DYNAMIC POSITIONING CONFERENCE
October 13-14, 2015

OPERATIONS

Automated Hardware-In-the-Loop Testing – Experience from Onboard Remote Testing with CyberSea Signature

By Luca Pivano, Nicolai Husteli
Marine Cybernetics

Jan Mikalsen, Paal Liset
Marine Technologies

Abstract

Modern ships and offshore rigs have advanced computer systems for dynamic positioning, power generation and distribution, drilling, lifting operations and other automation systems. It is well known that software errors may lead to delays and non-productive time, and compromise safety and lead to environmental disaster. While the testing and verification regime for structures and machinery systems is well established, most of the computer systems on today's vessels are put into operation without independent testing and verification. The risk of software failure can be mitigated by performing Hardware-In-the-Loop (HIL) testing. HIL testing is a well proven test methodology from several other industries. It facilitates systematic testing of control system design philosophy, functionality, performance, and failure handling capability, both in normal and off-design operating conditions, and is conducted in a virtual test-bed where there is no risk to man, vessel, or equipment. In order to perform testing in an efficient and effective way, automated HIL testing has been developed.

This paper briefly presents HIL testing for DP control systems and shares experiences and challenges from automated HIL testing performed on a series of Edison Chouest Offshore platform support vessels. This is the result of a joint effort of Marine Technologies and Marine Cybernetics. By developing an enhanced HIL interface towards the DP control system, Marine Technologies provides the possibility to replace the DP Operator with a *virtual one*, offering the opportunity for running automated software regression testing with Hardware-in-the-Loop technology developed by Marine Cybernetics.

Contents

Introduction 1

Risk management for maritime control system software 3

Hardware-in-the-loop testing of control system software 3

HIL Test Process 4

Lifecycle software change management 5

Automated HIL testing 7

Experience from automated HIL testing 9

Conclusion 11

References 12

Introduction

In a few decades, the complexity of control systems and software on board marine vessels have increased significantly. Propulsion and maneuvering systems, power systems, cargo-handling systems and navigation systems on modern vessels are examples of systems that are often a collection of hardware and software from different vendors. For a dynamic positioning (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 local and remote control systems, as well as all the auxiliary systems needed for electric, mechanical, and hydraulic power, lubrication, cooling, ventilation, and fuel. At the heart of these subsystems lie computer control systems, which in turn run complex software. This software is critical for the safety and efficiency of the operations.

Recent development has led to increasingly distributed functions between different systems and vendors, where hardware and software components must work as one integrated system. The software systems on a vessel today by far exceeds any mechanical, electrical or hydraulic system in complexity and – more importantly – in lack of transparency. This has introduced challenges in designing, building, and maintaining these systems. One of the key challenges is to manage the control system software.

Why is software difficult to manage, and why does software fail? Firstly, software is invisible to the eye as compared to hardware. Secondly, software is extremely flexible and enables implementation of highly complex logics, state machines and dynamic models. Software cannot only replace existing functions, it can also implement new functions, which are too costly or difficult to implement by hardware. This is a great advantage, but there is a downside, described by [11] as "the curse of flexibility". Software has no physical constraints that limit the flexibility and complexity of what we build, and the limits of what is possible to accomplish are different from the limits of what can be accomplished successfully and safely. It is easy to construct complex software that goes beyond human intellectual limits, making it hard to understand how it will behave under all conditions. If we look to the maritime industry, software deliveries are often unique and tailor-made for a specific vessel. A lot of software functions and configurations are written under a tight time schedule, and finished late in projects. Furthermore, integration of systems from different vendors is challenging and error-prone due to the complexity of the control systems, connected via many signals and interfaces.
Change management of software is also an important issue. While a defect hardware unit can be replaced, a faulty software function cannot be replaced, it has to be updated. Updating software is usually quick and straightforward, but herein also lies the challenge. Updates and patches may introduce new problems, including issues related to security and safety. Modifications and repairs can and tend to be made locally and at low cost, often by different people from one time to another. This may also lead to deficiencies in documenting the modifications.

What are the consequences if the DP system software fails? The most serious safety breach during DP operation is when the vessel no longer is capable of maintaining its desired position and/or heading, which may result from a drive-off or a drift-off. A drive-off is considered the most dangerous situation, where the thrusters force the vessel off position. A drift-off occurs if the weather forces drive the vessel off position, usually due to lost thrust capacity.
Software failures may also cause business interruptions due to loss of capability/capacity to conduct the planned operation.

While the testing and verification regime for structures and machinery systems is well established, most of the computer systems on today's vessels are put into operation without independent testing and verification. In order to solve this challenge, independent Hardware-In-the-Loop (HIL) testing has been introduced to the maritime and oil and gas industry more than one decade ago, see for example [12][15], [16] and [17].
Hardware-In-the-Loop testing is a well proven test methodology from several other industries. By employing advanced simulators, it facilitates systematic testing of control system design philosophy, functionality, performance, and failure handling capability, both in normal and off-design operating conditions, and is conducted in a virtual test-bed where there is no risk to man, vessel, or equipment.

