In the Loop

System verification evolution.

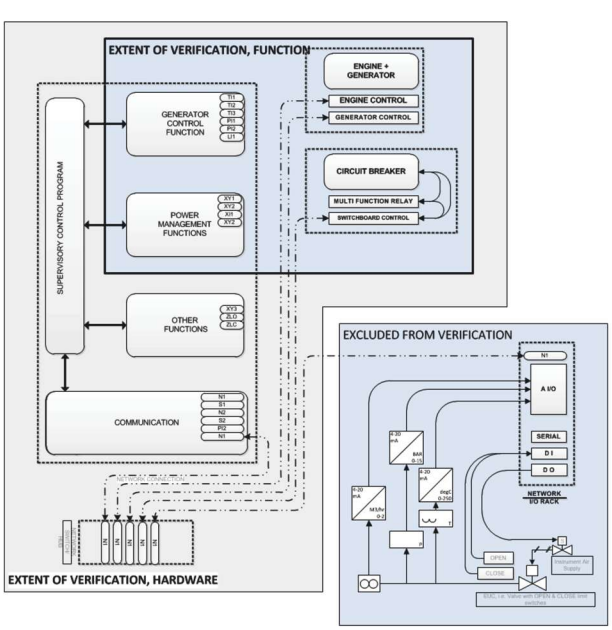
by Mr. Milton Korn
Managing Senior Principal Engineer
American Bureau of Shipping

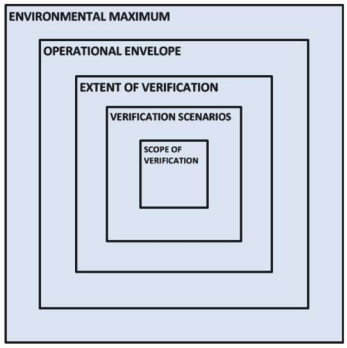
Even a cursory glance at marine casualty lists shows that the root cause of a disturbingly high number of vessel casualties is system failure. In July 2012, the American Bureau of Shipping published a guide for system verification including "hardware in the loop" (HIL) testing, as part of its mission to safeguard life by minimizing system failure.

Verifying System Integrity

Stakeholders use system verification to affirm their shipboard equipment and systems operation are in accordance with appropriate specifications and functional descriptions, which provide a structured method to develop, manage, and implement a test scope for verifying system performance throughout the system life cycle. Implicit in the concept is the recognition that although a system has been verified, the test scope may need to be updated as that system changes. Therefore, a simple "snapshot" of system performance at a particular instant is of limited value.

An additional benefit from system verification is the ability to ascertain that system functionality is as intended, but, perhaps the specification is wrong. As the system is being verified, any system operation that is not in accordance with the functional description or that is not intended is identified as a defect. To verify operation and to identify as many defects as possible, the equipment and systems are tested in accordance with a relevant and appropriate test scope contained within a verification plan.





The test scope is developed from functional descriptions including systems analysis such as:

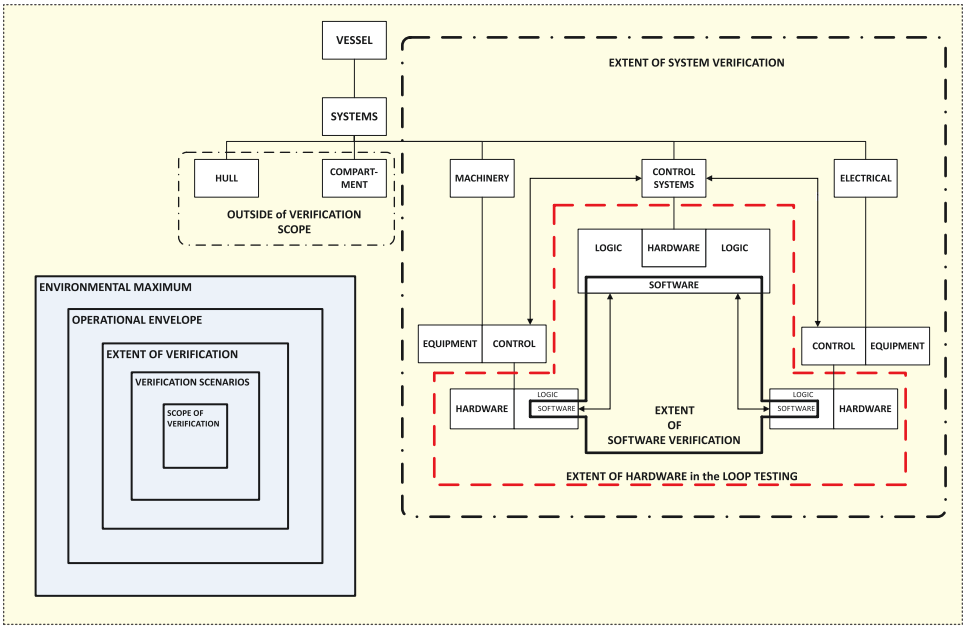
- failure mode effect and criticality analysis,
- fault tree analysis,
- safety analysis.

