MODELING, IDENTIFICATION AND CONTROL, 2006, VOL. 27, NO. 4, 239–258
doi:10.4173/mic.2006.4.3

Modeling,
Identification
and
Control

Hardware-in-the-loop testing of marine control systems¶

ROGER SKJETNE*† and OLAV EGELAND†‡

Keywords: *Hardware-in-the-loop simulation, black box testing, functional testing, marine control systems, failure modes, testability, IEC 61508, dynamic positioning system*

Hardware-in-the-Loop (HIL) testing is proposed as a new methodology for verification and certification of marine control systems. Formalizing such testing necessitates the development of a vocabulary and set of definitions. This paper treats these issues by constructing a framework suitable for industrial HIL test applications and certification of marine systems.

1. Introduction

As modern machinery systems for marine vessels become increasingly complex, there is a need to develop new and improved methods for testing and verification (Marine Cybernetics *et al.* 2004). This is important in order to give the vessel owner confidence in the acquired systems, to document sufficient quality, functionality, and performance to vessel contractors, and to verify compliance with classification rules. In this context, testing by HIL simulation of the control and monitoring systems has recently been proposed. This is a well-proven methodology from the automotive, avionics, and space industries; see e.g. IPG Automotive (2005). Eventually, HIL testing may also set a new standard for certification of marine control systems.

This paper tries to clarify concepts such as what the primary target system is for HIL testing of an integrated marine control system, what functions that are targeted, and the requirements for testability of those functions. Moreover, the paper discusses HIL simulators and characterizations such as SW/HW ratio and level of modeling. Based on this, a framework for HIL testing is developed to target the operational and safety functions of industrial marine control systems. Dynamic positioning systems is a suitable application and used as an example in the text.

Abbreviations:

CAT	Customer Acceptance Test
DNV	Det Norske Veritas
DP	Dynamic Positioning
FAT	Factory Acceptance Test
HIL	Hardware-In-the-Loop
HMI	Human Machine Interface

*Corresponding author.

†Marine Cybernetics AS, Trondheim, Norway.

‡Norwegian University of Science and Technology, Trondheim, Norway.

E-mails: rs@marinecybernetics.com & oe@marinecybernetics.com

¶An early version of this paper was presented at SIMS 2005, the 46th Conference on Simulation and Modeling, Trondheim, Norway, October 13–14, 2005.

HW	Hardware
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMCA	International Marine Contractors Association
IMO	International Maritime Organization
ISO	International Organization for Standardization
MC	Marine Cybernetics
OS	Operator Station
SW	Software
TaD	Test at Dock
TaF	Test at Factory
TaS	Test at Sea
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit

2. Control system

Control is to monitor and/or command the essential states (i.e. the representing variables) of a physical process in an autonomous fashion using technological components such as sensors, actuators, and computer equipment. Pure monitoring—using sensors, or pure commanding—using actuators, yields open-loop architectures, while combining equipment for both monitoring and command yields a closed-loop feedback architecture that satisfies an overall control objective. The most common control objectives are *regulation*—to control the process output variable to a fixed reference, and *tracking*—to make the process output variable track a time-varying reference; see Skjetne (2005).

The following definitions apply:

Def: **Plant:** The physical process to be controlled or monitored. The plant describes the dynamic behavior of the process resulting from the input actions such as exogenous loads and actuator efforts (e.g. environmental forces and thruster forces for a vessel). The dynamic behavior is represented by physical variables providing the essential states of the process (e.g. position, heading, velocity, temperature, pressure, etc.) at each continuous or sampled instant of time.

Def: **Control system:** All systems and components, hardware, software, and user interfaces, necessary to perform the required control function. The main subsystems are:

- Power system.
- Actuator system.
- Sensor system.
- Control computer system.

Def: **Power system:** All systems and equipment necessary to supply electric power to all the essential consumer units in the control system, including associated cabling, segregation, and cable routing.

Note: The essential consumers are those needing continuous (or prioritized) supply in order to assure continuous operation and safety of the control application.

Def: **Actuator system:** All components and subsystems necessary to supply the control system with necessary effort (action) to make the plant behave in the desired manner. This includes:

- Actuation devices (e.g. thrusters, propellers, winches, motors, etc.) and necessary auxiliary systems (e.g. gears, pumps, lubing, cooling, etc.).
- Local actuator control system.
- Actuator sensors for monitoring and local control.

Def: **Sensor system:** All measurement equipment, with hardware, software, and algorithms (e.g. Kalman filters), including signal communication equipment, that supply the control system with information and corrections necessary to perform the required control and monitoring function of the application.

Note: Signal communication equipment includes all equipment and cabling that exclusively transmits the specific sensor information up to some sink, e.g. a serial link up to the respective control computer cabinet I/O point.

Def: **Control computer system:** A system consisting of at least one computer or processor with CPU processing and I/O capacity, one or several operator stations, and power supply incl. UPS units. The control computer system includes also common network, interface, and cabling for signal communication, and the HW/SW platform with the controllers containing e.g. the application specific control and guidance algorithms, and the monitoring functions.

Notes:

- The control computer system also includes control and management networks and interface used for integration with other control systems and decentralized management from several terminals. Serial connections are not considered part of the computer system, but instead typically included with the peripheral equipment they serve, e.g. a DGPS.
- The operator stations constitute the command and monitoring functionality of the control system, consisting usually of human-machine interfaces (HMIs), VDUs, alarm panels, joysticks, switches, printers, etc.

Def: **Automation system:** A *complex system* (DNV 2004, Pt.4 Ch.9) consisting of a stand-alone or several integrated control systems performing one or several specified autonomous functions related to control of one or several plant processes.

2.1. *System realizations*

A marine *Control System* is organized into *subsystems* and *components*, according to the hierarchy shown in Figure 1. It is physically coupled to the *plant*, i.e. the physical process to be controlled, through measurements by different sensors and/or actions provided by the actuation devices. Hence, it is further distinguished between:

- *Monitoring system*—designed with sensors integrated with operator stations having indicators and alarms for supervision of essential physical states and processes of the plant (open-loop control).
- *Command system*—designed with actuators that can be commanded from operator stations in order to manipulate the plant (open-loop control).