The aim of this paper is to give a short introduction on HIL-testing for marine control system software and present experiences and challenges from automated HIL testing performed on the DP control system of a series of platform support vessels from Edison Chouest Offshore. This is the result of a joint effort of Marine Technologies and Marine Cybernetics. By developing an enhanced HIL interface towards the DP system, Marine Technologies offers the possibility to replace the DP Operator with a virtual one providing the opportunity for running automated software regression testing with Hardware-in-the-Loop technology.

Risk management for maritime control system software

As described in [14], the IMO standard for safe management and operation of ships [9] sets requirements to identifying hazardous failure modes for equipment and technical systems, and this holds for software as well as hardware. Specific measures to promote safety and reliability of such systems through proper safety management and regular testing of safety-functions are also required.
There are well-established processes for independent risk assessment of structures and electro-mechanical hardware systems using the risk assessment methods such as HAZOP, FMEA/FMECA, Fault trees, quantitative risk assessment (QRA) and safety integrity level (SIL), see [14] for further description. Some of these methods are also suitable for assessment of software if they are adapted to the way software fails. However, while hardware components have established failure modes and well-known physics of deterioration, two versions or configurations of software may fail in completely different ways. This means that it is necessary to verify a risk analysis through testing.
So, what is the status of software verification in the maritime industry today? The desktop DP system FMEA study analyses the physical layout of the vessel systems, 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. In the DP system FMEA proving trials, focus is on the hardware components and only sparsely the software. The software functionality of the computer systems is only superficially tested, mainly due to a lack of appropriate testing tools. Vendors apply their development and delivery quality processes which may comply with various standards and class rules. An important standard that recommends independence in the verification effort is IEEE 1012 [7] .The IEEE 1012 Standard for System and Software Verification and Validation is recognized as the de-facto verification standard for development of high quality software systems by several US organizations such as US armed forces, NASA, Federal Aviation Administration (FAA) and Department Of Defense. Typically the internal testing performed by the vendor does not possess the characteristics of independence described in the IEEE 1012 Standard.

Quantification methods used for hardware cannot be applied to software. The standard for SIL, IEC 61508 has recognized this, and focuses on software development and testing. However, SIL is much less widespread in the maritime industry than in the automotive, railway, and nuclear industries.
In order to improve the risk assessment of software, the industry should focus on four areas:

- More focus on software in risk assessment, in particular software FMEA and software HAZOPS.
- Software engineering processes, and the verification of these through use of recognized standards such as IEEE 12207, ISDS [5], ISQM [2], and ISIS [13].
- Testing and verification using recognized standards such as IEEE1012, ISO 29119, ESV [6] or SV [1].
- Life-cycle software change management.

Hardware-In-the-Loop (HIL) testing is today the main tool for testing of control system software, and it plays an important role in all of the four areas of improvement.

Hardware-in-the-loop testing of control system software

Hardware-In-the-Loop (HIL) testing is a well-proven test methodology from automotive, avionics, and space industries, and has been available to the marine and offshore industries for almost a decade. The main idea of HIL-testing is to use advanced simulators (see the test setup shown in Figure 1) capable of simulating the dynamic response of the vessel with its power plant, thrusters, and other relevant equipment. In this way, the control system will not experience any difference between the real world and the simulated world. 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. In order to properly assess and verify control systems from different vendors and the integration between these systems, independent testing technology is essential. See [12][15], [16] and [17] for more details.
HIL testing has also been recognized by the Class Societies as an effective testing technology. DNV has developed voluntary class notations [6] for DP-HIL, PMS-HIL, Drill-HIL and Crane-HIL testing and a Standard for Certification of HIL testing [4] that describes generic requirements to HIL testing. Similarly ABS has introduced a voluntary class notation [1] that supports extended system verification using HIL or Software-In-the-Loop testing.

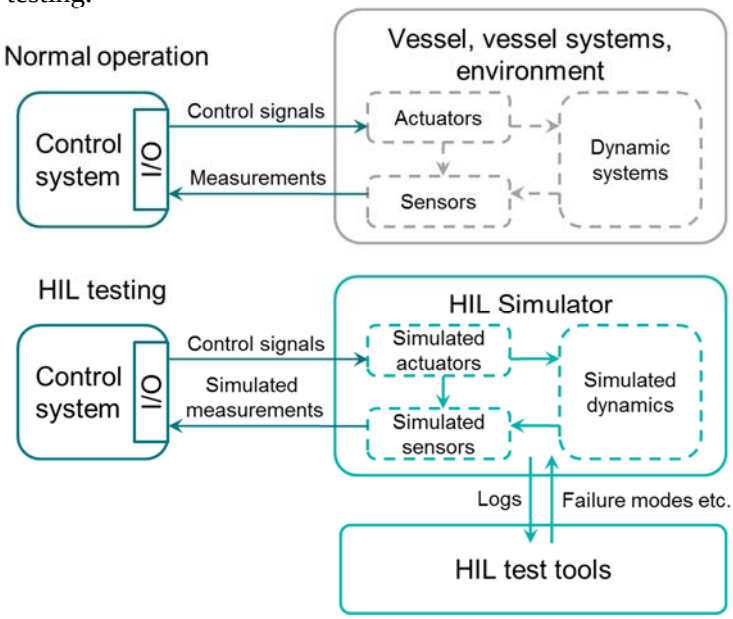

Figure 1 HIL test conceptual setup

For testing and approval, the main Class concern is control system handling of single failures. However, other concerns like operational availability, reliability 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.

