Return to Session Directory

DYNAMIC POSITIONING CONFERENCE
October 12-13, 2010

LUNCH SESSION

Experiences from five years of DP software testing

By Øyvind Smogeli

Marine Cybernetics, Trondheim, Norway

ABSTRACT

The DP system on a modern vessel is often a collection of hardware and software from different vendors. To achieve optimal safety and performance, all these hardware and software components must work as an integrated system. This includes the position reference systems and sensors, the DP computer system, the power plant including the power management system (PMS), the thruster remote control systems, and the local thruster control systems, as well as all the auxiliary systems needed for electric, mechanical, and hydraulic power, lubrication, cooling, ventilation, and fuel.

An increased focus on multi-purpose vessels and fuel economy has pushed vessel and system designers to come up with more complex power and propulsion setups. Innovative new switchboard designs, closed bus-tie operation, and hybrid electric/mechanical propulsion setups with multiple power modes intended for different operations and situations have lead to increasingly distributed software functions between different systems and vendors. This has amplified the importance of a thorough understanding of the integrated functionality of the DP system by all involved parties. Experience has shown that lack of such understanding quickly results in a vessel that is not operating within DP class rules due to e.g. misunderstandings regarding definition of worst case single failure, misinterpretation of status signals between DP, PMS and thruster system, or inconsistence in actual and expected power system behavior.

Analyzing the redundancy design intent of the vessel and defining the worst case single failure are some of the main tasks of the desktop FMEA study which is undertaken for all newbuilds. In this work, the understanding of the complete DP system with all its components and their interaction is of major importance. The desktop FMEA study is by nature limited to analysis of the physical layout of the vessel, i.e. the hardware part of the DP system. The FMEA analysis of the various software components, on which the overall vessel FMEA analysis relies, is usually undertaken by the software vendors themselves without third party testing and verification. Also in the FMEA proving trials focus is put on the hardware components and partly the IO layer of the computer systems. In order to properly assess the DP system software it has been necessary to introduce additional tools. Hardware-In-the-Loop (HIL) testing is a well proven test methodology from automotive, avionics, and space industries, and is now also gaining recognition in the marine and offshore industries. The main idea of HIL-testing is to use advanced simulators capable of simulating the dynamic response of the vessel with its power plant, thrusters, and other relevant equipment. The simulators interface to the target control systems and are capable of simulating a wide range of scenarios defined by operational modes, operational tasks, and single and multiple failure modes in order to verify correct functionality and performance during normal, abnormal and faulty conditions. This includes verification of interfaces and integrated functionality between the DP computer system, PMS, and thruster control systems. Software functions for specialized operations like offloading, pipe-laying, trenching, etc. are even more difficult to test with traditional tools, especially when considering failure handling and off-design situations; testing such functionality in real life may be both dangerous and costly.

This paper summarizes experiences from HIL testing of DP system software on more than 50 DP drilling, supply, anchor handling, and construction vessels, including some interesting examples and a comprehensive analysis of finding statistics. The analysis shows how errors and weaknesses in core software and system configuration are distributed on the different functions in the DP system, as well as the potential consequence these errors could have had if they had not been identified and solved through early testing. The presented experiences demonstrate that independent testing of control systems using HIL testing technology is an important and effective service to ensure safe and reliable operation of offshore vessels.

1. HIL TESTING OF DP SYSTEM SOFTWARE

HIL testing is accomplished by connecting the control system which is the target for testing to a real-time simulator representing the vessel, vessel systems and environment, see Figure 1 as well as [1] and [2] for more details. The control system will not experience any difference between the real world and the simulated world. Functionality, performance and ability to handle failure

situations can then be tested under realistically simulated operating conditions, and weaknesses and errors in core software and configuration can be identified. Presently one classification society (DNV) has developed a voluntary class notation [3, 4] for DP-HIL testing and a Standard for Certification of HIL testing [5] that describes generic requirements to HIL testing.

1.1. The DP system

A DP system is comprised of a DP control system, a power system, and a propulsion system including thrusters [6]. The DP control system is further comprised of the DP computer system and the position reference systems and sensors. The HIL test setups are typically structured similarly:

- **DP-HIL** focuses on the DP control system, and mainly on the DP computer system.
- **PMS-HIL** focuses on the Power Management System.
- **SPT-HIL** (Steering, Propulsion, and Thruster HIL) focuses on the propulsion and thruster computer control systems, including remote and local thruster control.
- **Integration testing** of the DP, PMS and SPT control systems focuses on physical and functional integration of the different control systems.

