


VERIFICATION OF DYNAMIC POSITIONING SYSTEMS

AMOS Days 2016
Børge Rokseth

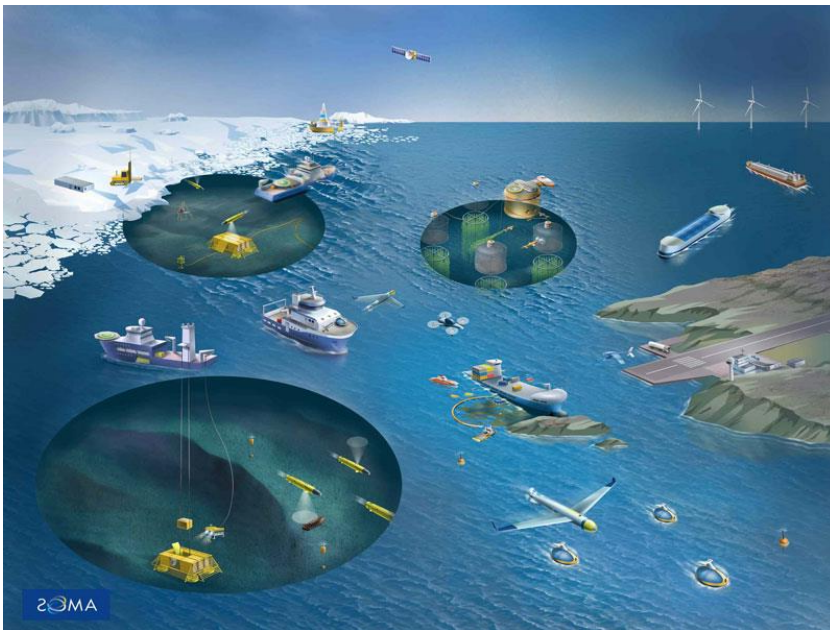
 **NTNU AMOS**
Centre for Autonomous Marine
Operations and Systems

Outline

1. Current state of verification of DP systems
2. Results from a study comparing traditional methods to Systems-theoretic process analysis (STPA)
3. Future work: Verification of these systems and the shift towards greener and smarter vessels

Safer, Smarter and Greener

- Expectations for the future:
 - Safer, greener and smarter maritime operations

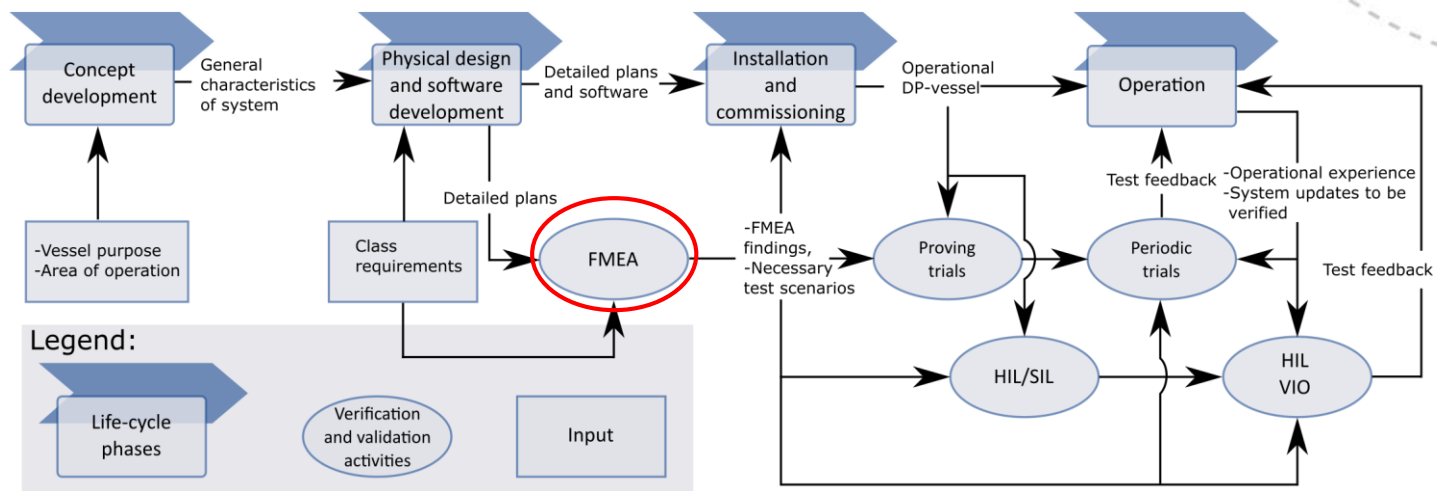


- Hybrid power systems
 - Energy storing units
 - Autonomous control and power management
- Autonomous maritime operations