HIL Test Process

A typical test process adopted for HIL testing is shown in Figure 2. Preparations for HIL testing starts with collection of vessel and system documentation. This work typically starts 3-6 months before the first HIL test, and includes analyzing functional design descriptions, user manuals, single line diagrams, operating procedures and guidelines, and other relevant documentation. Based on the documentation and dialogue with the end user, yard, and equipment vendors, the test programs, HIL simulators and interface protocols are established. After a period of HIL interfacing and commissioning, where the performance of the test setup is validated and verified, the first HIL test commences. The first test is typically performed in a Lab with the actual target system hardware or with replica-hardware. The timing of the first HIL test typically coincides with the software Factory Acceptance Test (FAT). For a DP control system the first test can vary

from 40 to 80 hours depending on the complexity of the system. During testing, a number of test cases are executed, and any deviations from the expected system behavior are analyzed and recorded. All stakeholders take part in the analysis and categorization of findings, and an agreement is made for follow-up of each item. When the test is completed, a period for software updates by the vendor is scheduled before a follow-up test is conducted.

The second test typically coincides with onboard commissioning, either directly before or directly after depending on customer requirements. The primary goal of the second test is to close findings from the first test, and to perform spot-checks to confirm that the performance and robustness of the system is preserved. Further test activities for the newbuild are scheduled on demand. HIL testing may also be performed as part of the vessel acceptance phase, to help secure the delivery to the end user.

The HIL testing process is inherently a detailed review of the system design, functionality and robustness. System drawings and documentation are scrutinized, assuring that the documentation is complete and consistent, and according to its intended use. Throughout the project - from system analysis, test design and simulator design to test conduction and analysis – the continue focus on "what could possibly go wrong" will ensure that the complete system meets its requirements.

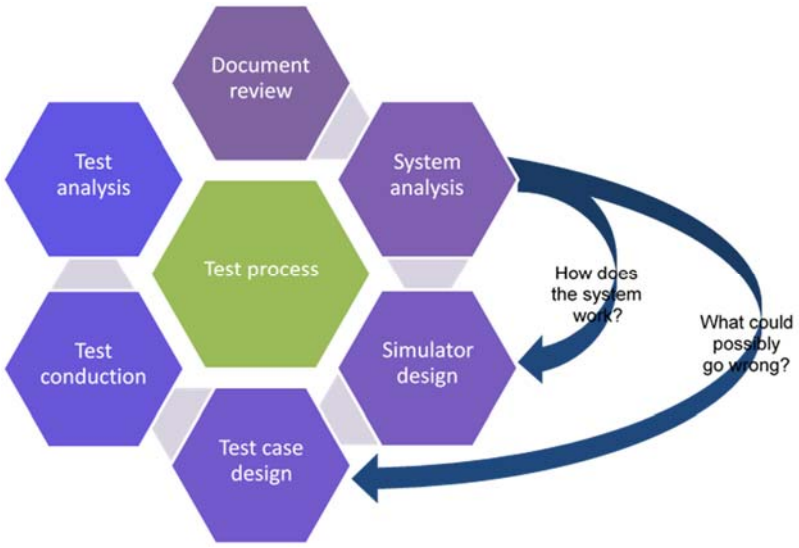

Figure 2: HIL test process

Lifecycle software change management

Life-cycle software change management (SCM) on vessels is a rather new concept, but is now receiving increased attention across the industry. DNV, ABS and Lloyds Register released new class notations for life-cycle software management [5][2][13], termed ISDS (Integrated Software Dependent Systems), ISQM (Integrated Software Quality Management) and ISIS (Integrated Software Intensive Systems) respectively. The aim of these notations is to introduce a system for improving and securing the software quality, all the way from design/development to decommissioning, and to manage the risks associated with software throughout the vessel lifecycle.
In this context it is important to realize that such assessment of software risks is highly challenging. One of the reasons is that there are very few limits to how software may be designed. An apparently small change to one part of the software may cause unexpected behaviour in another part of the software, potentially causing a complete failure to comply with the designed system functionality. Integrated systems with software from different vendors make this challenge even harder to manage.

