Looking Forward - Reliability of Safety Critical Control Systems on Offshore Drilling Vessels

Jon Espen Skogdalen[i]
Department of Industrial Economics, Risk Management and Planning
University of Stavanger, 4036 Stavanger, Norway
jon.e.skogdalen@uis.no
Phone/fax: +47 99 02 41 71

Øyvind Smogeli[ii]
Marine Cybernetics
Vestre Rosten 77, 7075 Tiller, Norway
oyvind.smogeli@marinecyb.com
Phone: +47 900 88 750

Abstract

The drilling industry is characterized by a rapid technology development to conquer larger ocean and drilling depths. The level of automation on offshore drilling vessels has been steadily increasing over several decades, growing from manually operated sledge-hammer technology to space-age computer-based integrated systems. These automation systems are essential for the safety, reliability, and performance of the vessels. Examples are the Dynamic Positioning (DP) computer systems, Power Management Systems, Thruster Control Systems, Drilling Control Systems, BOP Control Systems, Crane Control Systems, and Ballast Systems. While third party testing, verification, and classification of structures and mechanical systems are well-established in the maritime and offshore industries, the increasing use of computer control systems has not yet been met by corresponding third party testing and verification activities. This is a paradox considering that a single control system may be more complex than all the mechanical systems onboard; incident reporting from IMCA showed an average of 1.08 incidents per vessel in 2007, with computer caused incidents being the most prominent. It is also a paradox that the automation systems often contain safety-critical failure handling functionality that may be difficult or dangerous to test onboard the real vessel, and therefore is not properly tested until it is activated during an emergency situation. Hardware-In-the-Loop (HIL) testing is a well proven test methodology from automotive, avionics and space industries. The aim of this white paper is to clarify what HIL testing is, how third party HIL testing can be applied to control system software on drilling ships, semisubmersibles, jack-ups and FPSO's, and why this is an important contribution to technical safety for offshore operations.

Keywords: Technology Delivery System (TDS), Control systems, Hardware-In-the-Loop (HIL) testing, safety critical systems

[i] Jon Espen Skogdalen studied Health, Safety and Environment at Norwegian University of Science and Technology (NTNU). He received the Master's Degree in 2002 and has thereafter worked as a safety adviser in Safetec Nordic AS related to risk management for the offshore industry. Skogdalen is currently working on a PhD within risk analysis at the University of Stavanger.

[ii] Øyvind Smogeli studied Marine Technology at the Norwegian University of Science and Technology (NTNU), specializing in hydrodynamics and control systems. He received the Master's Degree in 2002 and the PhD Degree in 2006. In 2006 he joined Marine Cybernetics, where he has worked with development and conduction of HIL testing of DP control system SW. He currently holds the position as Chief Technology Officer.

Table of Contents

Acknowledgements

The authors are grateful to comments and reviews by members of the Deepwater Horizon Study Group. Special thanks to Dr. Michael Olson for inputs and review. Skogdalen also acknowledge the financial support from the Norwegian Research Council, Statoil and Fulbright.

1 Introduction

A fundamental premise in the DHSG work is to look forward to ensure that the oil and gas resources are developed in a reliable, responsible and accountable manner. These major steps forward will require implementation of an effective Technology Delivery System (TDS). An effective TDS endeavors to unify and address the needs and requirements of the concerned public, governmental agencies, industrial–commercial enterprise, and environmental communities so that vital resources and services can be delivered. The TDS must have desirable and acceptable Quality (serviceability, safety, compatibility, durability, resilience, sustainability) and Reliability (likelihoods and consequences of Quality) characteristics. This white paper addresses important aspects of the TDS related to safety critical systems, namely control system software.

1.1 Background

The drilling industry is characterized by a rapid technology development to conquer larger water and drilling depths. The mid-90s thrust into frontier depths precipitated the upgrade of a number of units and conversion of vessels from different uses, stretching existing hulls and associated technology for program objectives in as much as 10,000 feet of water. Compromised efficiencies and constraints on space, variable load, and handling weights motivated the design and construction of a new generation of rigs with extreme water depth capability. The 5th and 6th generation semisubmersibles and drill-ships, like the 5th generation ultra-deepwater semisubmersible Deepwater Horizon, are large displacement new-builds, outfitted with high pressure pumps, generous high-flow solids control suites, big bore drill pipe, dual mud systems with upwards of 15,000 bbl pit capacities, and automated pipe handling. Most are dynamically positioned, drawing on upwards of 58,000 hp power plants, boasting 1,000 ton hook loads, and either dual activity or significant off-line activity.[1]

The level of automation on these vessels is high, and the automation systems are essential for the safety, reliability, and performance of the vessels. Examples are the Dynamic Positioning (DP) control systems, Power Management Systems, Thruster Control Systems, Drilling Control Systems, BOP control systems, Crane Control Systems, and Ballast Systems. Examples of incidents and accidents that may be caused by failures in these systems are loss of position due to drive-off or drift-off, complete or partial black-out, failure of Emergency Disconnect (EDC), damage to the well, and possibly fire/explosion as a secondary effect of a failure.