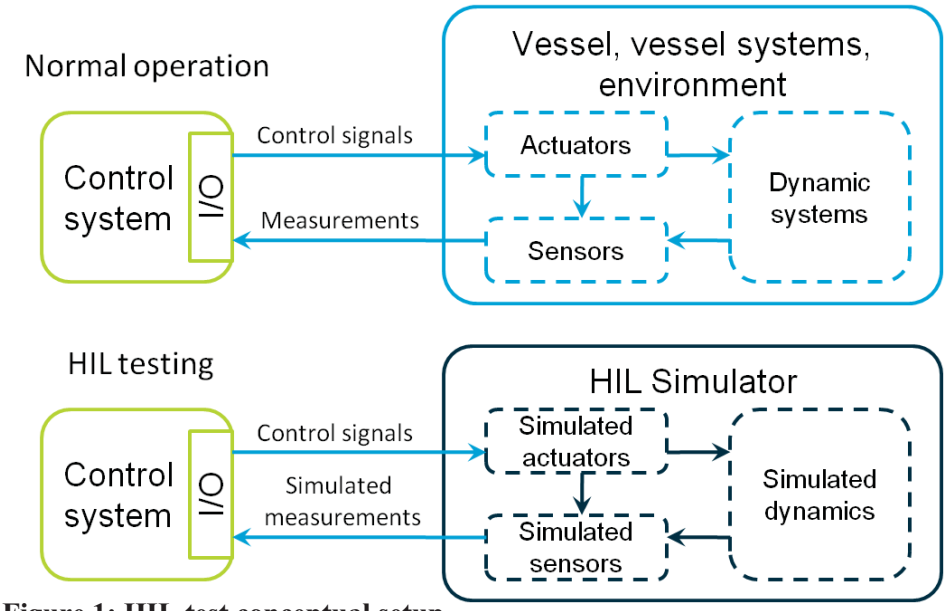

Figure 1: HIL test conceptual setup

1.2. Test cope

The overall test scope for a specific vessel is tailored to its specific target control systems, and the HIL test programs are based on the following acceptance criteria:

- Rules and regulations: class rules, flag state rules, IMO regulations, etc.
- Specification and functional design documentation of the target system.
- The vessel's operational philosophy.
- User documentation.

For testing and approval, the main Class concern is control system handling of single failures. However, other concerns like operational availability and performance may be equally important to the vessel owner. In addition, experience has shown that unexpected multiple failures, often combined with some level of human error, may have adverse consequences. A HIL test program therefore consists of several types of tests:

- **Functional testing**: Verification of control system functions and modes.
- **Failure mode testing**: Testing of control system failure detection and handling.
- **Performance testing**: Testing of control system performance under different operational and environmental conditions. Performance testing requires high fidelity models and is subject to careful analysis of model accuracy and sensitivity.
- **Integration testing**: Testing of integration between at least two control systems.

1.3. Test Activities

A typical HIL project is comprised of the following test activities:

Software testing is performed at an early stage using actual system HW or similar replica HW. The objective is to ensure that the control system SW is ready and verified as extensively as possible before start of commissioning and trials. Most findings from this test should be closed during a re-test using the control system HW (or similar replica HW). Software testing may also include some integration testing.

Integration testing can be performed in conjunction with software testing when it is beneficial to set up several systems at the same test site. The objective is to verify the integrated functionality and interface between different systems, often involving different vendors. Integration testing may also be performed in conjunction with onboard testing. In addition, a first and important level of functional integration testing is covered by coordination between simulators and test programs for the different target systems.

Onboard testing is carried out during the commissioning and sea trials period, and is used to close findings, and verify and validate the control systems. Onboard testing may include a second stage of integration testing where also the physical interface between the installed systems is included in the test scope.

Periodical testing secures the control system software during the vessel's life cycle. The periodical testing is executed as a software test on replica HW or onboard test when needed, or at intervals like annual DP trials. This testing shall ensure that SW or HW updates/upgrades, or changes in operational condition during the life-cycle, do not introduce new weaknesses or errors in the DP system.

2. FINDING STATISTICS

By July 2010, 60 DP-HIL and 23-PMS-HIL projects have been fully or partly completed, resulting in a total of 426 A-findings and 1166 B-findings. The projects cover a variety of vessel types and vendors. A thorough analysis of the findings has been undertaken, and will be presented in the following. Some of this material has also been presented in [7] and [8].

There is currently not sufficient statistical material for presenting results from SPT-HIL testing. In addition to a pilot project in cooperation with ABB in 2008 [9], the first commercial SPT-HIL projects are currently being conducted.

Table 1 defines the severity grades used in categorization of the findings. In addition a number of *observations* are usually reported in a given project. Observations are test results that are not considered findings, but still may be useful for the vessel owner and/or the target system vendor.

Table 1: Severity grade definitions

Severity grade	Definition
A	Non-conformity with rules and regulations (IMO, flag state, coastal state, class rules, and similar)
B	Non-conformity with requirements (specifications, industry guidelines and standards, documentation such as functional design specifications and user manuals, or intended use)

2.1. Statistics material and definitions

To categorize and analyze the findings beyond the severity grades defined in

Table **1**, a set of potential consequences along with associated weighting factors and typical severity grades have been defined in Table 2. The potential consequence is defined as the worst case consequence if the target system failure associated with a finding should occur during operation. If it is reasonable that other barriers would detect and act upon the failure, e.g. by other protection mechanisms or human intervention, this has been accounted for. The weighting factors will be used in the analysis to weigh the findings according to their potential consequence, such that potentially more harmful findings are given more weight. It should be emphasized that the potential consequences are non-exclusive, but that a given finding is weighted with its most severe potential consequence. For example, any failure leading to drive-off or drift-off is also a deviation from rules and regulations, but not vice-versa.