The Art of System Verification

System verification includes developing a test scope that provides a venue appropriate to the point in the system life cycle at which testing will occur and applying reasonable and relevant tests that fit into the constraints of time, resources, and effort. It is best to follow a structured approach to select tests that are appropriate and

The scope of the system verification notation assigned to a vessel, offshore installation, or facility is defined by the verification process completed in accordance with the ABS-reviewed verification plan. The notation applies only to the hardware, firmware, and functions of the target system and equipment under control that are included in the verification plan. All graphics courtesy of the American Bureau of Shipping.

relevant to the verification goals and justify exclusion of other tests. For example, a verification scope that cannot be completed in the time available or in which the perceived benefit is less than the cost of development and execution, is of little value.



System verification extends classification to provide a higher degree of confidence that the systems are capable of and do function in a planned and specified fashion under a variety of states.

System verification is also complicated by the need to manage expectations and changes throughout the life cycle. Those new to system verification may have unwarranted confidence in systems that have been verified, mistakenly believing that it is possible to identify all defects. This is simply not possible, especially with a test scope constrained by time, cost, and venue. It is anticipated that equipment and systems will be tested during development and construction prior to installation, during commissioning, and periodically throughout the system life cycle as warranted by time, change, or casualty. However, aspects of equipment and system functionality and the risk of damage and personal injury can constrain the extent of feasible onboard testing. These constraints are problematic, especially after change is introduced into a deployed system.

To achieve the full value, the stakeholder commitment must be for the lifetime of the equipment and systems. Without this commitment, system performance can only be verified at a particular instant and with only a specific system hardware, logic, firmware, and software configuration. Change introduced to a previously verified system could necessitate additional testing, which must be performed in accordance with an updated test scope to identify new defects. Uncontrolled change can effectively negate system verification benefits.

Introducing Guidelines

The ABS System Verification Guide provides direction to define and develop a meaningful testing scope that identifies and remediates as many defects as possible prior to system deployment. Defect remediation prior to deployment is less costly than remediation in service when the total cost of remediation can include the consequential cost of damage to equipment, the environment, personal injury, or even death.

The system verification notation can be assigned to a specific vessel or facility for specified equipment or systems that have been verified in accordance with guide requirements. To that end, the guide recognizes three system verification methods:

- hardware in the loop,
- software in the loop,
- system state estimation.

Additionally, the guide recognizes that a combination of these techniques may be a more appropriate and practical approach.

Control Systems

Many modern control systems—especially those with a large input and output (I/O) count and/or great dispersion throughout a vessel or facility—connect processors to I/O via a communication network. Some control systems use a single communication network for all input/output and control functions, while others use multiple networks. A typical installation can have remote data-gathering cabinets distributed throughout a vessel connected to the processors via a communication network; input and output local to the data-gathering cabinets are typically hard-wired to them.

There are variants of this scenario where in some implementations, input/output is directly connected to the communication network and others, such as those used for navigation or dynamic positioning, where a second communication network can be used. The National Marine Electronic Association bus, for example, is especially configured for communication among navigational instruments such as GPS, radar, compass, and wind speed.

Modern control systems also include error-checking and annunciation capabilities, which typically allow for diagnostic and error identification at the rack and card level and can extend down to the I/O level, where individual loops can be checked for open, short, ground, and such. They can also be used to perform transducer and measuring instrument diagnosis and calibration.

Control Systems Redundancy

One aspect of modern control systems is the level of redundancy built into the system to facilitate continuous operation in the event of a single failure. Examples include dual communication networks, master/slave processor relationships, voting processor relationships, and multiple power supplies. In practical terms, this means that for systems using a single communication network, the network is duplicated, and the two networks operate in parallel. Should one network fail, it is assumed that the other will continue to operate.

Because it is difficult to "separate" redundant parts during system verification, redundancy introduces challenges and complexities, especially when verification testing is to be performed on the installed hardware of an operating control system.

