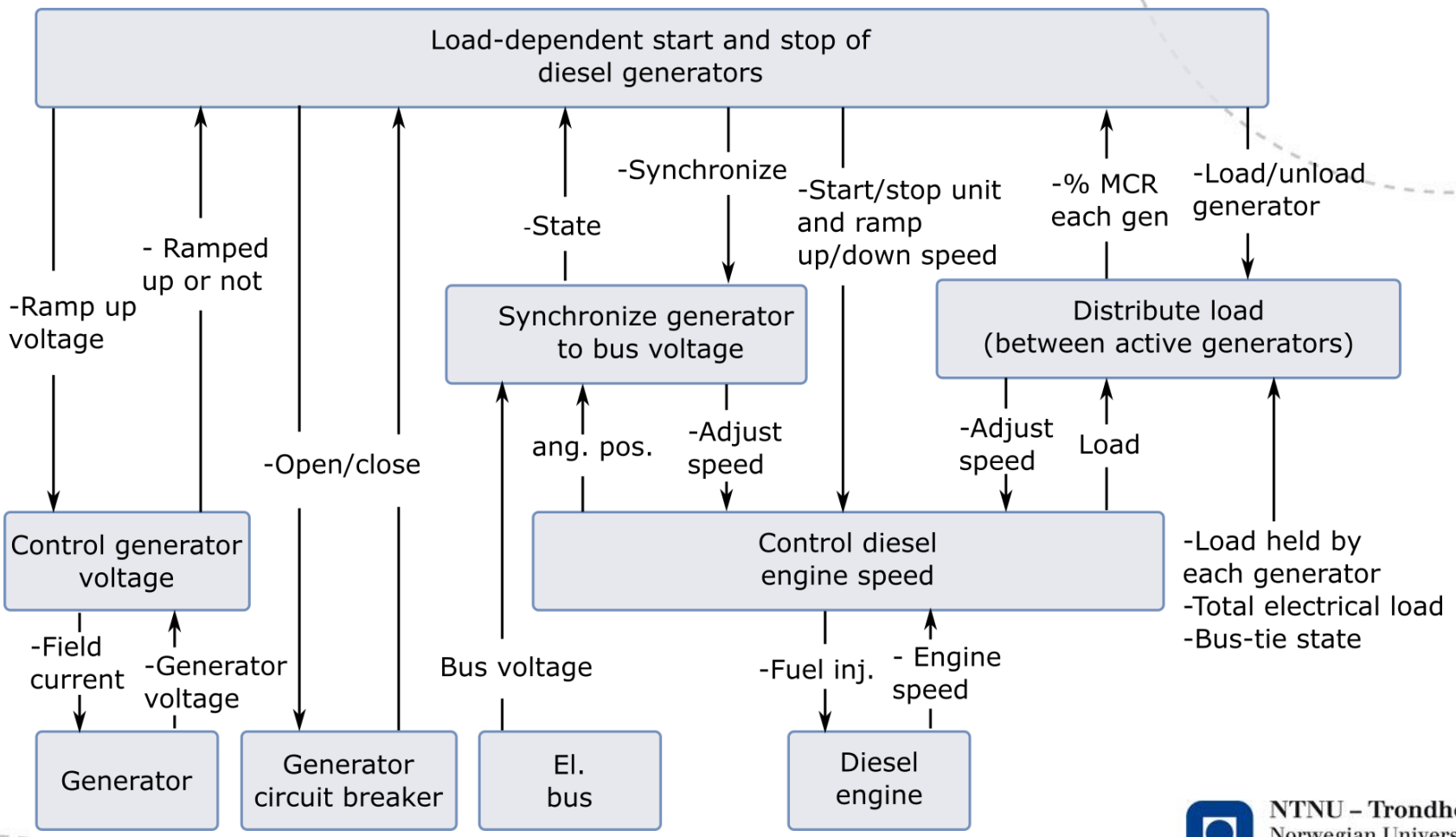
The Research Council of Norway

DNV·GL

KONGSBERG

AMOS

Establishing System Control Structure



NTNU – Trondheim
Norwegian University of Science and Technology

Establishing System Control Structure

Examples of control actions (LDSS)

- Load/unload generator
- Synchronize voltage
- Start/stop diesel engine
- Stop diesel engine
- Open/close generator circuit breaker

Examples of process model variables

- Which generator to activate next
- Which generator to deactivate next
- Power consumption
- Available power
- Level of loading on each active generator