Table 2: Definition of potential consequences and associated weighting factors

Potential consequence	Weighting factor	Typical severity grade	Consequence group for plots
Drive-off	10	A or B	Drive- / drift-off
Drift-off	5	A or B	
Other deviations from rules and regulations	2	A	Dev. rules & regulations
Operational unavailability	1	B	Operational unavailability
Degraded system performance	0.5	B	Less serious
Deviation from specification	0.2	B	

Both the DP computer system and the PMS are sophisticated computer control systems with a multitude of functionality. For the finding analysis, they have therefore been divided in a set of main functions, and the findings have been categorized by their associated functionality. The main functions in a DP computer system are defined in Table 3, while the main functions in a Power Management System are defined in Table 4. The DP computer system function definitions have been inspired by the DP system definitions in [10], but have been modified to fit with an analysis of the DP computer system only.

Table 3: DP computer system function definitions

Function	Definition
DP computer system hardware	Power supply to DP controllers, operator stations and panels, network communication equipment, IO units
HMI and alarms	HMI (GUI, displays, operator stations, operator panels), alarm and messaging functionality
Monitoring functions	Online consequence analysis, DP backup control monitoring, DP class monitoring, network monitoring, online capability analysis, online motion prediction, UPS status monitoring
Network, communication and synchronization	Communication and synchronization between OS, automatic controller change-over, automatic reboot, etc.
Position reference system functions	Handling of position reference systems
Power functions	Power load limitation (blackout prevention) and feedback from generators, circuit breakers, bus-tie breakers, prime mover, and clutch
Sensor functions	Handling of sensor feedback from gyros, MRU's, wind sensors, external force measurements, draught sensors, riser monitoring, etc.
Station keeping functions	DP modes, mode control and mode changes, mode setpoints and references, dynamic vessel model (Kalman filter), wind force feedforward, current/rest force estimate, external force compensation, dead reckoning

Thruster functions	Thrust allocation, thruster feedback and command, thruster load reduction feedback, thrust force and moment calculation
Other	Functionality not covered by the other definitions

Table 4: Power Management System function definitions

Function	Definition
Blackout prevention	Power reservation for thrusters and propulsion; start interlock of heavy consumers; load reduction and limitation functions
Blackout restoration	Automatic startup from black bus; blackout restoration
Fault detection and handling for power distribution	Commands and feedback to power breakers (bus-ties, generator incomers, feeders, and other circuit breakers); commands and feedback to variable speed drives (VSDs), heavy consumers; commands and feedback from switchboards, synchronization controller
Fault detection and handling for power generation	Start of standby generator on pre-warning, shutdown or fault; feedback from prime mover and speed governor (status signals, measurements, alarms); commands and feedback to generator and automatic voltage regulator
Frequency/Voltage monitoring and control	Bus frequency control; under- and over-frequency detection and handling, voltage control; under- and over-voltage detection and handling
Load sharing functions	Active power load sharing between gensets; asymmetric active power loading of prime movers; reactive power load sharing; active and reactive power unbalance detection and handling.
Mode control	Automatic control; semi-automatic control; manual control; emergency mode; harbor mode; transit mode; DP mode; max/min generators; 0/2/3/…-split mode
PMS functions in HMI and alarms	HMI (GUI, displays, operator stations, operator panels), alarm and messaging functionality
PMS HW, Network and communication	PMS controller redundancy functions; PMS computer system hardware functions (UPS, OS, controllers, power supply); network communication
Other	Functionality not covered by the other definitions

2.2. DP-HIL and PMS-HIL finding overview

Figure 2 shows how the DP-HIL and PMS-HIL findings are distributed on the different potential consequences in Table 2. A total of 15% of the findings could have lead to drive- or drift-off if the errors had gone unnoticed into operation, and an additional 18% are deviations from rules and regulations.

2.3. DP-HIL statistics

DP-HIL testing targets the DP computer system. Barriers in surrounding systems such as GPS receivers, HPR computers, PMS, and thruster control, come in addition to the tested barriers in the DP computer system. A final barrier to protect against failure is operator intervention. It is therefore important that the alarm and messaging functionality of the DP computer system and other bridge systems enable the operator in making the correct actions. In considering the potential consequence of a finding, it has been attempted to account for the probability of an arresting operator action given the presented warnings and alarms.

Figure 3 shows the DP-HIL findings categorized by DP computer system function according to Table 3, distributed on the 4 potential consequence groups from Table 2: “Drive- / drift-off”, “Deviation from rules and regulations”, “Operational unavailability”, and “Less serious. The horizontal axis shows the number of findings in each category. Figure 4 shows the same data, with the blue lines representing the total number of findings associated with each DP computer

system function (i.e. equal to the total length of the bars in Figure 3), whereas the red lines show the weighted consequence of the findings.