No matter what kind of SCM approach that is chosen, there is an immediate need for tools and processes to test and verify that the software meets the chosen acceptance criteria. The testing and verification activities are based on the risk assessment and verification management. For a given verification process, a number of different verification methods may be combined to provide the best verification coverage. Independent HIL testing provides these tools and processes for the complete life-cycle of the vessel, and goes hand-in-hand with a proper SCM program.
As described in the ISDS notation [5], the vessel life-cycle can be coarsely divided in two main activities, new-build/retrofit and operations. The new-build/retrofit phase can be further divided in engineering, construction and acceptance phases, as shown in Figure 3. HIL testing can be adapted, planned and carried out to fit the needs of each phase. However, HIL testing as well as the other test activities that may involve software (FMEA, vendor internal testing, FAT, CAT) today focus mainly on the new build phase.

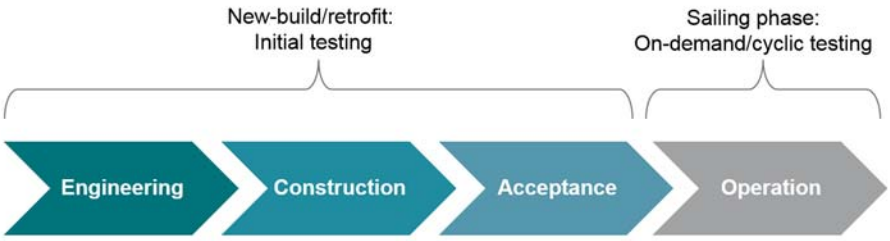

Figure 3: Vessel lifecycle phases

In the vessel operation phase the focus is on operational safety and efficiency. During this phase maintenance to both hardware and software is carried out and software changes are implemented for various reasons. The vendors may want to update their software when relevant bugs are discovered or in order not to have too many versions installed on the vessels with their system. Changes may also be implemented to solve integration problems or operational issues discovered during operations. In case of incidents, investigations are typically carried out and upgrades may be installed when the systems are checked or as the result of the investigation. When new equipment is installed due to a replacement or add-on, software may need to be updated, reconfigured or tuned depending on the needs. New versions can also be installed when a vessel operator requires new functionality due to a new chartering requirement or another operational need.
If testing is performed in the build phase, as soon as the software is updated the value of the testing may drop significantly. This is a challenge as HIL testing implicates a substantial investment in technology, time and money. As described in the previous session, testing involves the understanding of the system that is the target of the test, understanding the vessel's operational philosophy and building sophisticated vessel simulators. How to exploit this technology and this knowledge after the new build phase? When applying a proper life-cycle SCM (see Figure 4 for an example), a risk assessment of the control system software upgrades may require conducting HIL testing of the updated control software in order to reduce the risk. As the most of the preparation done for the HIL testing was done in the build phase, this new test should not be difficult to perform. However, HIL testing, as it is performed today, is labour intensive. The test operator has to operate the target control system through its Human-Machine Interface (HMI) as well as operate the HIL simulators manually. This includes setting up test scenarios, triggering test cases and failure modes, and noting down the resulting target system performance in terms of response and warnings/alarms. This limits the test scope and number of test activities, since time and resources for testing are limited, especially for vessels in operation. To overcome these limitations, the next generation HIL test setups will include automated testing for parts or the entire the test scope. This is presented in the next section.

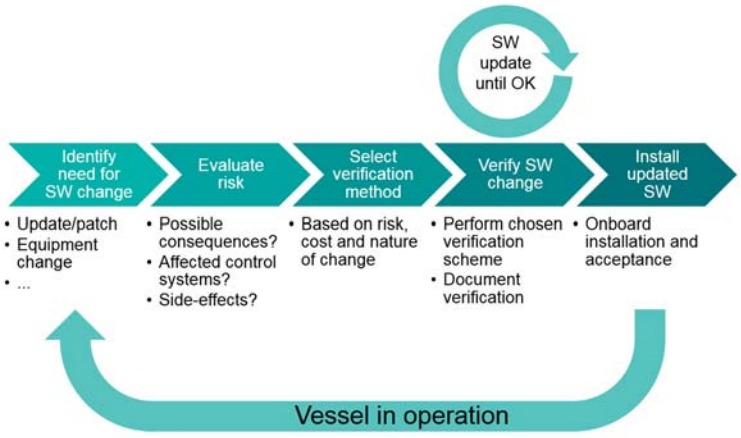

Figure 4: Software Change Management process

Automated HIL testing

Automated DP-HIL testing is the result of a joint effort of Marine Technologies and Marine Cybernetics. By developing an enhanced HIL interface towards the DP control system, Marine Technologies provides the possibility to replace the DP Operator with a virtual one. All main operations with the DP control system can now be performed in real-time via software as the enhanced HIL interface allows the following:

- Alarm messaging and acknowledge of alarms
- Enable/disable of thrusters
- Enable/disable sensors and positioning reference systems
- Manipulation of set points
- DP Mode selector
- Gain settings
- Joystick commands
- Thrust allocation settings

The enhanced HIL interface provides the opportunity for running automated software regression testing with Hardware-in-the-Loop technology developed by Marine Cybernetics.
By connecting a vessel simulator and a supervising test tool – CyberSea® Signature – to the DP control system (see Figure 5 and compare also with a standard HIL setup in Figure 1), testing of the DP software can be performed in a controlled environment and in an efficient way. The assessment of the test results can also be done automatically, providing the test operator the information in real-time if the tests have been successfully passed. Expected test results, in particular alarm handling, must be established as part of the manual HIL testing process performed during the build phase.
Figure 6 shows a screen shot of CyberSea® Signature while Figure 7 show one of the test cases performed with the automated HIL testing for DP control systems.