Common Mode Failure

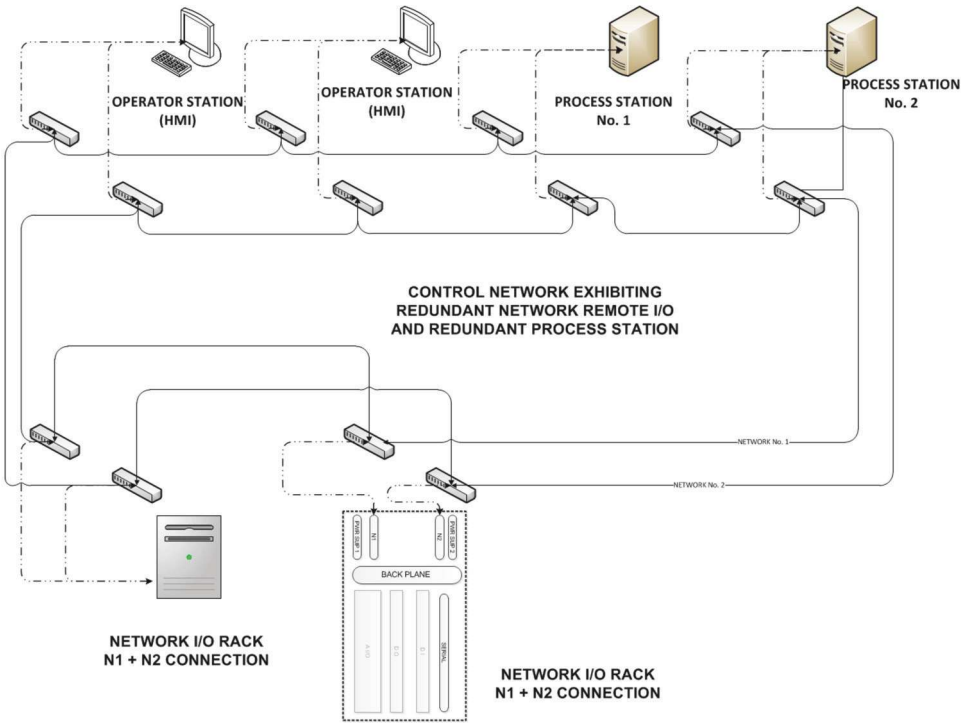
A common element that is without redundancy is the logic, including software. This commonality can prove to be an Achilles heel for the control system. If the master and slave processor are running the same software and a software defect disables the master processor, it simultaneously disables the slave processor. Similar issues exist regarding the data communication networks.

Hardware in the Loop

Hardware in the loop or HIL testing is the result of 30 years' worth of technological evolution; it allows simulations to connect to and interact with the real world. HIL testing consists of connecting equipment under test to a simulation of another collection of hardware and performing a series of tests that verify key functionalities. Before this type of testing, simulation, consisting of models and logic developed from functional descriptions, were executed on the simulator hardware. Early simulations had limited facility to connect to and interact with the world outside and rarely occurred in real time.

These early efforts were the precursors of what now is called software in the loop (SIL) testing, so with the introduction of HIL testing, the art has developed into two distinct branches:

- power hardware in the loop,
- control hardware in the loop.



If redundant or parallel processors or automatic control systems are fitted, it is recommended that the redundant automatic control systems be independent, self-monitoring, and arranged such that, should one fail, control is automatically transferred to a non-failed automatic control system.

In its purest form, hardware in the loop testing uses the actual hardware deployed aboard the vessel or facility and the actual logic, some of which is implemented in software. Verification testing is then tied to the real-time characteristics of the actual hardware, firmware, software, and interfaces—which means that there is limited ability to accelerate the control system speed to shorten the testing process. The logic is loaded into and operates on the actual hardware. HIL testing provides the opportunity to identify logic defects as well as defects that are coupled to the control system hardware and firmware.