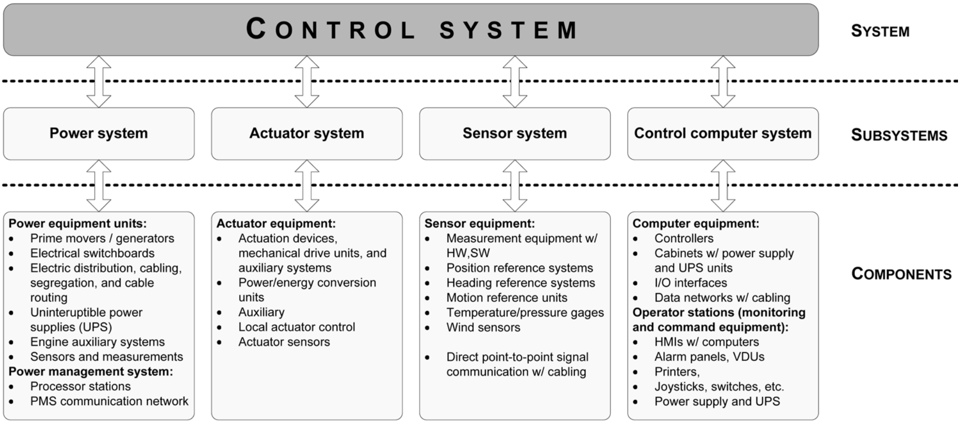
CONTROL SYSTEM
SYSTEM
Power system
Actuator system
Sensor system
Control computer system
SUBSYSTEMS
Power equipment units:
Prime movers / generators
Electrical switchboards
Electric distribution, cabling, segregation, and cable routing
Uninteruptible power supplies (UPS)
Engine auxiliary systems
Sensors and measurements
Power management system:
Processor stations
PMS communication network
Actuator equipment:
Actuation devices, mechanical drive units, and auxiliary systems
Power/energy conversion units
Auxiliary
Local actuator control
Actuator sensors
Sensor equipment:
Measurement equipment w/ HW,SW
Position reference systems
Heading reference systems
Motion reference units
Temperature/pressure gages
Wind sensors
Direct point-to-point signal communication w/ cabling
Computer equipment:
Controllers
Cabinets w/ power supply and UPS units
I/O interfaces
Data networks w/ cabling
Operator stations (monitoring and command equipment):
HMIs w/ computers
Alarm panels, VDUs
Printers,
Joysticks, switches, etc.
Power supply and UPS
COMPONENTS

Figure 1. Control system hierarchy

- *Feedback control system*—combination of a monitoring and command system through computer algorithms designed to perform autonomous control of the states of the plant according to a control objective. This is also called automatic control (closed-loop control).

Most marine control systems can be fitted into this structure. For instance, for a DP System according to IMO (1994), the Actuator system is called the Thruster system, the Control computer system is called the DP computer system, and the Sensor system consists of position reference systems and other sensors such as gyros, VRUs, and wind sensors.

A marine vessel consists usually of many control systems. Each of these may be stand-alone, or they may be integrated in a marine automation system as illustrated in Figure 2; see Rensvik *et al.* (2003). An automation system is the collection of, usually, several integrated control systems (e.g. electric power generation and distribution, propulsion systems, ballast systems, cranes, drilling, dynamic positioning, nautical systems, etc.) For example, the power system and the thruster system are integrated subsystems in a DP system, but have functions beyond DP; the power system must deliver power to all other consumers and the thruster system must also respond to commands from e.g. nautical systems.

The generic structure of a marine automation system, as shown in Figure 3, can be divided between *Real-time control and monitoring systems* and *Operational and Business enterprise management systems* (Sørensen & Ådnanes 2005). For the real-time control systems it is further distinguished between *high-level* control systems, such as e.g. a DP system, and *low-level* control systems such as local control of a variable speed drive.

A characteristic of a high-level control system is that it integrates many components, possibly with many low-level control systems built in, where each component by itself is well-tested to ensure high integrity. However, when the components are integrated into the high-level system, the overall integrity reduces with the result of increased failure rate; see Marine Cybernetics *et al.* (2004). This motivates improved test methodologies such as HIL simulation for testing such high-level integrated control systems.

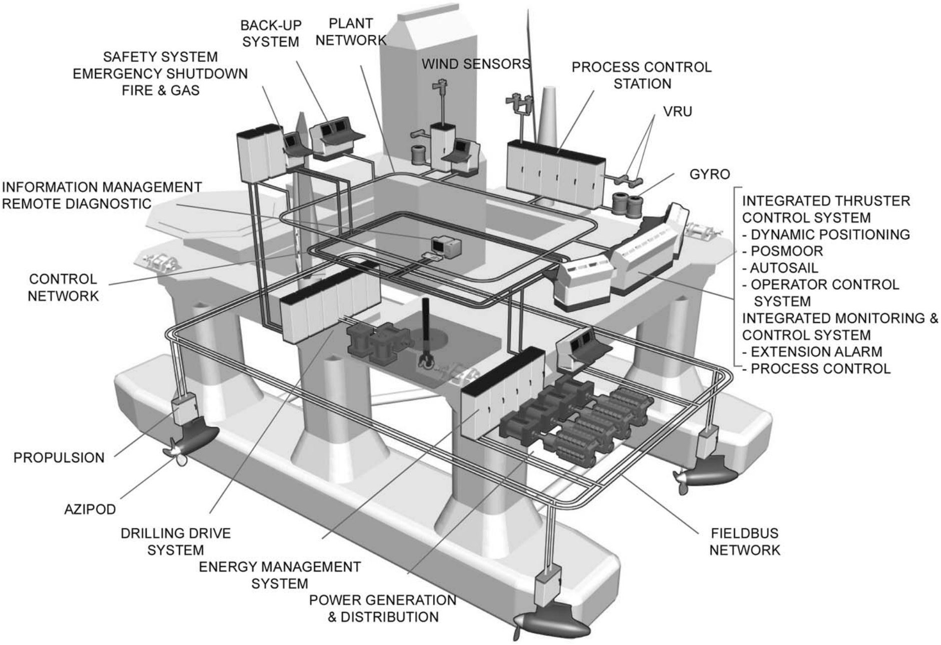

Figure 2. Integrated automation system in a semi-submersible (Courtesy: ABB)