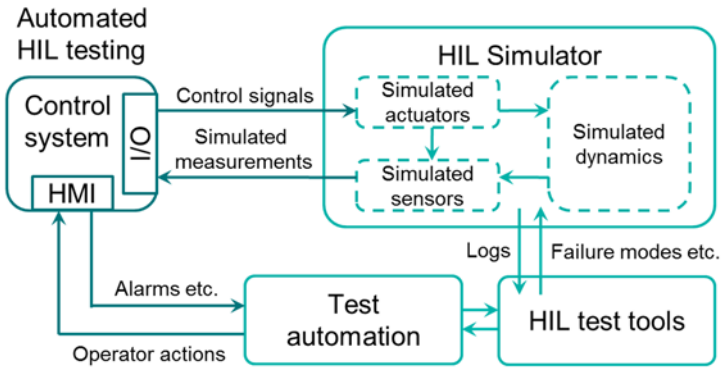

Figure 5: Automated HIL test conceptual setup

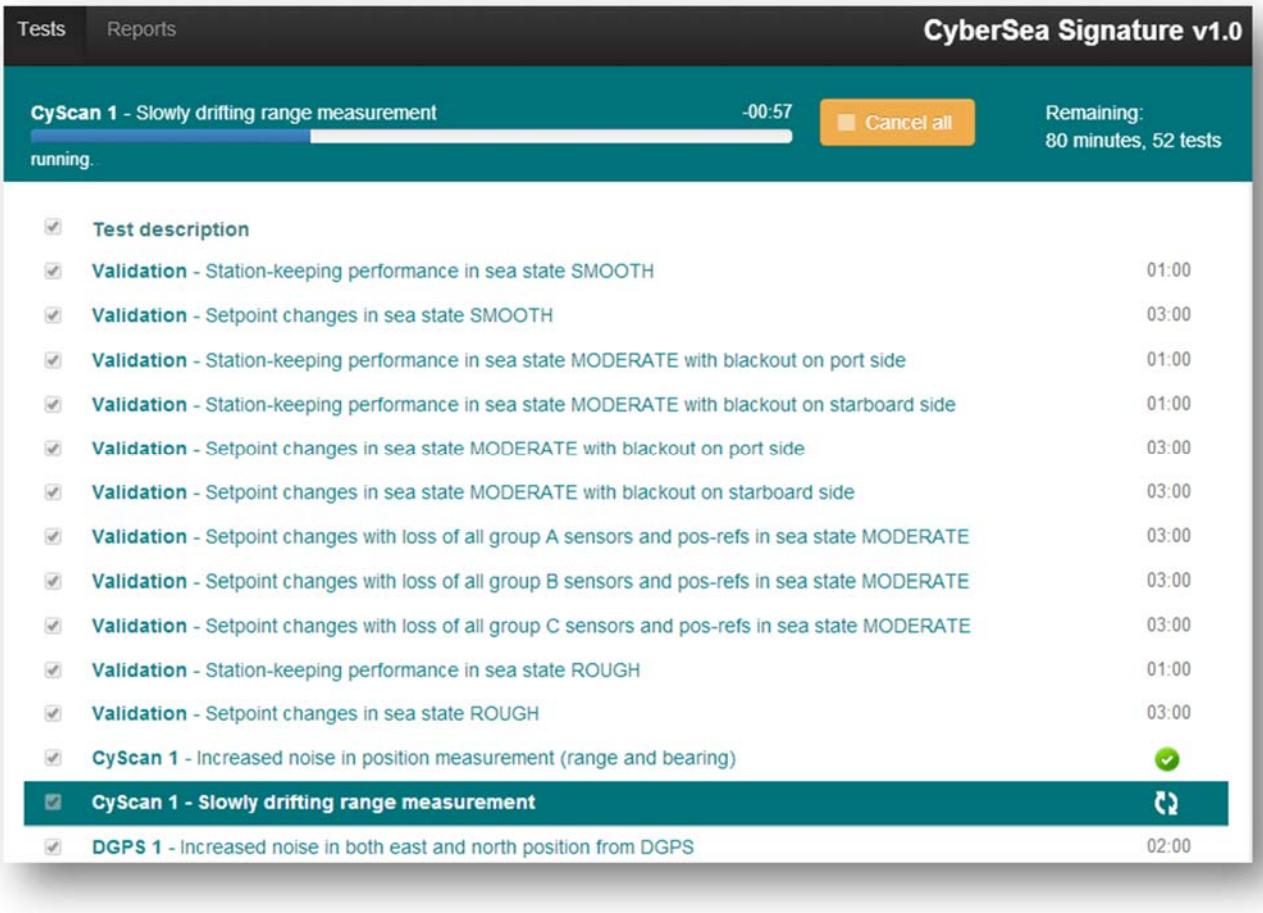

Figure 6: Screenshot of CyberSea Signature

The main goals for performing automated testing are:

- Automate repetitive and predictable tests during the newbuild phase
- Enable long-term endurance testing

- Facilitate automatic regression testing of the complete target system software once initial testing has been completed and a test result baseline established

The automated HIL test setup can be used both in a lab environment and on-board a vessel. Typically the lab setup would be used during the vessel build phase. Automated HIL testing can also be used in the vendor testing process during the product development phase, providing an independent assessment to ensure that a product's performance and safety meet the regulatory, safety and quality requirements. For the operational phase, both the lab setup and the on-board test represent valid alternatives.

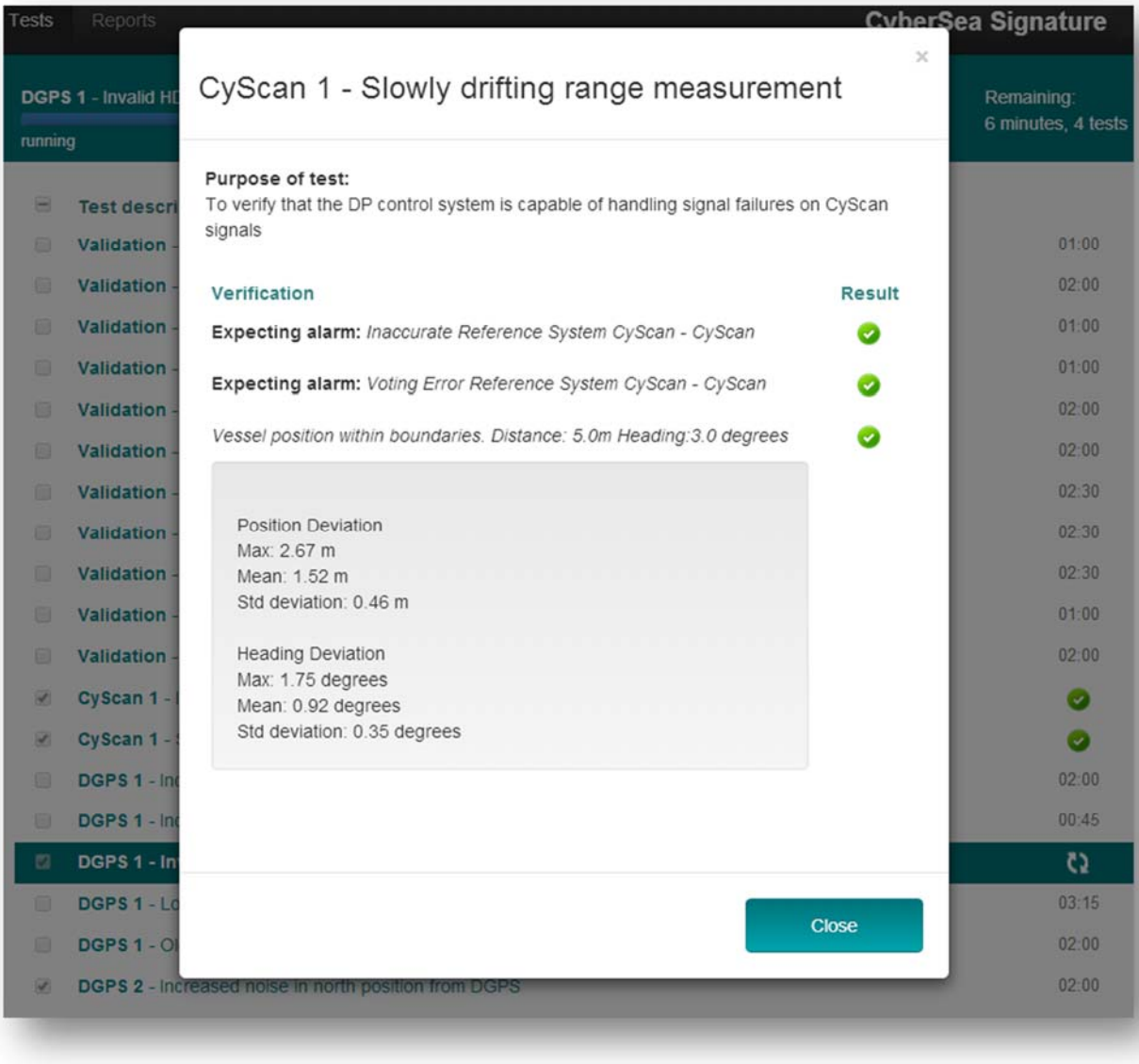

Figure 7: Example of a test case for the automated DP-HIL

Experience from automated HIL testing

A pilot project for a DP control system delivered by Marine Technologies to Offshore Service Vessels has already been successfully conducted. The system is now installed on a series of 13 Edison Chouest Offshore (ECO) vessels, the 312' platform support vessel series (see Figure 8). The hardware for the vessel simulator