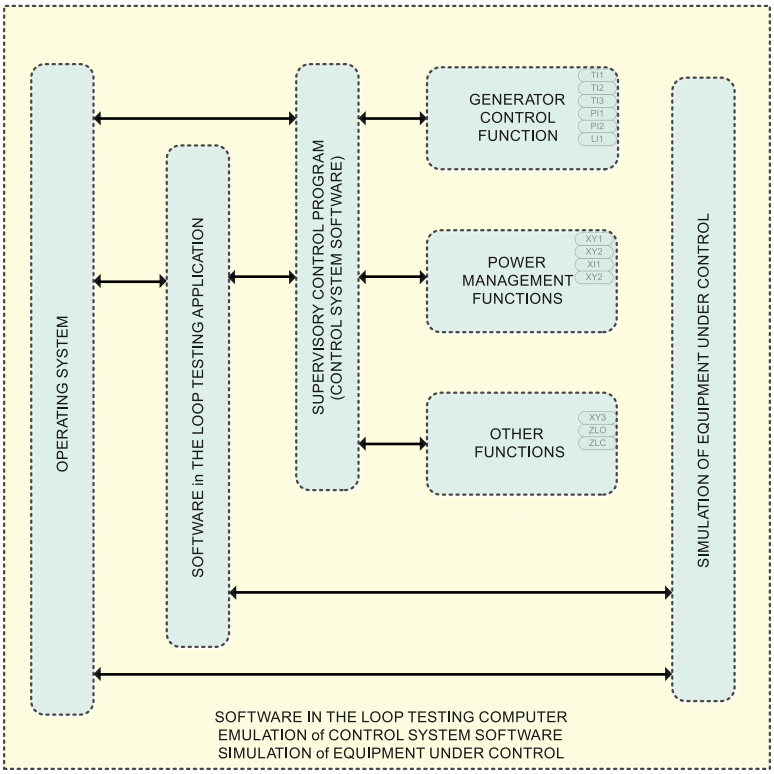
In practice, it is nearly impossible to meet this criteria, which is the actual logic (including software) running on the actual hardware. Reasons for this include the challenge of bringing the actual hardware together; the inability to connect the actual hardware; and, for

the case of onboard testing, the difficulties associated with HIL testing, interfering with onboard operations and concerns about equipment damage or personal injury.

Some stakeholders address these challenges by building laboratories where "identical" hardware has been set up for verification testing. Some labs even duplicate the interconnecting communication networks. This arrangement allows for software verification on hardware prior to deployment.

Software in the Loop

SIL testing consists of loading control system models, logic, and software onto an emulation of the control system hardware on which the logic and software are intended to operate, coupling the emulation to a simulation of the equipment under control, and executing a test scope to verify the software. Software in the loop can be performed using a single computer that acts as the emulation and simulation host, or multiple computers. In all cases, users must implement an appropriate interface between the emulation and simulation.



Software in the loop can be performed using a single computer acting as the host for the emulation and simulation.

In the case of a single computer, the interface is often implemented in software, while in the case of multiple computers, other means would be required. Also, SIL testing can take place at much greater speeds than HIL testing, because the software is decoupled from physical time constraints or characteristics. SIL testing is a variant of simulation.

One of the major issues with SIL testing is how and where to connect the simulation to the system to be verified. For a system where the input/output is connected to data-gathering cabinets that are distributed throughout the vessel, one possibility is to distribute the simulation throughout the vessel and connect at the data-gathering cabinets. This approach is not likely in a large or distributed system due to the difficulty of distributing and synchronizing the simulation. An alternative is to connect the simulation to the communication network(s) or use the network connection of the control system. A connection such as this does not include the remote I/O data-gathering cabinets in the verification, so this exclusion has to be evaluated.