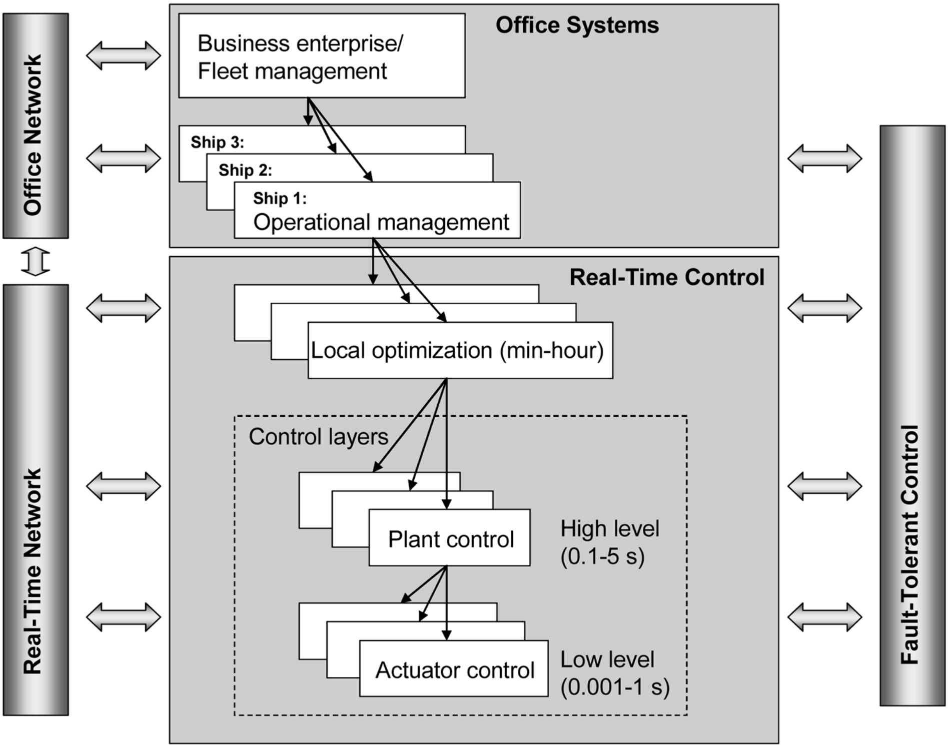

Figure 3. Marine management, control, and automation system (Courtesy: Sørensen & Ådnanes 2005)

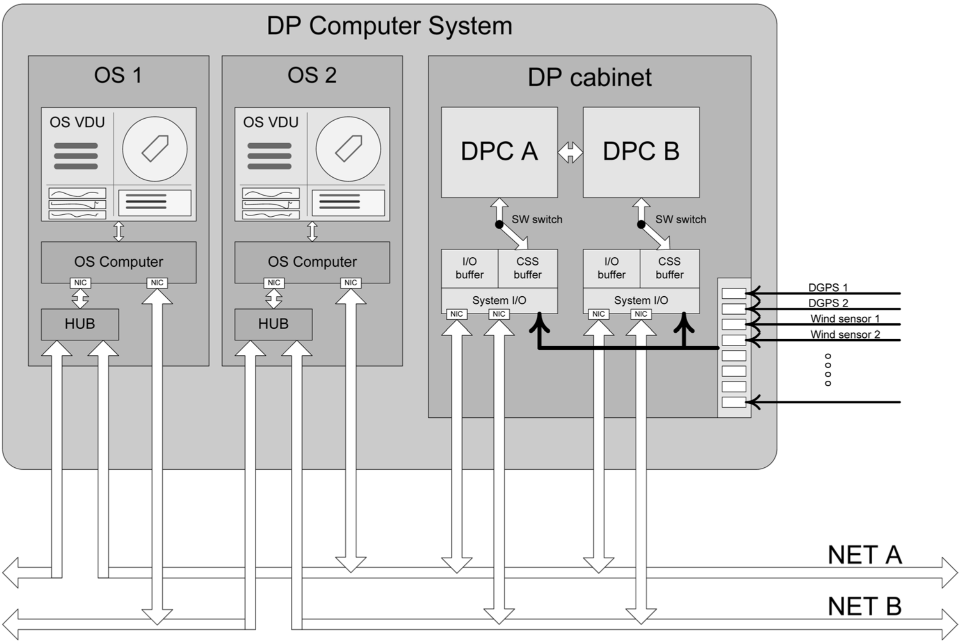

Figure 4. Example of a control computer system for DP

2.2. *The control computer system*

The control computer system performs all computations necessary to monitor and command the plant according to the control philosophy.

2.2.1. *Hardware/Software platform* The control computer system consists of a HW/SW platform with at least one controller or processor with CPU processing and I/O, instructed by *basic software* and *application software* (DNV 2004, Pt.4 Ch.9). Additionally, the control computer system consists of one or several operator stations with HMIs, alarms, switches, joysticks, etc., network, interface, and cabling for signal communication, and power supply including UPS units.

Figure 4 shows an example of a DP computer system with a cabinet containing two DP controllers (DPC A and B) and two operator stations. Each operator station is interfaced through Ethernet, while the cabinet also takes direct serial connections as inputs. Each controller has an I/O unit that converts both network and serial messages to the signal format required by the controller kernels.

2.2.2. *Functions of the control computer system* Associated with the control computer system there is a set of functions that implements the intended purpose or characteristic action of the system. The main functions correspond to the primary functional modes of the system, such as station-keeping for a DP system. Other functions may be safety related, e.g. to ensure system integrity, correct failure detection and handling, and fail safe actions with respect to system faults and limiting exogenous conditions (e.g. active redundancy).

Def: **Function:** (IEEE 1990) A defined objective or characteristic action of a system or component.

Def: **Safety function:** (IEC 1998). A function implemented by a safety-related system or component, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the control system, in respect of a specific hazardous event.

2.2.3. *Interfaces*

The different interfaces to a control computer system are the user interface, the signal interface (I/O), and often there are special test interfaces.

The user interface is realized by the operator stations and its visual display units, monitoring and alarm panels, keyboards, switches, and joysticks. Modern control systems often utilize several computer panels with many views and dialogues.

In addition to the regular user interfaces there may be specialized test interfaces in the form of software views and dialogues that are only accessible to a technician to give more in-depth information on the controller software processes.

The interface between the control computer system and the other subsystems is the signal I/O interface. This is usually spread out in the installation by several cabinets containing different equipment for processing the signals. The DP computer system shown in Figure 4 has its main signal interface through the network interface cards (NICs) for Net A and B and the interface for the serial connections. Figure 2, on the other hand, shows a larger system with more I/O points.

The signal I/O interface may also contain a specialized test interface for connecting a HIL simulator to the control computer system. This allows for a minimally invasive HW/SW testing of the control computer system since the real signal cables in the integrated control system do not have to be disconnected for testing to take place.

2.3. *The V-model for control system design, development, integration, and testing*

The V-model is central in the control system lifecycle. This is a work process model that relates specifications, SW and HW design and development, SW and HW integration, and testing at all levels in a new-building project.

As seen in Figure 5, the V-model divides each phase of the control system lifecycle into elementary activities and balances each specification and design activity (left-hand activities, top-down) with an adequate and targeted test and verification activity (right-hand activities, bottom-up). The main verification activities on the left-hand side are design reviews and different desktop analyses. At the bottom level, the actual product is built in different modules and further integrated bottom-up on the right-hand side. At each level of integration some form of testing, such as internal module and integration testing and in the end HIL testing and full-scale trials, is necessary to assure system integrity.