and the automated HIL testing tool is integrated with the DP control system hardware in the vessel bridge. The tool user interface runs in the same operator station that can be used for DP operations.
There has been an initial test which was performed manually, as described in the previous sections, where the results has been recorded and discussed. This test, performed before the FAT carried out from the vendor, has been the basis for building the expected results and acceptance criteria for the tests in the automated tool. Up to today, automated testing has mainly be used in two phases:

- Before the Factory Acceptance Test, to verify that the DP control system configuration, functionality and performance was according to the requirements. This test was performed at the Marine Technology laboratory. The DP control system software was then ready for on-board installation if all the tests were successfully passed.
- After sea trials and DP tuning as an extra software quality check and verification.

For a series of vessels such as the ECO 312', the DP control system software is identical. There may be few configuration parameters that differ between vessels but the basic software is the same. Experience from the automated testing have shown that errors in the configuration of the DP control system resulted in test failures and consequent fixes by the software engineer. This ensured that the software was thoroughly tested and issues discovered before the installation on-board.

Due to the advanced communication system developed by Marine Technologies (see Figure 9), software upgrades of the DP control system can also be pushed remotely. Every time there is a new update of the control system software, testing can be performed before the DP system is taken to use in operation providing a safety net against bugs and other software issues. In addition, testing can be started and witness also remotely. The test tool records the *software signature* after the new update and can compare it with the signature recorded before the software change, building confidence that the software will perform as expected.

Figure 8: Edison Chouest 312' PSV series (Courtesy of Edison Chouest Offshore)