Control system software is an essential and integrated part of all modern vessels. From small embedded control systems on panels and sensors to the vastly complex DP computer system, software constitutes an inherent part of a multitude of safety- and mission-critical automation systems. These automation systems are often collections of hardware and software from different vendors. To achieve optimal safety and performance, all the hardware and software components must work as an integrated system. For the complete DP 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.

It should also be noted that, as opposed to for example modern cars and airplanes, which are produced in identical numbers of thousands, almost every vessel is unique when it comes to

equipment and configuration. In a new-building project it is the yard that assumes the role of system integrator, attempting to harmonize and coordinate deliveries from multiple control system vendors. The yard's main competence and focus, however, usually is on mechanical completion. The result is that, although all physical equipment is in installed and running and all wiring is correctly finalized, the integrated software functionality may not have received much attention until the final sea trial phase of the delivery. At this stage, there is usually no time to carry out software testing beyond testing of the main control system functionality. Most of this testing is usually done by the control system vendors themselves, without focus on the integrated functionality.

While third party testing, verification, and classification of structures and mechanical systems are well-established in the maritime and offshore industries, the increasing use of computer control systems has not yet been met by corresponding third party testing and verification activities. The result is that a large portion of the automation systems on today's vessels are put into operation without independent testing. This is a paradox considering that a single control system may be more complex than all the mechanical systems onboard. It is also a paradox that the automation systems often contain safety-critical failure handling functionality that may be difficult or dangerous to test onboard the real vessel, and therefore is not properly tested until it is activated during an emergency situation.

Complexity has many facets, most of which are increasing in the systems we are building, particularly interactive complexity. We are designing systems with potential interactions among the components that cannot be thoroughly planned, understood, anticipated, or guarded against. The operation of some systems is so complex that it defies the understanding of all but a few experts, and sometimes even they have incomplete information about its potential behavior. Software is an important factor here: it has allowed us to implement more integrated, multi-loop control in systems containing large numbers of dynamically interacting components where tight coupling allows disruptions or dysfunctional interactions in one part of the system to have far-ranging "rippling" effects. The problem is that we are attempting to build systems that are beyond our ability to intellectually manage: increased interactive complexity and coupling make it difficult for the designers to consider all the potential system states or for operators to handle all normal and abnormal situations and disturbances safely and effectively.[2]

Hardware-In-the-Loop (HIL) testing is a well proven test methodology from automotive, avionics, and space industries. The aim of this white paper is to clarify what HIL testing is, how third party HIL testing can be applied to control system software on drilling ships, semisubmersibles, jack-ups and FPSO's, and why this is an important contribution to technical safety for offshore operations.

1.2 DP Equipment Class

DP vessels can be categorized by their DP Equipment Class, which indicates the level of redundancy in the vessel design. The classification societies have slight variations in their definitions of the different Equipment Classes; the following are the definitions by IMO and IMCA[3, 4]:

Equipment Class 1 Loss of position may occur in the event of a single fault.

Equipment Class 2 Loss of position should not occur from a single fault of an active component or system such as generators, thruster, switchboards, remote controlled valves etc., but may occur after failure of a static component such as cables, pipes,

manual valves etc.

Equipment Class 3 Loss of position should not occur from any single failure including a completely burnt fire sub division or flooded watertight compartment. A single fault includes a single inadvertent act by any person on board the DP Vessel.

A 5th or 6th generation drilling rig/ship will usually be required to have DP Equipment Class 3. According to the definition of DP Equipment Class 3, this means that no single failure including fire or flooding should cause loss of position.

2 Risk Analysis and Risk Management

Traditionally, risk management was based on a prescriptive regime, in which detailed requirements were set to the design and operation of the arrangements. This regime has gradually been replaced by a more goal oriented regime, putting emphasis on what to achieve rather than on the means of doing so. Risk management is an integral aspect of this goal oriented regime. It is acknowledged that risk cannot be eliminated but must be managed. Establishing an informative risk picture means identifying appropriate risk indices, and assessing uncertainties. Using the risk picture in a decision-making context means definition and application of risk acceptance criteria, cost-benefit analyses and the ALARP principle (risk should be reduced to a level which is As Low As Reasonably Practicable).[5]

Definition and modeling of safety barriers is central when analyzing the influence of technological, human and organizational factors on safety critical systems. The following definitions are extracted from Sklet[6]:

- Barrier function: A function planned to prevent, control, or mitigate undesired events or accidents.
- Barrier element: Part of barrier, but not sufficient alone in order to achieve the required overall function.
- Barrier influencing factor: Factor that influence the performance of barriers.

The Petroleum Safety Authority Norway (PSA) regulations require the following aspects of barrier performance to be addressed: Reliability/availability, Effectiveness/capacity, and Robustness. A wide discussion related to risk management of complex safety critical systems is not the scope of this paper, but the main principles (risk identification/analysis, uncertainties and barriers) are the framework for the presented material.