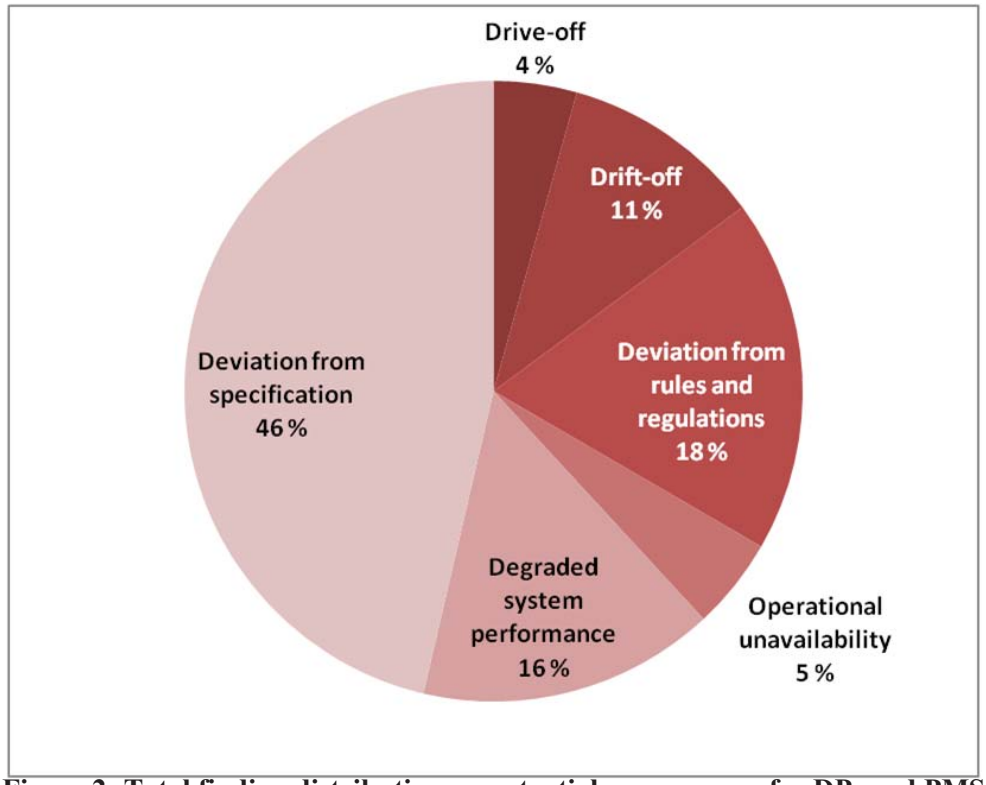

Figure 2: Total finding distribution on potential consequence for DP- and PMS-HIL

The weighted consequence is found by multiplying each finding with its associated weighting factor from Table 2, and summing up for all findings in each DP computer system function. The weighted consequence represents a better measure of the severity of the findings in each DP computer system function than only the number of findings. Figure 5 shows a simplified representation of the weighted consequence distribution of DP-HIL findings on different DP computer system functions. The statistics show that errors with potential severe consequences are found in all parts of the DP computer system, but also that some functions are more subject to severe findings than others. Based on the weighted consequence analysis, the most vulnerable part of the DP computer system appears to be the sensor functions, followed by thruster, HMI/alarms, monitoring, station keeping, and position reference system functions. It is also clear that a lot of less serious errors are found in the HMI and alarm system, these do however not contribute much to the weighted consequence.

2.4. PMS-HIL statistics

PMS-HIL testing targets mainly the high-level PMS, while functionality such as blackout prevention often is distributed also on other systems and components such as drives and protection relays. Often, there will be multiple barriers protecting against blackout with the PMS implementing only one or two of the barriers. For this reason, the consequences of failures in the high level PMS have been evaluated under a best case assumption, i.e. a conservative estimate with no other hidden error:

- All protection functions in the switchboard work as intended according to the design and operational philosophy of the vessel.
- There are no hidden errors in the protection relays, drives, governors, AVRs, or other relevant components.

- The consequences are evaluated depending on the actual number of online generators, breaker status, bus tie status, and the loads connected during the test.
- Operators respond correctly.