Current state of verification and survey of DP systems

The Main Steps in the Verification Process

- DP FMEA:
 - Required by all classification companies.
 - Objectives/function:
 - Demonstrate system redundancy
 - Provide input for verification tests (Formulate assumptions and conclusions as test cases)
- Sea-trials:
 - Required by all classification companies
 - Objective/function:
 - Verify that system is functioning according to intention
 - Verify that a selection of component failures do not result in loss of position
 - Verify assumptions and conclusions from DP FMEA
- Hardware-in-the-loop:
 - Optional classes provided by DNV-GL and ABS
 - Objective/function:
 - Testing and verification of computer control systems
 - Can also verify assumptions and conclusions from DP FMEA



Challenges

- Increased use of integrated control systems (hence HIL).
- Drive towards low-cost solutions in the industry.
- The old verification methods are no longer sufficient (e.g. measure steel plate thickness).
- How will an increasing rate of technological progress affect safety?
 - Autonomy
 - Hybrid power systems
 - New applications (e.g. deep sea mining, operations in remote and challenging environments)
- Traditional measures such as redundancy may become less adequate.



Centre for Autonomous Marine
Operations and Systems

Results from a study comparing traditional methods to Systems-theoretic process analysis (STPA)

Verification Based on Systems-Thinking versus DP FMEA

- A case study, using STPA (Systems-theoretic process analysis) was conducted and compared to an industry standard DP FMEA
- The study demonstrates that:
 - STPA may be more suitable for identifying hazards and providing input for verification tests than DP FMEA. Using both STPA and DP FMEA is beneficial.
 - The current redundancy –and component failure focus is too narrow.
 - Key issue covered by STPA and not by DP FMEA: How unsafe/inadequate control can occur and cause hazards.

STPA

- Starting point: How can we identify potentials for inadequate control in a system?
 - Safety is an emergent property of a system. I.e., safety is not a property related to individual components, but the interactions between them.
 - Should be treated as a control problem, because accidents can be avoided by enforcing safety constraints on interactions.
 - 1. Identify accidents (losses), hazards and safety constraints.
 - 2. Establish the system hierarchical control structure.
 - 3. Identify potentials for unsafe control.
 - 4. Identify causal factors and create scenarios.
 - 5. Figure out how to avoid unsafe control/enforce adequate control.
- Treats human operators, organizations, computer control systems, etc. in the same manner – as controllers (in a general sense).

Verification based on systems-thinking versus DP FMEA

- Findings:

1. STPA can be applied without detailed design documents, whereas DP FMEA cannot
2. Loss of position can occur without any failures occurring. DP FMEA cannot consider these events.
3. The DP FMEA is better suited than STPA for systematically going through design documentation and verifying that the system is designed according to requirements.
4. DP FMEA is not suited for verification of safety if the term safety is interpreted in a broader than robustness against loss of position. The DP FMEA, unlike STPA, cannot analyze whether requirements are safe.
5. Both methods can identify single point failures that may result in accidents.
6. DP FMEA does not treat software. STPA treats software in terms of unsafe control.
7. DP FMEA does not treat operators. STPA does in the same manner as software.
8. Both methods are suited for providing input to verification tests (e.g., HIL testing and sea trials). Due to different scopes and areas of focus, some differences in test cases are expected.

Future work: Verification of these systems
and the shift towards greener and smarter
vessels

Safer, Smarter and Greener Systems, and DP Regulations

- How to maintain or increase safety while increasing level of smart and green?
- How to make sure that regulations support, rather than resist, technological progress.
- A new approach based on Systems-theory is required?