2.1 FMEA and HIL

Failure Mode and Effect Analysis (FMEA) is an important and well-established method for risk analysis related to safety critical systems including soft- and hardware.[7] FMEA is a single failure-oriented technique. Analyzing the redundancy design intent of the vessel and defining the worst case single failure are some of the main tasks of the desktop DP System FMEA study which is undertaken for all new-builds. 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 rig, i.e., the hardware part of the DP system. The DP System 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, which constitutes an important part of the sea trials for a new-build, focus is put on the hardware components and partly the I/O layer of the computer systems. The software functionality of the computer systems is only superficially tested, mainly due to a lack of appropriate testing tools.

While the DP System FMEA focuses on physical layout and hardware, HIL testing focuses on the software part of the control systems. With few overlaps, FMEA and HIL are complementary activities that both are needed and should be coordinated. The FMEA desktop study will reveal possible weak points in the physical design, and point to critical software functions that deserve increased attention. This provides important input to the HIL testing, which in turn will provide essential information on the functionality and failure handling capabilities of the control system software that may be included in the FMEA.

Historically however, independent HIL testing has not been available to be incorporated into the vessel commissioning process. The yard, which should have the role of system integrator, usually focuses on mechanical completion, and leaves software integration and testing to the vendors. In addition, there have been no specific class rules on independent testing and verification of software. The end result has been that verification of software functionality, failure handling capability and safety barriers has received very little attention in a vessel commissioning process.

2.2 Potential incidents/accident examples

Some of the potential consequences of failures in the DP control system are:

- Drive-off, where the vessel drives off position by use of its thrusters and propellers, typically due to an error in the position reference and sensor systems, or fail-to-full of a thruster or main propeller.
- Drift-off, where the vessel drifts off position/heading due to insufficient available thrust, typically due to some single failure combined with errors in specialized software functions like consequence analysis or thrust allocation.
- Unnecessary loss of DP class, causing an abortion of the ongoing drilling operation.

Some of the potential consequences of failures in the Power Management System are:

- Complete black-out, causing a drift-off and loss of power to all drilling operations.
- Partial black-out, causing abortion of ongoing drilling operations and loss of DP class.
- Failure on PMS blackout recovery after a complete or partial black-out leading to a sustained blackout and possible loss of the ability to perform an emergency disconnect (EDC) from the BOP.
- Loss of position due to incorrect load reduction of the thrusters and following lack of thrust capacity.

2.3 Incident statistics

The most prominent available incident statistics are provided by IMCA, who distributes an annual overview of incidents reported by their members, including an analysis of primary and

secondary causes. The latest report[8] is from 2007, where 67 reports from 49 vessels are categorized and analyzed. Of the reports, 53 were categorized as "incidents" and 14 as "undesired events." This gives an average of 1.08 incidents per vessel in 2007. Of the 53 incidents, 15 were reported by drilling vessels. This was only exceeded by diving support vessels, from which 16 incidents were reported. Computer related issues were reported as the largest main cause of the reported incidents, see Table 2.1. Although it can be anticipated that the reported incidents only represent a fragment of the total number of offshore incidents each year, the statistics emphasize the fact that computer caused incidents do happen, and that they happen at a high frequency compared to other causes.

The incidents reported[8] are analyzed in "incident trees," which describe the serial course of events that lead up to the incident in question. As an example, one reported incident was caused by a DP computer system software error that had been lying hidden for 8 years of operation. Ultimately, an unfortunate combination of events and button-presses by the DP operator triggered the bug, which in turn caused a drive-off on a diving support vessel.

In year 2000 the Petroleum Safety Authority of Norway launched the project "Trends in Risk Levels." The aim of the work was to measure the impact of HES-related measures in the petroleum industry and thereby help to identify areas which are critical to HES, and in which priority must be given to identifying causes in order to prevent unplanned events and accidents. This project also includes improving industry understanding of the possible causes of accidents and their relative significance in the context of risk. The goal is to create a reliable decision-making platform for both the industry and the authorities in planning preventive safety and emergency preparedness measures.[9] The project collects the average annual numbers of tests and failures related to major hazard barrier elements such as fire detection, gas detection, Wing/Master valves, BOP, Deluge valve and Fire pump starts. There is, however, no collection of data related to software failures in safety critical systems. The number of total black-outs where emergency power is not functioning as intended is captured, but these incidents are recorded as situations of hazard and as accidents with no major accident potential. It is the authors' view that these incidents should be taken more seriously, and that these incidents are indicators of serious malfunctions in safety critical systems.

Table 2.1 – Causes of incidents reported to IMCA in 2007.[iii]

Cause of incident	Main cause	Secondary cause
Computer	15	4
Electrical	2	3
Environment	3	1
Human error	7	6
Power generation	10	4
Reference	10	0
Thruster	5	0
Procedures	0	7
Other	1	3
TOTAL	53	27

[iii] IMCA. M 198 Dynamic Positioning Station Keeping Incidents Reported for 2007 (DPSI 18). International Marine Contractors Association; 2009.