Responsibilities

- Evaluate need for activating standby generator set
  - Evaluate power reserves
- Decide which standby generator set to activate
  - Consult startup sequence
  - Identify standby generator sets
- Activate standby generator set
  - Connect generator to bus
  - Start diesel engine
  - Load generator
  - Synchronize generator to bus

Examples of UCAs

Control Action	Mode	Unsafe control action
Load generator	Not provided	**UCA-1:** Load generator command for a generator that has been connected is not provided or not followed. *Rationale: If the connected generator do not take up a share of the electrical load, the situation is not improved by connecting it. (**H-1**)*
	Provided too early	**UCA-2:** Load generator command issued before the generator has been connected to the bus. *Rationale: Will disturb synchronization process, and generator will not be possible to connect to bus. (**H-1**)*
	Provided too late	**UCA-3:** Load generator command for a generator that has been connected is provided too late when the available power is insufficient or close to insufficient and load is increasing. *Rationale: Available power will remain too low while new generator does not receive load. (**H-1**)*
Remove load from generator	Not provided	**UCA-4:** Unload generator command is not provided for a generator holding load, before it is disconnected from the bus. *Rationale: This will result in a sudden load step for the remaining generators, something which might result in under-frequency and blackout.* (**H-4**)
		UCA-5: A generator is not (partially) unloaded when the generator is overloaded. (**Does not fit with any of the hazards. Means that generic study was incomplete?**)
	Provided	**UCA-6:** Unload generator commanded when this will result in over-load for the remaining generators. (**Does not relate to hazards.**)
Synchronize generator voltage to bus	Not provided	**UCA-7:** Synchronize command is not provided before generator is connected to the bus. *Rationale: Large disturbances on the bus will occur, and may cause blackout* (**Does not relate to hazards**)
		UCA-9: Synchronization not successfully executed when the available power is too low. *Rationale: Will not be able to connect the new generator and increase the available power. (**H-1**)*
	Provided	**UCA-10:** Synchronize commanded for a generator that is connected to the bus. *Rationale: This may result in speed adjustment commands that will alter the load distribution. (**Does relate to hazards**)*

Examples of scenarios for UCA-1

UCA-1: Load generator command for a generator that has been connected is not provided or not followed		
Scenario	**Description**	**Possible reasons**
S-1	Load generator command not issued	a) Command not issued because circuit breaker appears as open when it is closed b) Command not issued because circuit breaker is actually open/do not close on command
S-2	Load generator command not followed	a) Command is issued, but the load distribution controller does not receive the command b) Load distribution is unable to follow command because diesel engine controller does not respond to adjustments c) Load distribution does not follow command because the circuit breaker appears to be open

Possible Safety Constraints for UCA-1

- Load generator command must be issued once a generator has been connected to the bus
  - Command should be followed even if a faulty signal from the circuit breaker state that the circuit breaker is not closed when it actually has been closed
  - Circuit breaker must close when so commanded from the "load dependent start/stop of generators"-function.
- Load generator command must be followed
  - Commands issued from "load dependent start/stop of generators"-functions to load distribution, must be transmitted correctly
  - Diesel engine controller must respond to load distribution speed adjustments (if they are not unsafe(!))
  - Command should be followed even if a faulty signal from the circuit breaker state that the circuit breaker is not closed when it actually has been closed

Some verification activities that will help satisfy VO-1

Verify that:

- Load is transferred to a generator once it has been connected to the bus
  - Load dependent start/stop issues command to transfer load to a generator once it has been connected to the bus (**UCA-1, S-1**)
    - Command to load generator is followed even if a faulty signal from the circuit breaker state that the circuit breaker is not closed when it actually has been closed
    - Circuit breaker closes when commanded to do so from the "load dependent start/stop of generators"-function.
  - Load generator command is followed by load distribution (**UCA-1, S-2**)
    - Commands issued from "load dependent start/stop of generators"-functions to load distribution, are transmitted correctly
    - Diesel engine controller respond to load distribution speed adjustments
    - Command to load generator are followed by load distribution even if a faulty signal from the circuit breaker state that the circuit breaker is not closed when it actually has been closed

Conclusions

- STPA applied to DP:
  - Seems feasible
  - Desktop FMEA may still have a role in verifying redundancy
  - STPA should in any case set the scope for the FMEA – what should the FMEA look for
- STPA for identifying a verification program:
  - Seems like a promising approach
  - Advantages over current state:
    - Facilitates technological advance
    - When something new appear, classification societies wait and see what can go wrong, and then use experience to update the rules.
      - Better to figure out what can go wrong in advance…
    - The system will be analyzed wrt. safety, not only reliability