Proposed Approach

1. Generic study (Class responsibility)

- 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

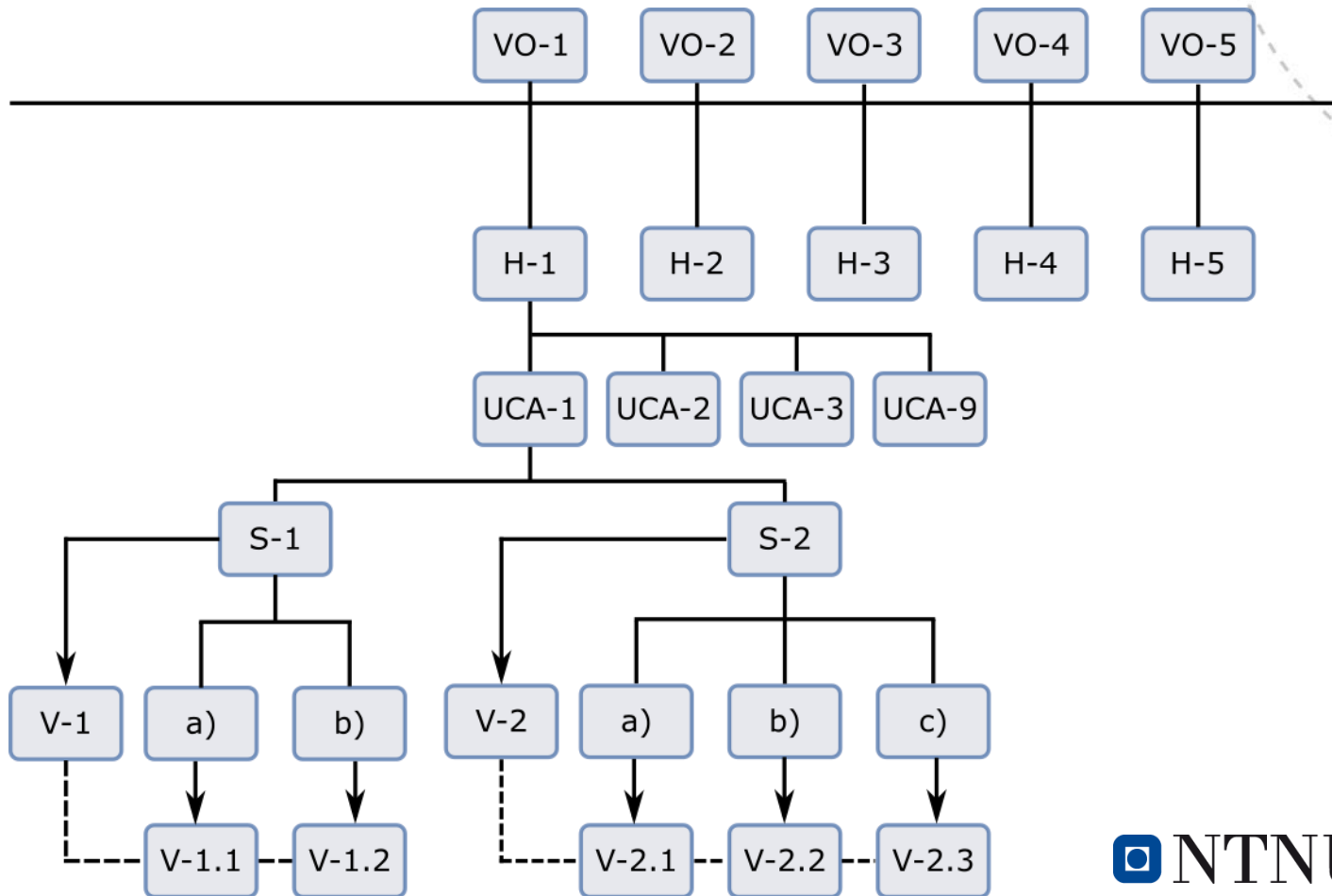
Question: Can it be made generic enough to not be an obstacle to innovation, yet ensure reasonable safe vessels and operations?

2. Vessel-specific study (Responsibility of developers)

- Derive system hazards from high level verification objectives
- Use STPA to figure out how to avoid them
- This results in a number of constraints and requirements necessary for the high-level verification objectives to be satisfied.

Safer, Smarter and Greener Systems, and DP Regulations

- **Examples of possible high-level generic verification objectives (note that no assumptions regarding level of autonomy are made):**
 - **VO-1:** Verify that additional power source will be activated before available power becomes too low
 - **VO-2:** Verify that heavy consumers will be interlocked when there is not sufficient available power serve them
 - **VO-3:** Verify that heavy consumers are not able to increase loading at a higher rate than the power sources can handle
 - **VO-4:** Ensure that equipment, such as thrusters, that can fail to full power, can be physically separated from the electrical system
 - **VO-5:** Ensure that sudden, rapid, or unexpected reduction in power production cannot occur



Class-regulations

Vendors, academia or other developers