Malfunctioning software may be totally hidden for the user until it fails, but in many cases the users do get precursor incidents (e.g., "blue screens of death" and irresponsive systems). These precursor incidents may last just for a short time (1-3 seconds), or require a "reboot" of the system. It is the authors' experience and view that many of these precursor incidents do not get reported due to the fact that the systems work again afterwards, and that the user does not properly understand what happened. We use the word "precursor incident" intentionally, since these incidents may be warnings about serious failures in the software.

3 The Concept of HIL Testing

In a computer control system, SW capability is generally invisible as compared to HW. The HW, typically comprised of PLC's or computers, I/O cards, network, and operator panels, look the same with SW and without SW. HIL testing, which is an industry term for simulator based testing, is an efficient and effective tool to expose the full capability and robustness of the control system SW.

A control system interacts with its surroundings through a set of Input/Output (I/O) communication channels. Inputs are provided by sensors that measure dynamic states and parameters, as well as inputs from operator stations and other control systems. Based on the inputs and internal models in the control system, the control system calculates control signals that are sent to actuators via the I/O output channels, see Figure 3.1.

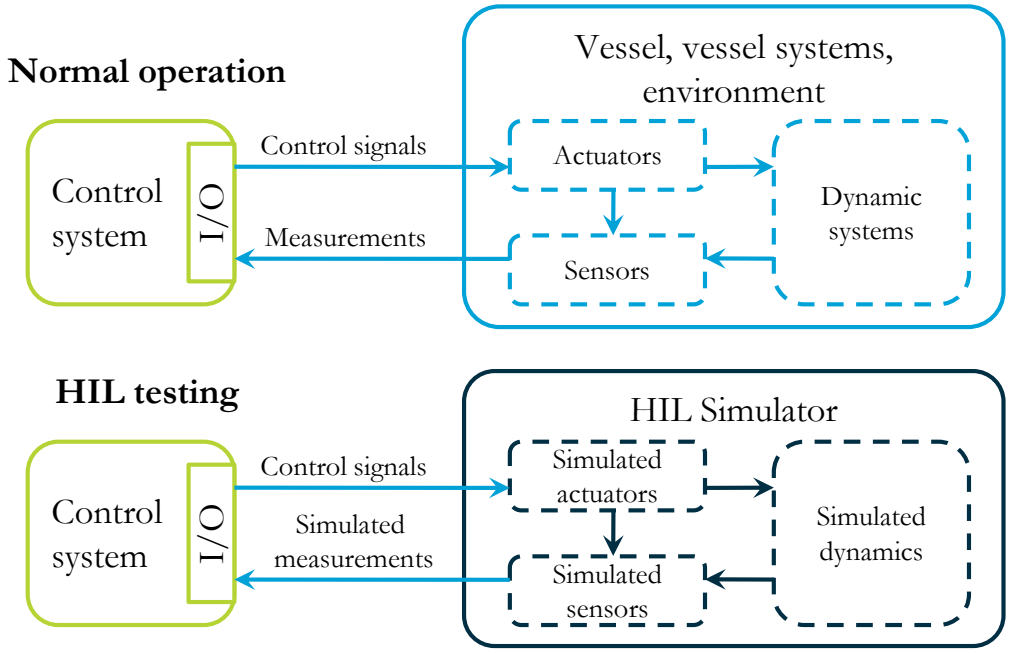

Figure 3.1 – HIL test conceptual setup.

HIL testing is accomplished by isolating the control system and its operator stations from its surroundings, and replacing all actual I/O with simulated I/O from a HIL simulator in real time. The HIL simulator imitates all the surroundings (i.e., dynamic systems, actuators, and sensors) of the control system, responds to control signals in a realistic manner, and provides realistic and consistent measurements. The control system cannot sense any difference between the real world and the virtual world in the HIL simulator. The HIL simulator thereby facilitates systematic testing

of control system design philosophy, functionality, performance, and failure handling capability, both in normal and off-design operating conditions.

In HIL testing the control system is viewed as a black box, i.e., no first-hand knowledge of the inner workings of the control system is necessary. However, a functional description of the control system is needed in order to establish a proper test scope. In addition, detailed knowledge of the control system I/O and its surroundings is necessary in order to develop a sufficiently accurate simulator.

Some of the advantages of HIL testing are:

- Facilitates early testing of the software.
- Facilitates thorough and extensive testing, since most of the testing can be done outside the critical timeline for vessel construction.
- Facilitates testing of failures and off-design situations that would be difficult, dangerous, or costly to test onboard the vessel
- Facilitates testing on similar replica hardware at a lab or at the vendor's site when the actual hardware onboard the vessel is not available.
- Facilitates integration testing of control systems from several vendors.
- Facilitates third party testing, since no detailed design knowledge about the control system software is needed for testing.
- Facilitates tests that could harm the equipment if tested onboard the vessel.

3.1 Example: HIL testing of a DP system

A DP system is comprised of several interconnected control systems, the most prominent being the DP computer system, the PMS, and the thruster control systems. A HIL test of a DP system would typically target all these systems, both individually and as an integrated whole.