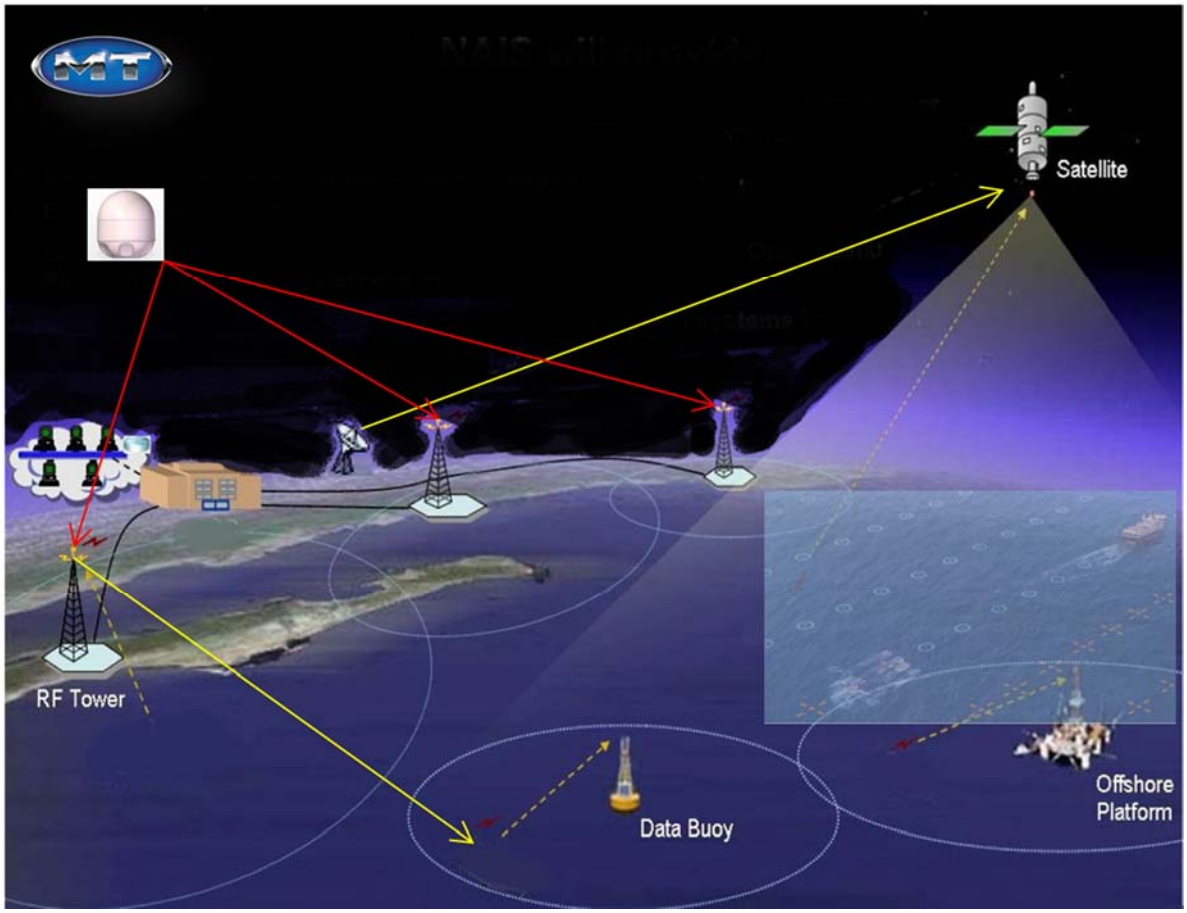

Figure 9: Marine Technologies Communication System C-Comm

Conclusion

Today, control and safety systems are to a large degree software driven. Highly complex logics, which are too difficult or costly to implement in hardware can easily be implemented in software. Software is extremely flexible, and it is straightforward to make changes to functionality. However, highly complex and flexible functionality is also associated with high risk for errors, and software can be extremely fragile. It is therefore important to focus also on software in safety management and risk assessments.

Traditional risk assessment techniques have been developed for hardware, and care should be taken when applying these to software. Some techniques are not suitable for software at all, due to fundamental differences in how hardware and software fail. Risk assessment of software is challenging, and it is easy to take shortcuts, by either ignoring the software (assuming it functions perfectly) or simplifying the analysis too much.

This aim of this paper was to highlight how independent Hardware-In-the-Loop (HIL) testing can be used to test, verify and validate software of the DP control system in the all vessel life-cycle, to manage and mitigate software risk, both for new-builds and vessels in operations. The paper showed how this can effectively be achieved by performing automated HIL testing. The paper also presented experiences and challenges from the automated HIL testing performed on a series of platform support vessel from Edison Chouest Offshore. This was the result of a joint effort of Marine Technologies and Marine Cybernetics.

The automated HIL testing has been successfully performed before the Factory Acceptance Test, to verify that the DP control system configuration, functionality and performance was according to the requirements, and after sea trials as an extra software quality check and verification.
Manual FMEA tests (for new-build, annual trials and 5-year renewal trials) can also be integrated in the tool and the results recorded. Reporting features in the tool provide the test result documentation right after the tests. This is the first step towards enhance system verification performed in an efficient way, where manual tests of the DP system performed in the FMEA activities are integrated and coordinated with automated software testing, in turns reducing risks and costs and at the same time increase testing coverage.

References

[1] ABS (2012). Guide for Systems Verification (Including Hardware-in-the-Loop and Software-in-the-Loop Testing).
[2] ABS (2014). Guide to Integrated Software Quality Management (ISQM).
[3] Christopher Goetz (2012). Managing software on new drilling rigs. Digital energy journal Nov-Dec.
[4] DNV (2011). Standard for Certification of HIL testing. SfC No. 2.24.
[5] DNV (2012). Integrated Software Dependent Systems (ISDS) - Offshore Standard DNV-OS-D203.
[6] DNV (2013). Rules for classification of Ships, Part 6 Ch 22 Enhanced System Verification (ESV).
[7] IEEE (2012). 1012-2012 Standard for System and Software Verification and Validation.
[8] IMO (1994). Guidelines for Vessels with Dynamic Positioning Systems. IMO Maritime Safety Committee Circ. 645.
[9] IMO (2010). International Safety Management Code.
[10] Jan Fredrik Hansen and Thomas N. Nielsen (2009). Fuel Efficient LNGC Propulsion Using Variable Speed Electric Propulsion Drives. Propulsion and Emissions Conference.
[11] N. Leveson (1995). Safeware: System Safety and Computers.
[12] L. Pivano, Ø. Smogeli (2013). Independent HIL testing of DP systems – a life-cycle perspective. Dynamic Positioning conference Brazil, Rio the Janeiro.
[13] Lloyds Register (2013). Rules and Regulations for the Classification of Mobile Offshore Units, Part 3, Chapter 14, Integrated Software Intensive Systems (ISIS), June 2013.
[14] Ø. Smogeli, B. Vik, O.I. Haugen. and L. Pivano (2014). Risk management for control system software for the maritime and offshore oil and gas industries. Proceedings of the IMCA Annual Seminar, London.
[15] Tor A. Johansen and Asgeir J. Sørensen (2009). Experiences with HIL Simulator Testing of Power Management Systems. Dynamic Positioning Conference, Houston.
[16] Tor A. Johansen, Asgeir J. Sørensen, Ole J. Nordahl, Olve Mo, Thor I. Fossen (2007). Experiences from Hardware-in-the-loop (HIL) Testing of Dynamic Positioning and Power Management Systems. OSV Singapore.
[17] Tor A. Johansen, Thor I. Fossen, Bjørnar Vik (2005). Hardware-in-the-loop testing of DP systems. DP Conference, Houston.