2.4. *Redundancy*

The most commonly used safety function in marine control systems is redundancy. It is usually required for marine control systems developed for safety-critical operations to be redundant with respect to any single failure in the system.

Def: **Redundancy:** (IEEE 1990). The presence of auxiliary components in a system to perform the same or similar functions as other elements for the purpose of preventing or recovering from failures.

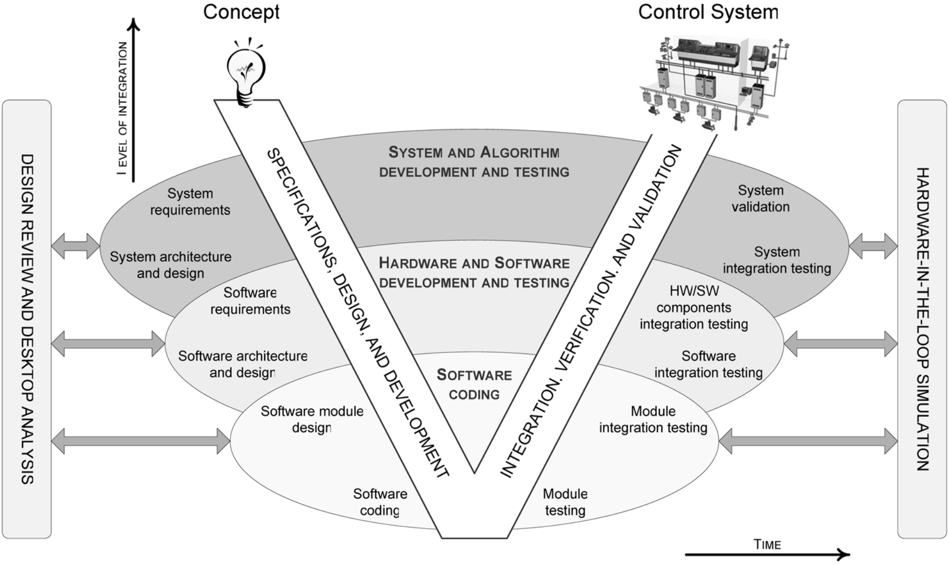
Concept
Control System
LEVEL OF INTEGRATION
DESIGN REVIEW AND DESKTOP ANALYSIS
HARDWARE-IN-THE-LOOP SIMULATION
SPECIFICATIONS, DESIGN, AND DEVELOPMENT
INTEGRATION, VERIFICATION, AND VALIDATION
SYSTEM AND ALGORITHM DEVELOPMENT AND TESTING
HARDWARE AND SOFTWARE DEVELOPMENT AND TESTING
SOFTWARE CODING
System requirements
System architecture and design
Software requirements
Software architecture and design
Software module design
Software coding
System validation
System integration testing
HW/SW components integration testing
Software integration testing
Module integration testing
Module testing
TIME

Figure 5. V-model for control system development and installation

Notes:

- *Active redundancy* (IEEE 1990) is the use of redundant elements operating simultaneously to prevent, or permit recovery from, failures.
- *Standby redundancy* (IEEE 1990) is the use of redundant elements that are left inoperative until a failure occurs in a primary element.

In a control system, redundancy is implemented in hardware by duplicating each hardware component and in software by failure handling mechanisms, i.e. decision making algorithms that based on received signal status flags, quality indicators, and measured failure symptoms in the hardware installation selects which hardware components to use at each instant of time.

Different selective functional barriers are usually implemented to detect and handle upon a failure as close up to the fault as possible. For instance, the first technical barrier is often the peripheral unit's own ability to perform self-diagnostics and detect internal failures. Typically, some form of quality indicator is transmitted to help decide to what degree the measurements or information sent by the unit can be trusted.

The second technical barrier is often found in the signal I/O interface of the receiving component. This typically checks for different communication failures such as open loop, short-circuit, checksum errors, etc.

The third technical barrier is often found inside the receiving component's kernel, where each signal is compared against an internal model and possibly compared to other signals received from redundant units. Methods for this are:

- *Voting*—requires at least 3 redundant components with measurements or indications of the same quantity. Two of the components are compared to the last. If there is a deviation then based on certain criteria the last is voted out.
- *Selection*—requires at least 2 redundant components with measurements or indications of the same quantity. Each measurement is compared to the mean or median

of all. If there is a discrepancy larger than some threshold, then the respective measurement is deselected. In the case of only two measurements, the operator must give priority to one of the components. The other component is then deselected in case of a large discrepancy.

- *Weighting*—requires at least 2 redundant components with measurements or indications of the same quantity. Based on calculations of signal-to-noise ratio, variance, etc., each measurement is at each sample given a relative weight that specifies how much that measurement is trusted.

2.5. *Safety fallback system*

A *safety fallback system* is a system, independent from the normally operationally control system, which in the event of a complete failure of the operational control system can, by manual or automatic means, bring the plant into a safe state.

For instance, the required safety fallback system with respect to a DP system is an independent joystick system facilitating direct manual control of the thrusters. For DP class 3 vessels (IMO 1994), there is an additional requirement for an independent backup DP system (DNV 2004, Pt.6 Ch.7).

2.6. *Signal communication*

Messages of information are sent between the different subsystems and components by signals of various types. In modern marine control systems, most signals are transmitted as data telegrams in computer networks. However, a single component such as a sensor will usually transmit its messages either as a digital signal in a serial line or as an analogue signal in an electric signal cable. These point-to-point connections are then interfaced either directly to an I/O point of the control computer cabinets or to the data network at a convenient location (also called *remote I/O*) and converted to data telegrams.

Signal communication must at different levels in the control system adhere to strict communication requirements with respect to real-time performance, noise and interference, and possibilities for different signal failures.

2.7. *Faults and failures*

A variety of faults and failures do happen in marine control systems. Classification rules typically require that the system shall be robust to any single failure. Safety mechanisms such as redundancy and different functional barriers are therefore built into the control system to detect and handle such failures.

Def: **Fault:** A defect in a system or component; e.g. a software bug or a short circuit in a component.

Def: **Failure:** (IEEE 1990). The inability of a system or component to perform its required functions within specified performance requirements. It is distinguished between the following failure conditions:

- *Intact* means there are no failures present in the system.
- *Single point failure* means that only one failure is present in the system, e.g.:
  - ○ any functional failure of a component,
  - ○ total failure of a vessel machine room, etc.