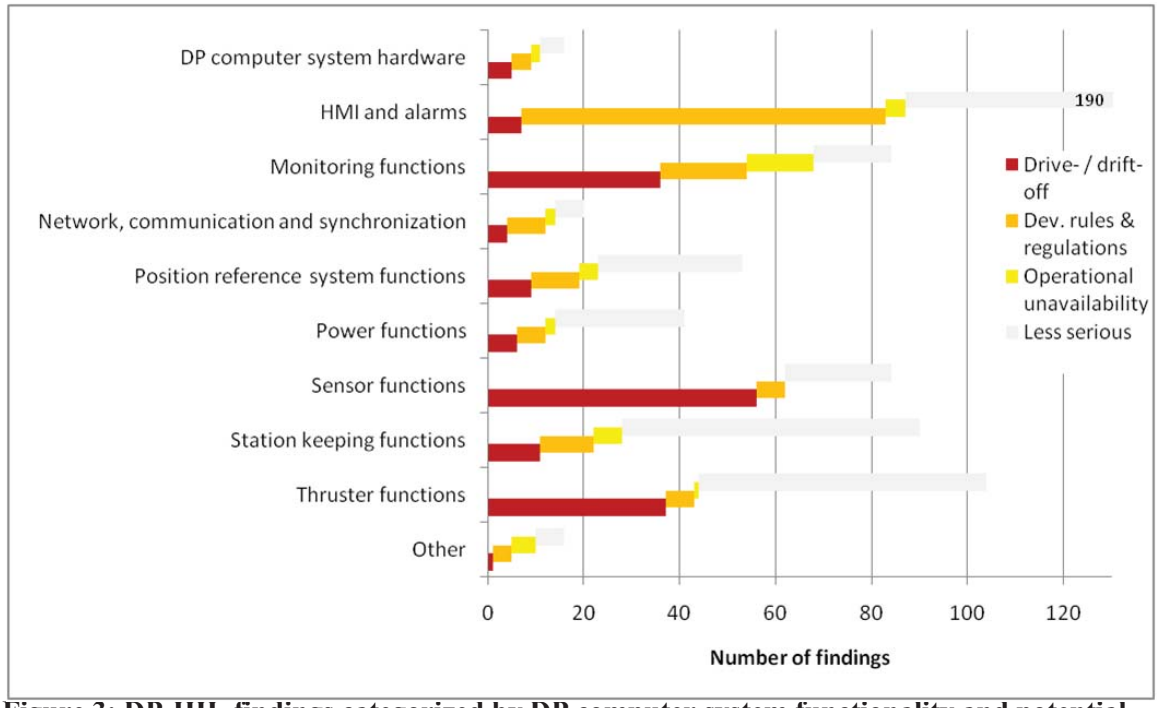

Figure 3: DP-HIL findings categorized by DP computer system functionality and potential consequence