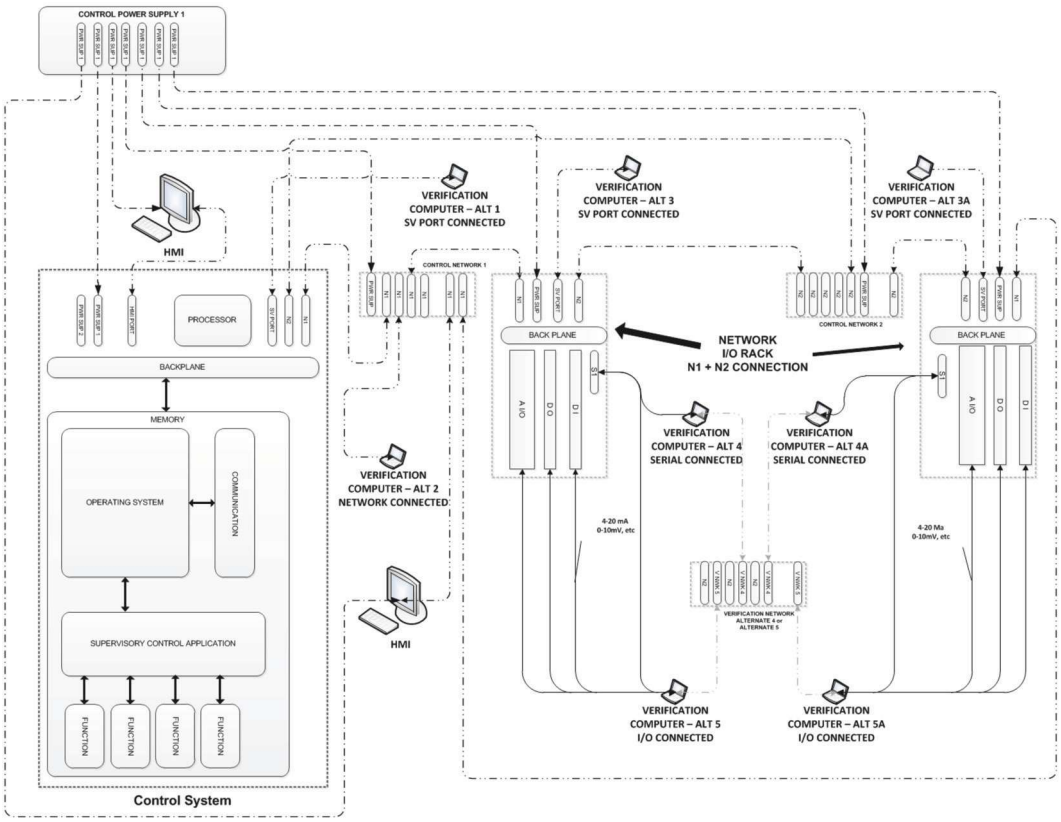
A third option is to use a dedicated communication port built into the control system. This kind of connection does not include the communication networks and adds a layer of complexity, as there needs to be some switching method implemented in hardware or software to direct the control system to look at the verification port, as opposed to the normal connection for I/O.

An additional complexity for these last two scenarios is that often diagnostic and error-checking functions are built into the control system and are operating in the background in some combination of hardware and software. With the control system operating, the I/O loops are not connected, so the diagnostic and error-checking functions can generate a large number of errors or alarms that must be managed throughout the verification testing procedure.

Applications, Challenges, and Results

In preparation to develop a test scope, it is important to know what is proposed to be verified. Is it only logic, including software, or does it also include the coupling of the logic to the hardware? If the only interest is in software verification, SIL testing alone could be appropriate. If there is interest in knowing how hardware and firmware influence system performance, SIL testing alone may not be adequate, and HIL testing could be the vehicle for verifying logic on hardware. The significance of differences between the verification hardware and installed hardware are not fully understood or quantifiable.

Onboard control system and software testing (either as part of the initial deployment/ commissioning or as part of the management of a proposed change) is especially challenging if the equipment installed onboard the vessel or facility is in operation. A major challenge is to



Guidance to identify and remediate as many defects as possible prior to system deployment.

decouple the control system from the operating equipment to perform verification testing, while maintaining effective equipment operation and supervision.

An instance of a control system failure illustrates the potential system verification application. For example, imagine that, upon the conclusion of a port stay, a vessel was making preparations to get underway. It was not able to transfer propulsion remote control to the bridge, because two mechanical contacts from adjacent mechanical indicator pushbuttons were simultaneously closed. One button was for port wing control, the other for central console control. This occurrence of mutually exclusive events prevented the use of propulsion remote control. There was no physical manifestation that the vessel technical team could see, and the control system did not have the ability to identify the error.

A test scope prepared in accordance with system verification guide requirements would have considered the occurrence of mutually exclusive events and included verification tests for this potential situation. Logic that would not recognize this occurrence would have been identified, and the logic could have been updated to address this error.

Enhancing System Reliability

The nature of system development, installation, and deployment makes it highly unlikely that a single verification technique will be appropriate at each stage of the system life cycle. System verification lets the user identify and remediate defects prior to system deployment and manage change throughout the system life cycle using a variety of techniques that, when implemented in a coordinated fashion with an appropriate test scope, offer the opportunity to enhance system reliability in a timely and cost-effective manner.

About the author:
Mr. Milton Korn is a managing senior principal engineer at ABS. He is also an assistant professor of electrical engineering at the United States Merchant Marine Academy, in Kings Point, N.Y. He holds a chief engineer's license with Standards of Training, Certification, and Watchkeeping endorsement and is a registered professional engineer in New York and New Jersey.