- *Single worst-case failure* is a system specific term describing the single failure that reduces the capability or function of the system the most.
- *Common mode failure* is a type of single point failure where seemingly independent components or subsystems enter failure modes due to a common failure point. Such failures can easily be mistaken for multiple failures.
- *Multiple failures* mean there are two or more independent failures simultaneously present in the system.

Def: **Failure Mode:** (IEEE 1990). The physical or functional manifestation of a failure. For example, a system in failure mode may be characterized by slow operation, incorrect outputs, or complete termination of execution.

Note: A function is normally related to a given system and the physical boundary of the system. The function is thus observed at the physical boundary of the system. A failure mode is observed at the physical boundary of the system and is related to the functional requirement of the system. A failure mode is therefore a type of deviation from the specified function to be carried out by the system.

Def: **Signal fault:** A defect in a signal medium or device, e.g. a short circuit in a network switch or a broken fiber cable.

Def: **Signal failure:** The inability or deteriorated ability of a signal to be communicated to the receiving components.

Def: **Signal failure mode:** The physical effect of a signal failure, categorized among:

- *Scaling error*—the true signal is scaled erroneously.
- *Wild point error*—wild-points are corrupting the true signal due to e.g. bad software, hardware, or interference.
- *Bias error*—the signal has a bias relative to the true signal.
- *Drift error*—the signal drifts off relative to the true signal, either by a stochastic process (Wiener process) or deterministically (ramp).
- *Noise error*—the true signal is corrupted by a large noise, e.g. Gaussian white noise or a 1st order Markov process.
- *Signal freeze*—the signal freezes at some value.
- *Signal@boundary*—the signal is fixed at a boundary of its physical range, e.g. at + 10V for an analog signal due to a broken signal wire.
- *Signal out-of-range*—the signal enters an invalid application value range.
- *Loss of signal*—the signal stops being communicated.
- *Flags*—signal integrity flags, status bits, quality indicators, etc., are set erroneously. Also message checksum errors.
- *Network message failures*—deteriorated transmission of signal messages, e.g. erroneous status bits, slow transmission rate, empty messages, network storm, etc.

2.7.1. *Fault, failure, and failure mode* A defect in a component is called a fault. This results in a failure of that component to perform at least one of its functions. This failure is manifested by a failure mode, i.e., a functional deviation observed on the boundary of the component.

The boundary can be output signals from the component, physical actions performed by the component, or information visualized in a user interface. A component in failure mode due to e.g. a software fault will in this respect be identified by a deviation from the functional requirements of the component.

For instance, a fault of a thruster on a DP vessel can be to lose one of its propeller blades. One failure is then the inability of the thruster to produce the specified thrust. The failure mode is that the thruster produces a reduced thrust force as compared to its setpoint.

If not handled properly, a component in failure mode may cause other components or subsystems, and eventually the overall control system to fail its function. Clearly, there may potentially occur a large number of faults in a marine control system. However, many faults cause the same failure, and many failures are manifested by the same failure mode. HIL testing should therefore test a control system with respect to a manageable set of relevant failure modes.

2.7.2. *Component failures* Many different failures can occur in a component in the marine control system. The resulting failure modes, however, will usually be specific and somewhat concrete within each subsystem of the marine control system.

Components for which one function is to transmit signals to another subsystem (e.g. a sensor) will have *signal failure modes*. Seen from the receiving subsystem, a signal failure mode is the effect of some fault in the transmitting component or in the transmission link.

Components with other functions than signal transmission (e.g. an actuator) will have inherent failure modes, such as e.g. the thruster failure described above.

Referring to Figure 1, the typical groups of failure modes on components within the different subsystems are given in Table 1.

Table 1. Typical failure modes within the different subsystems.

Subsystem:	Failure mode:
Power system	Loss of electrical power at one or several switchboards. Loss of power at one or several consumers. Reduced quality of electrical power (wrong frequency, wrong voltage, voltage surges). Signal failure modes on PMS monitoring and command signals.
Actuator system	Loss of actuation effort at one or several actuation devices. Deteriorated actuation effort (scaling, offset, unsteady, fixed at full, drifting, etc.) at one or several actuation devices. Signal failure modes on actuator sensors.
Sensor system	Signal failure modes on measurement signals.
Control computer system	Shutdown of controllers or processors. Loss of power to OS, network devices, etc. Loss of UPS. User interface errors (keyboard errors, joystick calibration, wrong alarms and warnings, errors in views and dialogues, etc.) Signal interface (I/O) errors. Network signal failure modes. Erroneous setpoints sent to actuator system (signal failure modes). Erroneous control signals sent to power system (signal failure modes).

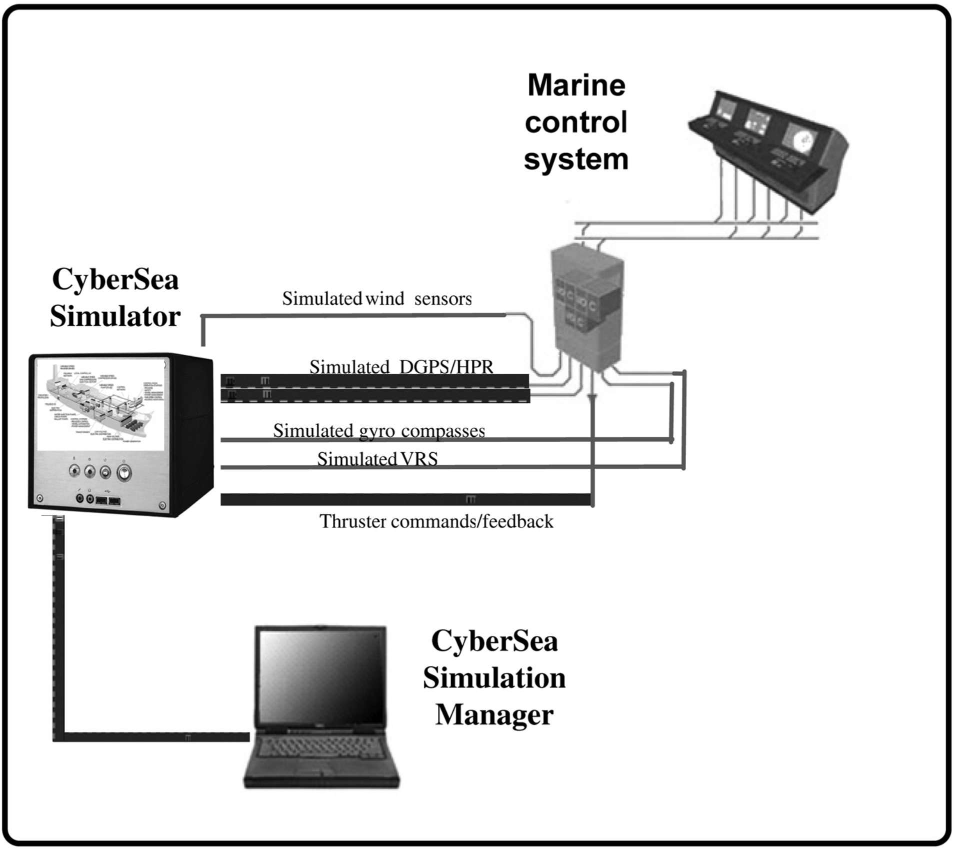

Figure 6. A HIL-Plant simulator interfaced with a marine control computer system to be targeted in testing.