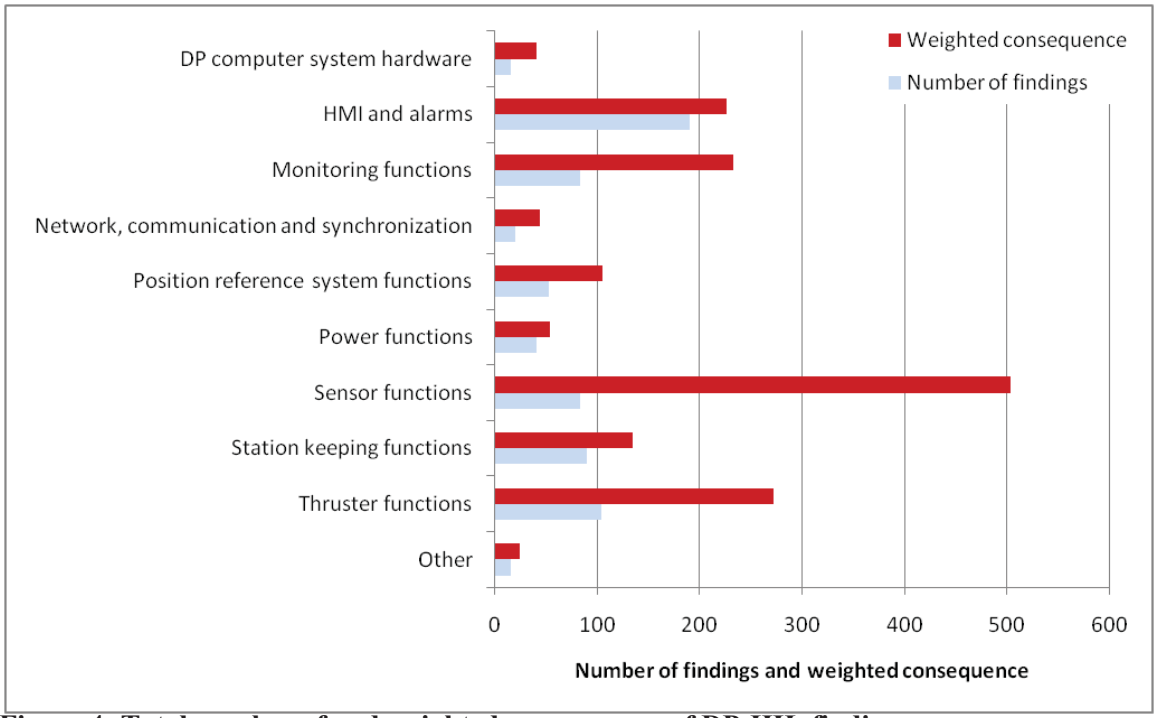

Figure 4: Total number of and weighted consequence of DP-HIL findings

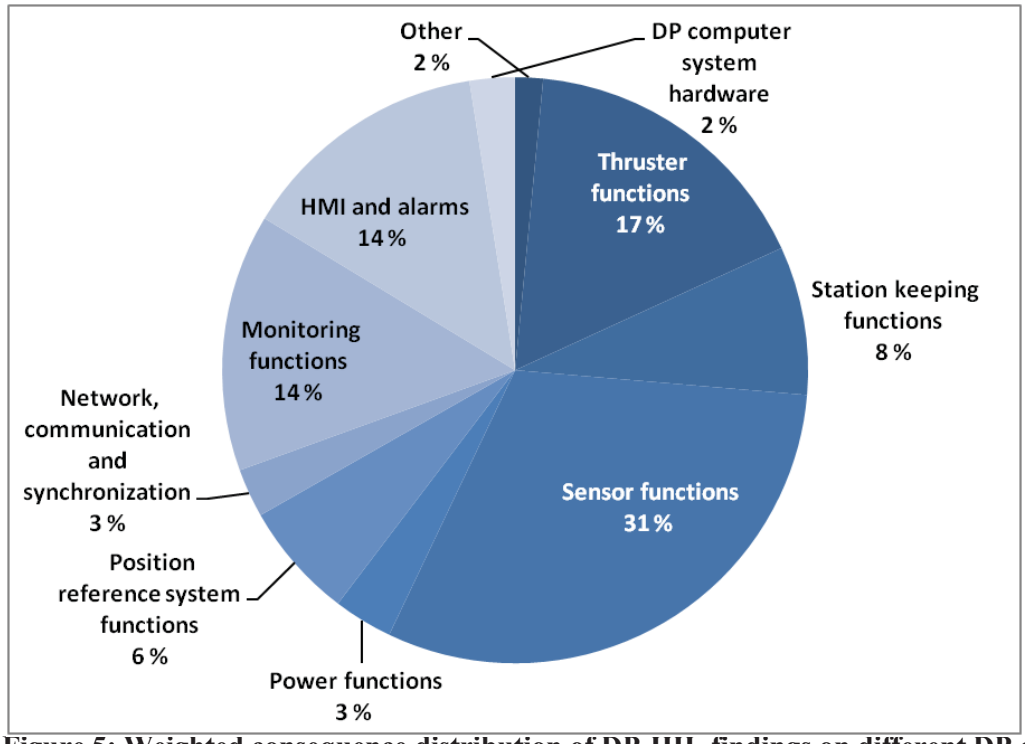

Figure 5: Weighted consequence distribution of DP-HIL findings on different DP computer system functions

The expected practical consequences are likely to be at least as severe as the analysis shows here, depending on the design, tuning and verification of the protection functions and others, as well as the competence of operators and technical staff.

Figure 6 shows the PMS-HIL findings categorized by PMS function according to Table 4, distributed on the 4 potential consequence groups from Table 2. The horizontal axis shows the number of findings in each category. Figure 7 shows the same data, with the blue lines representing the total number of findings associated with each PMS function (i.e. equal to the total length of the bars in Figure 6), whereas the red lines show the weighted consequence of the findings. The weighted consequence is found by multiplying each finding with its associated weighting factor from Table 2, and summing up for all findings in each PMS computer system function. Figure 8 shows a simplified representation of the weighted consequence distribution of PMS-HIL findings on different functions. Based on the weighted consequence analysis, the most vulnerable part of the PMS appears to be the load sharing functions, followed by fault detection and handling for power distribution and generation, and HMI/alarms. It is also clear that a lot of less serious errors are found in the HMI and alarm system, and also in the functions for fault detection and handling for power distribution and generation.

3. EXAMPLES OF FINDINGS

Experience has shown that a common understanding of the interface between systems and the integrated functionality of the DP system by all involved parties is of high importance. Some of the key problem areas of the integrated DP system appear to be understanding of the worst case single failure and associated implementation of the consequence analysis for all different power modes and system setups, common understanding of functionality and signals related to load limitation, blackout prevention and local load reduction, common understanding of reserved power functionality and signals, thrust allocation and implementation of forbidden/restricted zones including fix/zone release, and common understanding of pitch/rpm/azimuth response in different operational modes.

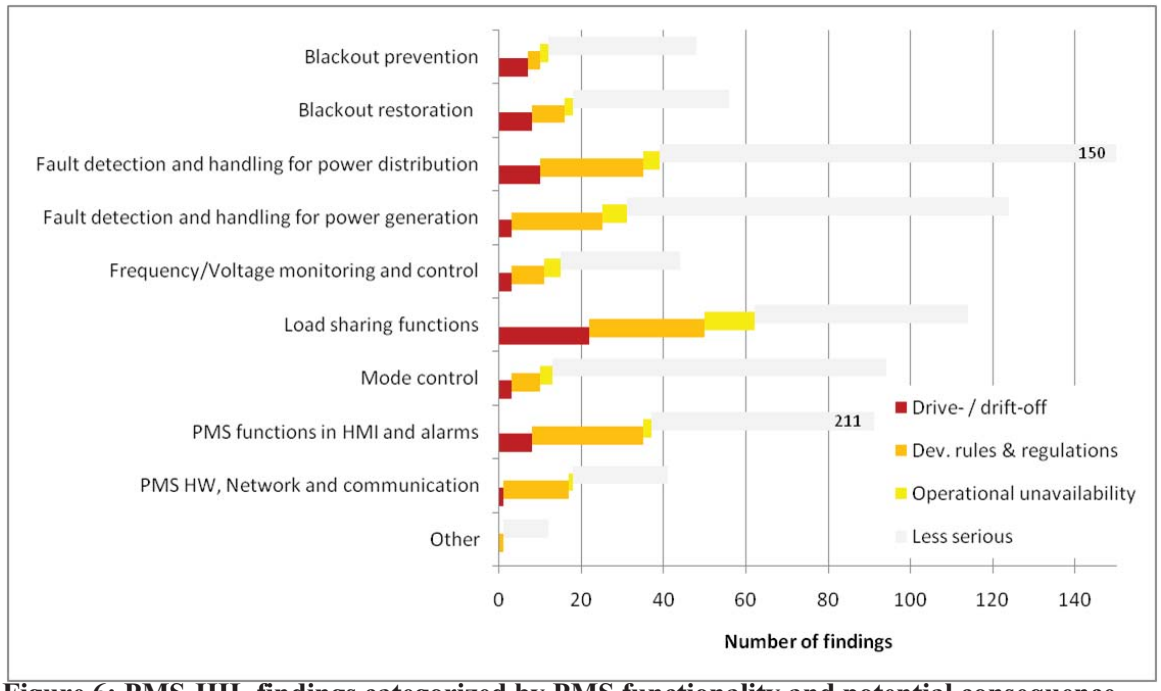

Figure 6: PMS-HIL findings categorized by PMS functionality and potential consequence