For the HIL test of the DP computer system, the HIL simulator includes models of the environment (wind, current, waves), the vessel motion due to environmental loads and thruster action, the thrusters, the power system, all position reference systems (DPGS, HPR, taut wire, Artemis, relative reference systems, etc.), and all relevant sensors (gyrocompasses, MRU's, wind sensors, draught sensors, riser angle sensors, etc.). The HIL simulator also includes the physical interaction between all these components. For a semisubmersible with thruster assisted position mooring, the mooring line forces would also be modeled. During HIL testing the DP computer system commands the simulated thrusters and receives measurements from the simulated position reference systems, sensors and equipment, and does not notice any difference from being in actual operation onboard the vessel. Functionality, performance, and failure handling capability can then be tested systematically in a controlled environment.

For the HIL test of the PMS, the HIL simulator includes models of prime movers, generators, power distribution, thrusters, breakers and bus-ties, as well as load sharing and synchronizing functions. For testing of the thruster control systems, the HIL simulator includes models of propellers, motors, drives, pitch and azimuth hydraulics, as well as relevant auxiliary equipment.

During testing of the individual systems, also interfaces and shared functionality between the various systems, usually delivered by different vendors, can be systematically tested at the same time.

If practically feasible, a HIL test of the integrated DP system can also be performed, with all systems interconnected and running simultaneously.

Verification of the interface between the individual systems and their shared functionality is of high importance to gain a common 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. There are multiple key problem areas surrounding the integrated DP system, including but not limited to:

- 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.
- Common understanding of pitch/rpm/azimuth response in different operational modes.

3.2 HIL testing in other industries

It is widely recognized in other industries that safety critical control systems should be subject to thorough and systematic testing. In many of these industries, including automotive, avionics, aerospace, power electronics, robotics, and nuclear, HIL testing methodology has gained increasing importance in recent years.[10, 11, 12, 13, 14, 15, 16, 17, 18, 19]

In the automotive industry, comprehensive HIL testing of Electronic Control Units (ECUs) is "Best Practice" for both automobile manufacturers and their suppliers, and is considered essential to reach the necessary safety levels and avoid vehicle recall campaigns. ECU examples[20] include ESP, ABS, cruise control, automatic four-wheel drive, fuel injection, ignition, and turbocharger control. Note that there is a major difference between testing of a car and a ship in the fact that identical cars are produced in numbers of thousands, whereas even sister ships never are truly identical. This means that the control systems and setups are unique for each single vessel, and the potential for errors in design, functions and configuration are significantly larger.

In the space industry, NASA has utilized HIL testing extensively in their Independent Verification & Validation (IV&V) Facility[20] for testing of mission-critical software components on spacecraft. In the aerospace industry, HIL testing has been used, e.g., in programs such as Future Combat System and Joint Strike Fighter[19] and by Bell helicopters to design a civilian tilt-rotor aircraft.[21]

3.3 Why third party testing?

When high standards of safety are required, detailed guidelines for testing of software and automated systems are usually adopted.[22, 23] An important question that arises is whether or not testing should be conducted by an independent third party. In the maritime and offshore industries the class societies have a long and successful tradition as providers for third party testing and verification.[24, 25, 26, 27] Also, the FMEA companies have a third party role in delivering FMEA analyses and trials.[7]

Within the space industry, the NASA guidelines[23] states that "software projects are to have formal software testing conducted, witnessed, and approved by an independent organization outside of the development team." NASA has implemented this in the NASA Independent Verification & Validation (IV&V) Facility,[20] which was founded after the space shuttle "Challenger" accident. According to NASA, Independent Verification & Validation requires:

a) Technical independence
b) Managerial independence
c) Financial independence

In the NASA IV&V Program, third party software verification is performed in parallel with the software design processes to mitigate risks at an early stage.

In the production of consumer software third party testing is extensively used in what is known as "Beta testing." New software is developed, verified and validated by a development team, and released in an "Alpha" version which is tested and corrected internally. A "Beta" version is then released and tested externally by selected users, acting as third party verification bodies, before the software is finalized and released to the market.

It is important to realize that third party testing does not replace internal test activities by the vendor or vice versa. Even if both third party and internal testing are done using HIL technology; both are important activities for achieving high quality software and meeting necessary standards for safety-critical control systems, see Figure . Without third party HIL testing, however, the control system software will not have been tested by anyone except the system vendor at delivery of the vessel.