3. HIL simulators

A HIL simulator operates in real time in closed-loop with the control computer system hardware and software and facilitates realistic and efficient testing of the control system functionality, performance, and failure handling functions.

Def: **HIL simulator:** A real-time simulator, constructed by hardware and software, that is configured for the control system under consideration, embedded in external hardware, and interfaced to the target system or component through appropriate I/O. During execution the target system or component will not experience any qualitative difference from being integrated to the real system.

Note: The HIL simulator will usually have a mathematical model of the specific plant and the environment modeled in software together with peripheral equipment modeled to a varying degree in hardware or software.

3.1. *Characterization*

There are different ways of characterizing a HIL simulator. One is the SW-to-HW ratio and one is the level of process modeling.

3.1.1. *SW-to-HW ratio* The SW-to-HW ratio quantifies how many of the components and subsystems of the target control system that is coded and simulated in the HIL SW versus the amount of HW kept in-the-loop. In one extreme, all subsystems of the control system including the control algorithms are implemented in SW, and the testing becomes a pure simulation study. Such a simulator is not HIL and does not need to run in real time. In the other extreme there is no SW implemented in a simulator, and the system must therefore be the actual control system. Any HIL closed-loop system is located somewhere between those two extremes.

3.1.2. *Level of modeling* A plant or component can be implemented in SW based on decision rules and logical switching, or it can be implemented based on accurate equations given by physical first principles such as Newtonian physics. This applies to all subsystems implemented in SW. E.g., an actuator may be modeled by accurate dynamical equations of motion representing its true behavior, or some simplifying static characteristic curves can be derived to approximate its dynamic behavior.

The most realistic behavior of the system is obtained by a high and accurate level of modeling. However, this will also require more know-how and a larger amount of parameters to be collected and configured into the simulator. A low level, on the other hand, requires usually less configuration parameters, but may yield a poorer representation of the real-time behavior of the system. In practice, the implementation of the different units will be a trade-off based on available configuration data and the know-how among the designers of the HIL simulator.

3.2. *HIL-Plant Simulator requirements*

3.2.1. *HIL simulator architecture* The simulator should simulate the dynamics of the plant, and the behavior of the control system hardware not included in the closed-loop (such as the power system, actuator system, and sensors). As a minimum, the target control computer, user interface, and communication links should be included in the closed-loop for testing. All components should be simulated in the time-domain in real time. The HIL simulator program must be embedded in a computer external to the control system being tested.

3.2.2. *Interfacing to the control computer system* The HIL simulator should be interfaced to the target control computer via its signal input/output (I/O), either through the normal hardware I/O interface (analog, digital, serial/NMEA protocol), the normal network protocol, or a dedicated HIL test I/O interface. The I/O interface should allow simulated sensor, actuator feedback, and power feedback signals to the control computer system to be transmitted, and all actuator command signals sent by the control computer system to be received by the simulator. It should be possible to verify which signals are interfaced. The communication delay in the interface should be less than 1/10 of the main sampling time in the control computer.

3.2.3. *Simulator functionality* The simulator should facilitate testability of the control computer system. This means that the simulator should be capable of simulating the necessary range of failures in equipment and signals according to a HIL test program. It should be an integrated system simulator where the interactions between the different equipment modules are correctly and accurately simulated. The simulator should allow the exogenous conditions (e.g. environmental conditions) to be defined.

3.2.4. *Failure modes* The simulator should be able to simulate the following general failures for all signals:

- Random signals: White noise, correlated noise (Markov process), random walk (Wiener process).
- Deterministic signals: Wild points, signal freeze, bias, drift, constant output independent of input, scale-factor error, flags and status bits.
- Signal communication (NMEA and vendor specified serial or network protocols): Erroneous rate of transmission, checksum errors, and empty fields.
- Power failures: Simulated failures in a UPS or low-voltage power system module should cause a simulated loss of power of the units connected to the module.

3.2.5. *Simulator accuracy* The plant and equipment should be modeled (or represented) to sufficient accuracy in order to give realistic interaction with the target control computer and accurate predictions of performance within the full expected operating envelope. The simulator should be configured with the parameters and properties of the particular plant, power system, actuator system, sensor system, and control computer system hardware. The time step in the numerical integration solver should be less than 1/10 of the normal sampling time in the control computer.

3.2.6. *Monitoring, data logging and test scenario scheduling* The simulator should have capabilities for data logging and real-time presentation of simulation results, such as trend plots and statistical properties. Deterministic (repeatable) simulations of pre-determined simulation scenarios should be possible. The purpose and implementation of each test should be presented in a clear manner in the simulator user interface such that test completion and test result can be witnessed and verified in a transparent manner. The simulator should contain internal quality monitoring in order to automatically detect and report when internal sub-models operate outside their validity range.

3.2.7. *HIL testing* The HIL-Plant simulator should have the capability to test the primary target system with at least the following test cases:

- All relevant functional modes and features.
- A sufficiently large set of single failures in the control system.
- Relevant common mode failures—to analyze the dependability between components and subsystems such as e.g. interaction between different sensors.
- Relevant multiple failures.
- Reconstruction of relevant reported incidents.

4. HIL testing

In testing of marine systems, it is distinguished between *verification* activities and *validation* activities. While verification is to test compliance of the system to the requirements, validation will additionally question the correctness and feasibility of the requirements with respect to philosophy and intended use, rules and regulations, societal norms, etc.

The objective in HIL testing is to test the target system with respect to the operational and safety functions and verify conformance to the functional and safety requirements. The following definitions apply:

Def: **Verification:** (ISO 2000) Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Def: **Validation:** (ISO 2000) Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Note: The acceptance criteria are set by the system philosophy, regulatory requirements, societal norms, common sense, and good practice.

Def: **HIL testing:** Verifying the required functions of a hardware/software system or component by interfacing it to a HIL simulator and executing the functions for the integrated system.