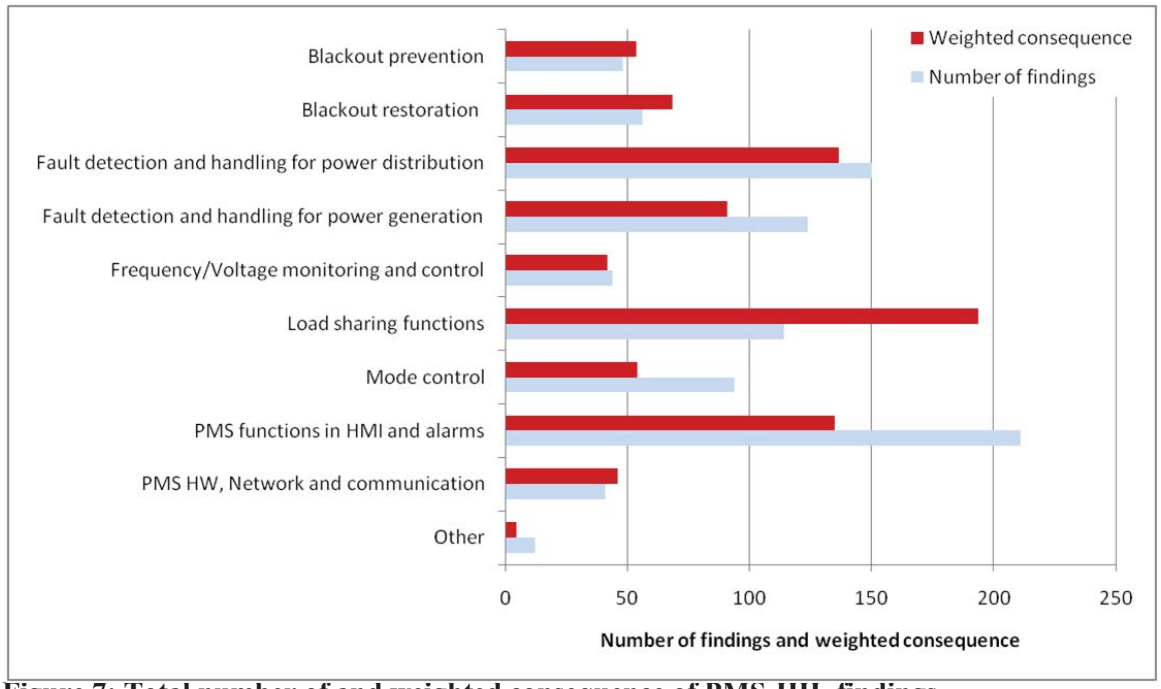

Figure 7: Total number of and weighted consequence of PMS-HIL findings

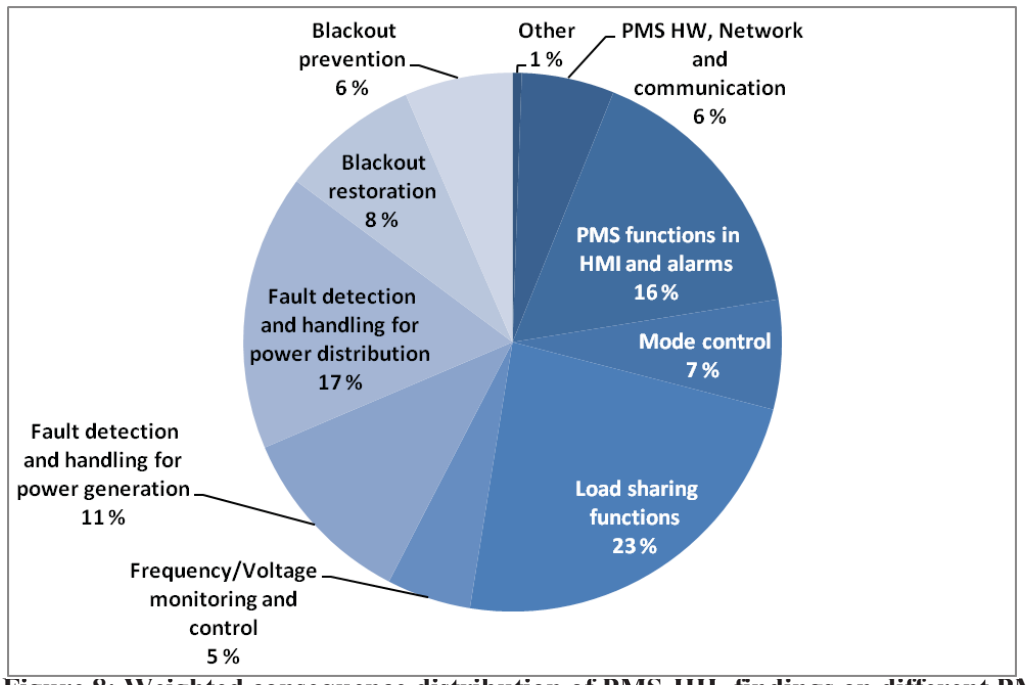

Figure 8: Weighted consequence distribution of PMS-HIL findings on different PMS functions

This section presents some interesting examples where HIL testing has enabled early detection and resolution of integration issues that probably would not have been discovered until either commissioning or during operation.