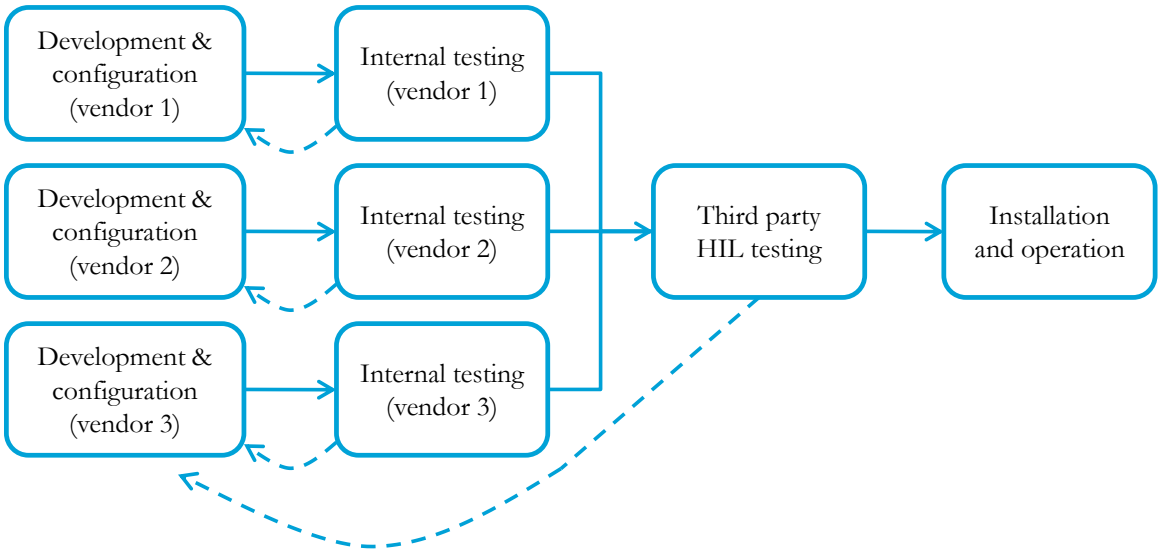

Figure 3.2 – Third party HIL testing of software.

3.4 Standards and class

Standards and guidelines for general software development[28] have been developed by organizations like ISO, IEC, and IEEE. These standards mainly consider the software development process, including software specification, development, testing and verification, and maintenance.

These standards are adopted by the different class societies and included in their rules for classification of ships.[24, 25] The class societies also give specific requirements for the functionality of the control system, and these requirements "flow down" to the control system software. Many of these requirements originate from the International Maritime Organization, IMO.[3] Also the International Marine Contractors Association (IMCA) and the different flag states have requirements or guidelines regarding control system functionality. There are, however, few specific requirements for software testing, verification and validation.

Presently one classification society (DNV) has developed a voluntary class notation[29, 30] for HIL testing of DP computer systems and a Standard for Certification of HIL testing [31] that describes generic requirements to HIL testing.

3.5 HIL test activities

Today a typical HIL project may be comprised of the following test activities[32, 33]:

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 the start of commissioning and trials. Most findings from this initial testing should be solved and closed during a software re-test. Software testing may also include some integration testing.

Integration testing can be performed in conjunction with software testing when it is beneficial and possible 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 the physical interface between the installed systems is included in the test scope.

Periodic testing secures the control system software during the vessel's life cycle. The periodic testing is executed as a software test on replica HW or as an 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 conditions during the life-cycle, do not introduce new weaknesses or errors in the target system.

3.6 HIL test scope

The overall test scope for a specific vessel must be tailored to its specific control systems. A typical HIL test programs may be 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 compliance with the class rules. 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 severe consequences. A typical HIL test program therefore consists of several types of tests:

- **Functional testing**: Verification of control system functions and modes during normal operation.
- **Failure mode testing**: Testing of control system detection and handling of failures and errors in signals, sensors, actuators and equipment
- **Performance testing**: Testing of control system performance under different operational and environmental conditions. Performance testing requires high fidelity models and should be subject to careful analysis of model accuracy and sensitivity.
- **Integration testing**: Testing of integration between at least two control systems.

Even with the benefits of HIL in facilitating early testing outside the critical timeline, it is not practically feasible to achieve 100 % test coverage for a complex control system, even if only single failures are considered. This is due to the fact that even a single signal may fail in a number of ways, including broken wire, short circuit, frozen value, slow/fast drift, noise, and wild-points, with typical interfaced signal counts ranging from a few hundred to several thousands. If considering also hidden, common mode, and multiple failures, the task of selecting a proper test scope becomes increasingly difficult. An important principle is then to focus testing on failures with large risk, i.e. considering both probability and consequence.

3.7 Relevant control systems for HIL testing

A modern DP vessel is equipped with a multitude of automation systems that are essential for the safety, reliability, and performance of the vessel. Example control systems that are relevant for HIL testing are:

- Dynamic Positioning (DP) Control Systems
- Power Management Systems (PMS)
- Thruster Control Systems
- Integrated Automation Systems (IAS)
- Drill-floor Control Systems
- Drilling Control/Safety Systems
- BOP Control Systems
- Well Control Systems
- Crane Control Systems
- Offloading Systems
- Diving Control Systems
- Pipe-laying Systems
- Ballast Systems

4 Discussion and Conclusion

Technology is changing faster than the engineering techniques needed to cope with the new technology are being created. Lessons learned over generations about designing to prevent accidents may be lost or become ineffective when older technologies are replaced with new ones. New technology introduces unknowns into our systems, and even so-called "unknown unknowns." Concurrently, as the development of new technology sprints forward, the time to market for new products is significantly decreased and strong pressures exist to decrease this time to market even further.[2] Deepwater drilling is continually in front when it comes to adopting new technology required to conquer larger ocean- and drilling depths.