Def: **Test application:** The Control system to be tested.

Def: **Primary target system:** The system, subsystem, or component within the Control system that is primarily targeted in the testing activity.

Note: For instance, when the test application is the DP system, the primary target for HIL testing is usually the DP computer system.

Def: **Secondary target system:** Other part of the control system, besides the primary target, which is being tested indirectly during testing of the primary target.

Note: For instance, when primarily testing the control computer system on sea trial with the other subsystems such as power, actuators, and sensors in the loop, then obvious flaws in these subsystems would most likely be discovered indirectly.

Def: **Functional testing:** To test a function of a target system and verify compliance to the specified functional requirements. The main objective is to eliminate failures occurring in implementation, integration, and configuration.

Def: **Performance testing:** To test and quantify the level of performance of a function of a target system under feasible conditions within specified working capacity. This includes verifying that:

- The performance under all normal operations satisfies the specified performance requirements.
- The capability in all specified feasible conditions, normal and extreme, is sufficient to meet the performance requirements.

Def: **Failure testing:** A type of functional testing that targets the safety functions of a system to verify compliance to the specified requirements for failure handling mechanisms. This is mainly done by inducing relevant failures in the system, either simulated or real, and observing and reporting the effects of these failures on the behavior and safety of the target system.

Def: **Signal FMEA testing:** To impose relevant signal failure modes on the communicated signals from subsystems or components in a control system and verify that the failure handling mechanisms in the control system satisfy the requirements (a type of failure testing).

Def: **Testability:** The extent to which a test objective and feasible test can be designed to determine whether a requirement is met. Testability of a function of a system or component requires controllability and observability of that function:

- **Controllability:** A function of a system is controllable if for each possible behavior of the function, i.e. each possible output data value, condition, or state, there exists a set of actions that can be applied to the inputs of the system such that the corresponding behavior is obtained.
- **Observability:** A function of a system is observable if any arbitrary behavior of the function can be determined from the outputs of the system.

A system or component is said to be testable if all functions of the system or component are testable. The applicable inputs and outputs are the user interface, the signal I/O interface, and dedicated test interfaces.

Def: **New-building phase:** Also called the manufacturing phase. The vessel manufacturing period at the yard in a vessel lifecycle, starting with contract award and ending with CAT and hand-over to the vessel owner.

Def: **Operational phase:** Also called the *sailing phase* or *Vessel-in-Operation*. The operational period in the vessel lifecycle, starting with CAT and ending with decommissioning and disposal.

Def: **Failure Mode and Effect Analysis (FMEA):** (US Dept. of Defense 1980), (IMCA 2002) A systematic process for identifying potential design and process failures before they occur, with the intent to eliminate them or minimize the risk associated with them.

Def: **Factory Acceptance Test (FAT):** The aim of the FAT is to verify the conformance of the control computer system to its functional requirements, after manufacture and configuration at the vendor factory and before installation in the vessel. The test is performed by use of a FAT test program that surveys all required functions of the integrated HW/SW system.

Note: Many of the involved tests are performed without closing the loop with the plant dynamics; typically logical tests of display views and menus. However, some form of closed-loop simulation is usually necessary to test the full function and performance of the control system at the vendor factory.

Def: **Customer Acceptance Test (CAT):** The aim of the CAT is to verify the compliance of the fully installed control system to its functional requirements and to validate it with respect to the intended use and regulatory requirements. Successful validation results in a class certificate as part of the overall ship classification and hand-over to ship owner.

4.1. *What to test*

HIL testing targets the required functions of the primary target system. All functions corresponding to the main operational modes should be verified and possibly quantified with respect to performance. In a safety-related system, all safety functions should be thoroughly tested by simulating failure modes in the system.

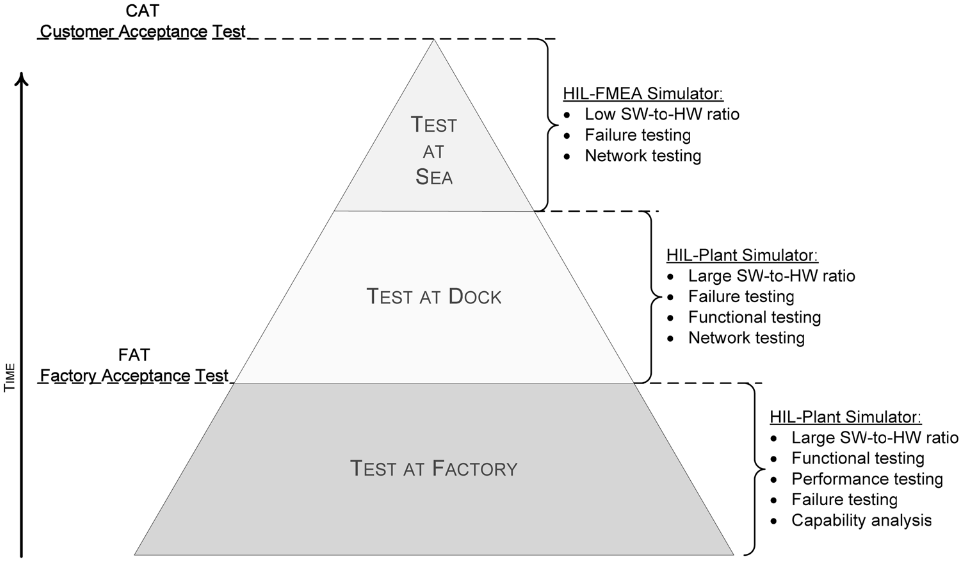

Figure 7. Scope of testing for HIL certification in a new-building project.

4.2. *HIL test scope*

Verification and validation of a marine control system by HIL testing require a *HIL simulator* and a HIL *test program*. The HIL test program must identify the test application and the primary and possible secondary target systems and specify all test cases to be executed in a given test activity.

In a HIL test activity one defines the test application to be the control system under consideration, such as e.g. a DP system. This control system is realized by subsystems and components as in Figure 7, where the primary target system is usually the Control Computer System.

The HIL test program details all test cases with sufficient test coverage. In a HIL test project there must additionally be an overall HIL test plan that gives a schedule of test activities and considers managerial and administrative issues. An important part of the HIL test plan is a *safe job analysis* for each test activity to reduce any unnecessary risk to personnel, equipment, and the environment during testing. For a new-building project, the test activities will normally be divided among testing at vendor factory, at yard, and on sea trials. For a vessel in operation, the test activities may be divided among testing at dock, in transit, or at sea trials.