- The main propulsion system enforces restricted zones on both main azimuths, even if one is disabled or shut down. Consequence: the vessel has almost no sideways force in one direction after the failure of a single thruster, rendering the vessel useless for DP class 2 or 3 operation.
- The DP system fails to release the restricted zone of a main azimuth thruster if the other main azimuth is only deselected in DP. If the other thruster is stopped or taken into local control, the restricted zone is released. Consequence: Even if no consequence analysis alarm is given, the vessel cannot maintain position in DP if a main azimuth is deselected on the DP panel, meaning that the vessel cannot operate correctly in DP class 2.
- The DP system implementation of worst case single failure in the consequence analysis deviates with the actual worst case failure in the PMS. Consequence: no consequence analysis alarm issued when the vessel will lose position after worst case single failure.
- The pitch rise time of a main propeller is reduced when a fi-fi pump is running, but the DP is not notified. Consequence: DP system warnings are steadily issued because the thruster is not following its setpoint as quickly as expected.
- The DP system misinterprets the meaning of a thruster status signal informing that the thruster has been reduced by the PMS. Consequence: Reduced DP system performance and misleading DP system warnings.
- Fixed angle azimuth thrust allocation is not released after a failure, although the consequence analysis relies on this happening. Consequence: Loss of position after a single failure without any consequence analysis alarm.
- A power reserved signal from the PMS is not properly accounted for in the DP. Consequence: Possible partial blackout if one or more generators are in local mode.
- With all generators set in local mode, the DP reduced all the thrusters to zero. Consequence: Drift-off.

- The PMS and thruster/drive vendors do not have the same understanding of and scaling of power limitation signals. Consequence: Possible partial blackout if load reduction fails to limit power as the PMS expects.
- PMS load reduction is implemented in a way that is too slow to save the power plant from a blackout. Consequence: Drift-off.
- A 4-20mA signal for available power on the bus was used for load limitation of the thrusters. The PMS set 2mA as the available power whenever the power available calculation failed; this was interpreted as zero available power by the thruster control system. Consequence: Full load reduction to all thrusters every time an available power calculation failed.
- Added load on the bus was not accounted for by the DP load limitation. Consequence: The DP will command too much power and thereby force the PMS to start load shedding, with a following loss of position.
- The PMS misinterprets class rules regarding standby equipment and failure handling, leading to a design where the DP system is forced to activate consequence analysis alarms significantly earlier than the design was intended to offer. Consequence: Vessel is unable to meet original design criteria.

4. SUMMARY

This paper has shared some of the experiences from the past five years of DP system software testing, highlighting the benefits associated with earlier and more thorough testing. A comprehensive analysis of finding statistics from 60 DP-HIL and 23 PMS-HIL projects was presented. It was shown how errors and weaknesses in core software and system configuration are distributed on the different functions in the DP computer system and PMS, as well as the potential consequence these errors could have had if they had not been identified and solved through early testing.

Some interesting finding examples focusing on integration aspects of the computer control systems comprising the DP system were presented, illustrating the importance of a common understanding of the interface between the computer control systems and the integrated functionality of the DP system by all involved parties.

REFERENCES

[1] Tor A. Johansen, Thor I. Fossen, Bjørnar Vik. *Hardware-in-the-loop testing of DP systems*. DP Conference, Houston, 2005.

[2] Tor A. Johansen, Asgeir J. Sørensen, Ole J. Nordahl, Olve Mo, Thor I. Fossen. *Experiences from Hardware-in-the-loop (HIL) Testing of Dynamic Positioning and Power Management Systems*. OSV Singapore, 2007.

[3] DNV. *Rules for classification of Ships, Part 6 Ch 22 Enhanced System Verification (ESV)*, 2009.

[4] DNV. *Rules for classification of Ships, Part 7 Ch 1 Sec 7 I. Enhanced System Verification - SiO*, 2010.

[5] DNV. *Standard for Certification of HIL testing*. Draft, 2005.

[6] IMO. *Guidelines for Vessels with Dynamic Positioning Systems.* IMO Maritime Safety Committee Circ. 645, 1994

[7] Øyvind N. Smogeli. *Ensuring Safety, Reliability and Effectiveness – Testing DP Systems.* European DP Conference, London, 2009.

[8] Tor A. Johansen and Asgeir J. Sørensen. *Experiences with HIL Simulator Testing of Power Management Systems.* DP Conference, Houston, 2009.

[9] Jan Fredrik Hansen and Thomas N. Nielsen. *Fuel Efficient LNGC Propulsion Using Variable Speed Electric Propulsion Drives.* Propulsion and Emissions Conference 2009, Copenhagen, 2009.

[10] DNV. *Rules for classification of Ships, Part 6 Ch 7 Dynamic Positioning Systems,* 2008.