The most common accident models are based on an underlying assumption that accidents are the result of an uncontrolled and undesired release of energy or interference in the normal flow of energy. Our increasing dependence on information systems is, however, creating the potential for loss of information or incorrect information that can lead to unacceptable physical, scientific, environmental and/or financial losses, as seen in the case of Deepwater Horizon.

It is important to realize that there are very few limits to how software may be designed. An apparently small fix to one part of the software may cause unexpected behavior in another part of the software, potentially causing a complete failure to comply with the designed system functionality. This means that commissioning, maintenance and testing of control system software are highly non-trivial tasks that deserve significantly more attention than they are currently receiving. Most of the automation systems on today's vessels are put into operation without independent software testing of any kind.

Regardless of the amount of testing and verification done by both the control system vendor and third parties, there is a significant probability that software bugs, weaknesses and configuration errors are present in the control system that is put into use. This is not unique to the maritime and offshore industries, but rather it is inherent in a control system based on sophisticated software. When such bugs, weaknesses or configuration errors are discovered, the control system vendor will usually go onboard the vessel to update the software to fix the problem, in a similar way to a service engineer replacing a malfunctioning hardware unit. This can be done through changes in the project specific software and configuration, installation of a software "patch" that fixes the problem, or by installing an update or new release of the core software (where also other changes, fixes, and improvements may have been made). When such a change of the control system software is done, it should be viewed as a major event and followed up by thorough risk assessment by the vessel's management, in a similar way as would be the case if a generator, a GPS, or another central piece of hardware was to be changed. To achieve this it is necessary to increase the focus on software as a safety critical component, and work to improve understanding of the functionality and criticality of the control system software amongst vessel owners and crew.

Digital technology has created a quiet revolution in deepwater drilling, but safety engineering techniques have not kept pace. Digital systems introduce new "failure modes" that are changing the root causes and course of events of accidents. Many of the approaches that worked on electromechanical components—such as replication of components to protect against individual component failure (i.e., redundancy)—are ineffective in controlling accidents that arise from the use of digital systems and software. Redundancy may even increase risk by adding complexity. Often,

technological systems are made to be so called "fail safe." Fail safe describes a device or feature which, in the event of failure, responds in a way that will cause no harm, or at least a minimum of harm, to other devices or danger to personnel. This "fail safe" terminology is often misapplied and misused, and for most of the safety critical systems there are no truly "fail safe" conditions. Either the system works as intended and maintains safety, or it does not and may cause or fail to prevent an incident or accident.

Emergency situations caused by control system failures or design weaknesses are often trusted to be handled and mitigated by human intervention. However, this requires both fast and accurate alarms and warnings, as well as detailed operator knowledge of the system. This may in practice be unrealistic, especially considering that the control system behavior and alarms after a control system failure may be undocumented and inadequate for making the correct decisions. All human behavior is influenced by the context in which it occurs, and operators in high-tech systems are often at the mercy of the design of the automation system software. Many recent accidents blamed on operator error could more accurately be labeled as resulting from flawed system and interface design. Inadequacies in communication between humans and machines are becoming an increasingly important factor in accidents.[2] Because of this, verification of adequate alarms and warnings during failure testing must be an important part of a HIL test scope.

A fundamental premise in the DHSG work is to look forward to ensure that the oil and gas resources are developed in a reliable, responsible and accountable manner. This white paper addresses an important aspect of the TDS related to safety critical systems including software/hardware. Safety critical systems are usually engineered according to the principles of barriers and independent systems to ensure redundancy. In a control system, many of these barriers will exist only in software. Failures in software can therefore act as common cause failures, and significantly reduce the reliability of the system. This paper has introduced HIL testing as a tool for independent verification and validation of safety-critical control system software, covering an evident gap in the presently available tools for risk management.

5 Definitions and Abbreviations

Term	Definition
ALARP	As Low As Reasonably Practical
Artemis	Artemis MK5 is an accurate, automatic microwave position fixing system based on range and bearing metrics and is used in the subsea oil and gas industry..
BOP	Blowout Preventer
DHGS	Deepwater Horizon Study Group, Center for Catastrophic Risk Management, UC Berkeley
DGPS	Differential Global Positioning System
DP	Dynamic Positioning
DP system	Comprised of a DP control system, a power system, and a propulsion system including thrusters. The DP control system is further comprised of the DP computer system and the position reference systems and sensors.
ECU	Electronic Control Unit
EDC	Emergency Disconnect
FMEA	Failure Mode and Effect Analysis

FPSO	Floating Production, Storage and Offloading vessels
HES	Health, Environment, and Safety
HIL	Hardware-In-the-Loop
HPR	Hydroacoustic Positioning Reference
HW	Hardware
IEC	International Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IMCA	International Marine Contractors Association
IMO	International Maritime Organization
I/O	Input / Output
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
Mission-critical system	A system whose failure or malfunction may result in abortion of an ongoing or intended task or mission
MRU	Motion Reference Unit
NASA	National Aeronautics and Space Administration
PMS	Power Management System
PSA	Petroleum Safety Authority Norway
Safety-critical system	A system whose failure or malfunction may result in death or serious injury to people, loss or severe damage to equipment, or environmental harm
SW	Software
TDS	Technology Delivery System