As indicated in Figure 7, the time consuming part of the overall test scope should be at TaF and TaD, where time constraints are normally more relaxed than at sea trials. Testing at factory and dock requires a HIL-Plant simulator where most of the plant (sensors, actuators and machinery, vessel dynamics, etc.) is modeled in the HIL software. This facilitates an extensive program for testing most of the functions in the target control system. These tests should in addition to some new tests form the basis for testing at sea trials.

4.3. *Testability*

HIL testing is a type of black-box testing where the inputs to the black-box system are manipulated and the outputs are observed and verified against requirements for intended use, e.g. through visual display units, alarm/warning messaging, or signals received by the simulator.

In order to adequately verify a function of the black-box system, the function must be testable. Testability is defined as controllability and observability of the function. In simple terms, controllability means that the function can somehow be reached and manipulated from the inputs of the black-box, and observability means that the behavior (effects and responses) of the function can somehow be determined from the outputs of the black-box.

It follows that *each function that is required to be tested must be testable.*

For instance, the main operational function in a DP computer system is to ensure station-keeping of the vessel. To manage this for a certain set of allowable environmental conditions, the DP computer system needs as input a set of measurements such as position, heading, wind speed and direction, and so forth, and some operator commands. The corresponding outputs are a set of command signals sent to the thrusters and visualizations of station-keeping status in the operator stations. Controllability of station-keeping is the ability to provide the necessary inputs (signals and operator commands) for station-keeping to occur. Observability is the ability to verify from the outputs (signals and visualizations) that correct station-keeping actually happens. There are only two ways of verifying this; either by integrating the DP computer system in a real DP vessel and performing station-keeping on sea trial, or by interfacing the DP computer system to a configured HIL simulator.

4.4. *Types of testing*

It is distinguished between functional and performance testing. While functional testing verifies that the functions of a target system fulfill the requirements, performance testing quantifies the level of performance when executing them.

A type of functional testing is failure testing where the main emphasis is to test the failure detection and failure handling functions of the target system.

Only the primary target system is extensively tested by using a HIL simulator. However, in one extreme type of HIL testing called *signal FMEA testing*, the real control system is fully integrated together with a HIL simulator in the loop. This is the version of HIL testing that contains the most hardware in the loop, and it will therefore indirectly test also the other subsystems in the control system, such as the power system, the actuator system, and the sensor system. These are then called secondary target systems.

4.4.1. *Functional testing* The aim of functional testing is to verify the functions of the primary target system to reveal flaws from the specification and design phases, and to discover failures occurred during implementation and the integration of software and hardware.

Functional testing is performed using a HIL simulator interfaced to the primary target system and executing the specified functions. The resulting behaviors are compared to functional requirements. If unacceptable behavior is observed, a test deviation form is filled out.

4.4.2. *Performance testing* Performance testing is concerned with how well the control system behaves in different functional modes when exposed to different exogenous conditions. The aim of performance testing is further to ensure that the working capacity of the system is sufficient to meet the specified requirements. Such tests give a quantitative answer to the ability of the primary target system to perform its different functions and the cost of operation in different exogenous conditions.

4.4.3. *Failure testing* Failure testing is to simulate failures in the control system to trigger the corresponding safety mechanisms for failure detection and failure handling in the primary target system and reporting their success in reducing the risk of failure in the overall control system.

To perform failure testing, a control system breakdown into subsystems and components is done, and the respective failure modes of the components are identified. The failure detection and handling functions are then extensively tested by effectuating or simulating these failure modes in the system.

Failure testing will therefore give an answer to the ability of the primary target system, perhaps in combination with a human operator, to avoid failures when exposed to equipment malfunctions and fault scenarios of different types. Failure testing is thus concerned with robustness of safe operation and availability of the control system in the event of failures. Mostly single failures are considered, but an extended test scope will also consider several scenarios for common mode failures and multiple failures.

5. Conclusion

In this paper we have discussed a framework for HIL testing of marine control systems, treating control system terminology, functions and failures, characterizations and requirements for HIL simulators, and the task of HIL testing.

HIL testing of a marine control system requires a configured HIL simulator and a HIL test program. The HIL simulator must have sufficient function and accuracy as well as options for interfacing. Standard interfaces are, in this context, an advantage. The HIL test program will contain all test cases. To construct the test cases, a list of all functions of the control computer system must be available, and a break-down of the control system into subsystems and components is necessary in order to identify all relevant failure modes in the system. Functional testing targets all relevant functional modes of the control computer system as well as the safety functions by testing w.r.t. a manageable set of simulated failure modes. Performance testing targets the efficiency of executing the main functional modes.

Through a set of definitions, a vocabulary has been established for use in the on-going development of HIL testing for marine control systems (Marine Cybernetics 2006).

References

DNV (2004). “Rules for classification of Ships/High speed, light craft and Naval surface craft,” Høvik, Norway, January 2004.

ISO (2000). “Quality Management Systems—Fundamentals and vocabulary,” Int. standard ISO 9000 : 2000(E).

IEC (1998). “Functional safety of electrical/electronic/programmable electronic safety-related systems,” Int. standard IEC 61508.

IMO (1994). “Guidelines for Vessels with Dynamic Positioning Systems,” Maritime Safety Committee (MSC) Circular 645, June 1994.

IPG Automotive (2005). http://www.ipg.de/44.html, Internet, visited 2005–07–24.

Marine Cybernetics *et al*. (2004). “Computer-based systems on ships and offshore vessels: The Software Problem + + ,” 2004–10–27.

Marine Cybernetics (2006). http://www.marinecybernetics.com, Internet, visited 2006–01–30.

Rensvik, E., Sørensen, A. J. & Rasmussen, M. (2003). "Maritime Industrial IT," Proc. 9th Int. conf. Marine Engineering Systems (ICMES), Helsinki, Finland, May 2003.

Sørensen, A. J. & Ådnanes, A. K. (2005). "Reconfigurable Marine Control Systems and Electrical Propulsion Systems for Ships," Proc. ASNE Symp. on Reconfiguration and Survivability, Florida, USA, Feb. 2005.

Skjetne, R. (2005). "The Maneuvering Problem," PhD thesis, Norwegian Univ. Science and Technology, Dept. Eng. Cybernetics, Trondheim, Norway, 2005–03–15.

IEEE (1990). "IEEE Standard Glossary of Software Engineering Terminology," IEEE Std. 610.12–1990, Sept. 1990.

IMCA (2002). "Guidance on Failure Modes & Effects Analyses (FMEAs)," report IMCA M 166, April, 2002.

US Dept. of Defense (1980). "Procedures for performing a failure mode, effects and criticality analysis," Military Standard MIL-STD-1629A, Washington DC, USA, Nov. 1980.