6 References

1. Keener, C., Keji-Ajayi, I., Allan, R., 2003. Performance Gains with 5th Generation Rigs, SPE/IADC Drilling Conference. SPE/IADC Drilling Conference, Amsterdam, Netherlands.
2. Leveson N. A new accident model for engineering safer systems. Safety Science. 2004;42:237-70.
3. IMO. Guidelines for Vessels with Dynamic Positioning Systems. IMO Maritime Safety Committee Circ. 645, 1994.
4. IMCA. M 113 Guidelines for Vessels with Dynamic Positioning Systems (IMO MSC Circular 645). International Marine Contractors Association, 1994.
5. Aven T, Vinnem JE. Risk Management: With Applications from the Offshore Petroleum Industry. London: Springer-Verlag London Limited; 2007.
6. Sklet S. Safety Barriers on Oil and Gas Platforms. Trondheim: NTNU; 2005.
7. IMCA. M 166 Guidance on Failure Modes & Effects Analyses (FMEAs). International Marine Contractors Association, 2002.
8. IMCA. M 198 Dynamic Positioning Station Keeping Incidents Reported for 2007 (DPSI 18). International Marine Contractors Association; 2009.
9. *PSA. Trends in risk level in the petroleum activity 2009. Petroleum Safety Authority Norway; 2010.*

10. *Kee-Choon Kwon; Soon-Ja Song; Won-Man Park; Sung-Pil Lyu; "The real-time functional test facility for advanced instrumentation and control in nuclear power plants," IEEE Transactions on Nuclear Science, Volume 46, 1999.*
11. Badaruddin, K.S.; Hernandez, J.C.; Brown, J.M.; "The Importance of Hardware-In-The-Loop Testing to the Cassini Mission to Saturn," 2007 IEEE Aerospace Conference.
12. Herbert Schuette; Peter Waeltermann, "Hardware-in-the-Loop Testing of Vehicle Dynamics Controllers – A Technical Survey," 2005 SAE International.
13. Seminario, M.A.; Insaurralde, C.C.; Jimenez, J.F.; Giron-Sierra, J.M.; "Hardware in the loop laboratory simulation to test a distributed avionic system," 2005 digital avionics system conference.
14. Handley, R.J.; Stokes, R.F.; Stevenson, J.; Owen, J.I.R.; "Hardware-in-the-loop testing of the NATO standardisation agreement 4572 interface using high precision navigation equations," 2008 IEEE/ION Position, location and navigation symposium.
15. Ayasun, S.; Fischl, R.; Chmielewski, T.; Vallieu, S.; Miu, K.; Nwankpa, C.; "Evaluation of the static performance of a simulation-stimulation interface for power hardware in the loop," Power Tech Conference Proceedings, 2003 IEEE Bologna.
16. Aghili, F.; Piedboeuf, J.-C.; "Hardware-in-loop simulation of robots interacting with environment via algebraic differential equation," IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2000.
17. Leitner, J., "Space technology transition using hardware in the loop simulation," IEEE Aerospace Applications Conference, 1996.
18. Ramaswamy, S.; Prasad, B.V.; Mahajan, R.C.; Goel, P.S.; "The role of hardware in-loop motion simulation for Indian satellites," IEEE Transactions on Aerospace and Electronic Systems, Volume 27, 1991.
19. dSPACE, http://www.dspace.com.
20. NASA Independent Verification & Validation Facility, http://www.nasa.gov/centers/ivv/home/.
21. Mathworks, "Bell Helicopter Develops the First Civilian Tiltrotor." http://www.mathworks.com/company/newsletters/news_notes/oct06/bellhelicopter.html.
22. NASA, "Software Engineering Requirements," 2009
23. NASA, "Software safety and guidelines," 1997.
24. Det Norske Veritas (DNV), "Rules for Classification of Ships," July 2010.
25. American Bureau of Shipping (ABS), "Rules for building and classing steel vessel," Jan. 2010.
26. Lloyd's Register, "Rules and regulations for the classification of ships." July 2007.
27. Germanischer Lloyd (GL), "Rules & Guidelines," 2010.
28. ISO/IEC, "ISO/IEC 12207:2008, Systems and software engineering -- Software life cycle processes." 2008.
29. DNV. Rules for classification of Ships, Part 6 Ch 22 Enhanced System Verification (ESV), 2009.
30. DNV. Rules for classification of Ships, Part 7 Ch 1 Sec 7 I. Enhanced System Verification - SiO, 2010.
31. DNV. Standard for Certification of HIL testing. Draft, 2005.
32. Smogeli, Ø.. Ensuring Safety, Reliability and Effectiveness – Testing DP Systems. European DP Conference, London, 2009.
33. Smogeli, Ø. Experiences from 5 years of DP system software testing. DP Conference, Houston, 2010.