Yards and vendors must act promptly to comply with upcoming IACS cyber security requirements

From aware to ready

by Jarle Coll Blomhoff, *Group Leader Cyber Safety & Security, Control & Bridge Systems – Ship Classification Maritime, DNV*

The International Association of Classification Societies' (IACS) unified requirements (URs) for cyber security – due to come into force on 1 January 2024 – herald a shake-up for the supply industry. They will require the full spectrum of critical onboard control and navigation systems to comply.

New technology and increasing automation and digitalisation are combining to streamline the efficiency of the maritime industry. But along with the increasing number of integrated vessels featuring multiple interconnected systems comes the threat of remote attacks that can potentially gain access to or impact critical onboard control systems.

Optimal cyber security needs to be in place to ensure vessels remain in operation and to safeguard the safety of the crew, passengers, assets, and the environment.

It is critical to implement optimal preventative measures against cyber attacks

Shipping is the backbone of global trade, and the potential disruption that attacks could cause, not to mention the danger to life and property, is a clear temptation for cyber criminals and state-sponsored hackers. It is imperative to protect both corporate infrastructure and individual ships amid increasingly high vessel connectivity. Most people are aware of the risks; the focus is now on implementing optimal preventative measures.

While corporate IT systems are considered 'mature' with a lot of attack surfaces, attacks are still most likely to have a financial impact on a company rather than directly on vessel operations (low-consequence). However, operational technology (OT) on board a ship or offshore mobile asset is increasingly connected to shore-based IT systems, providing a potential 'back door' for attackers. Cyber security must protect this low-maturity, high-consequence digital infrastructure so that a ship can stay safe and moving despite being attacked. You can't risk losing the main engines or any other system considered essential and important under SOLAS rules.

New IACS unified requirements focus on cyber risks of on-board systems

While regulations like the International Maritime Organization's cyber resolution from 2021 require owners, operators, and managers to consider overall cyber risks, there are no concrete requirements at the systems level. However, this is now changing, as IACS just published new URs that will oblige both yards as system integrators and system vendors to build cyber security barriers into their systems and vessels.

The URs will apply to everything computer-based on-board such as main-engine control systems, steering, cooling systems, fire detection, communications systems (including public address systems), and navigation systems – basically, anything that is integral to making the ship move, navigate, and operate safely.

Our team is also working on autonomous shipping, where class qualification of autonomous pilot tools such as object detection will also be very important. Any kind of decision-support system that provides critical navigation advice to the captain and contributes directly to steering the vessel will also be subject to the URs in future.

The URs will apply to all newbuilds contracted after 1 January 2024 and will also serve as non-mandatory guidance for existing ships as well as new vessels contracted before that date.

DNV is ready to apply IACS-compliant cyber secure rules to newbuilds

The URs are minimum prescriptive requirements agreed by all IACS members. Any class society appointed to oversee a newbuild naturally deals with the shipowner and the yard, but from that date they will also need to check that all vendor systems meet the requirements. How individual class societies implement the URs can vary, but for DNV-classed vessels our organisation is ready now to apply its existing IACS-compliant Cyber Secure rules to existing vessels and current newbuilds, as well as work closely with system suppliers to support a smooth transition in 2024.

With more than 100 vessels contracted so far for voluntary approval, as well as a larger range of automation and navigation system suppliers type-approving their systems with us, we believe DNV and the industry is on a good path. DNV class rules and the IACS URs use the IEC 62443 standards that address OT cyber security in a holistic way, including both technical and process-related aspects.

New URs ensure holistic cyber security of on-board equipment

Firstly, UR E26 aims to ensure the secure integration of both OT and information technology (IT) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship. This UR targets the ship as a collective entity for cyber resilience and covers five key aspects: equipment identification, protection, attack detection, response, and recovery.

Secondly, UR E27 aims to ensure system integrity is secured and hardened by third-party equipment suppliers. This UR provides requirements for cyber resilience of onboard systems and equipment plus additional requirements relating to the interface between users and computer-based systems onboard, as well as product design and development of new devices before their implementation on board.

The new IACS unified requirements (URs) – overview

… aims to ensure the secure **integration of both operational technology (OT) and information technology (IT) equipment** into the vessel's network during the design, construction, commissioning and operational life of the ship.

… targets the ship as a collective entity for cyber resilience and **covers five key aspects: equipment identification, protection, attack detection, response and recovery**.

… aims to ensure **system integrity is secured and hardened** by third-party equipment suppliers.

… provides requirements for **cyber resilience of on-board systems and equipment** plus additional **requirements relating to the interface between users and computer-based systems on board**, as well as **product design and development of new devices** before their implementation on board.

Source: DNV

Photo: Canva

System delivery across different industries

DNV believes that one strength of the new URs is that they are built on concrete requirements and based on internationally recognised IEC 62443 standards for control-system cyber security. This will greatly support suppliers that deliver their control systems across different industries.

It is also positive that the two URs are complementary. UR E27 lets suppliers focus on developing cyber-security barriers through, for example, a type approval of their system, so that yards and owners will have a range of pre-approved systems to choose from when implementing the requirements of UR E26 into their vessel designs and operation.

Steps vendors should take in view of the time pressure

The fact that yards and vendors will have to verify critical systems to meet the requirements represents a big change for the industry given that control systems have a long lifespan and development processes are time-consuming. Especially smaller vendors are likely to face resource challenges meeting the requirements within the tight time frame.

There are less than two years left and vendors and yards will need this period to assess and verify that their control systems are compliant. We encourage all vendors to, firstly, go through their portfolios and systematically assess which products/systems can they make cyber secure enough to still be in use after 1 January 2024. This pertains especially to vendors offering digital services in the cloud to prevent leakage of, for example, key environmental data.

Vendors should then make a detailed analysis of what needs to be done, and execute those actions followed by testing and getting type approval. To keep systems safe, they will need to look at attack surfaces, log-in security barriers, and configuration protection. They will also need to protect USB removable device interfaces and network interfaces, especially links to shore, as well as implement consistent patching so software is continually up-to-date.

They should also ensure that back-up and recovery procedures are in place to return the system to a safe state. If a system goes down, you should be able to recover it sufficiently to continue critical operation and ensure key technical functionality.

How can we help?

DNV can help in two main ways, by type approval for equipment and systems, either separately or as part of its Cyber Secure notation for a new ship, as well as by providing advisory services from its independent DNV Accelerator unit (which can help vendors examine all the above challenges on their journey towards type approval). Our experts aid customers with support system risk assessment/improvements, penetration testing and training in a third-party witnessing role, as well as system documentation if desired.

Even before the new IACS URs come into force, DNV is already conducting type approval of various automation and control systems with major suppliers on a voluntary basis. For example, DNV has already type-approved key systems from ABB, Kongsberg and Wärtsilä, and is working on the same for several other control and navigation systems.

Type-approved systems reduce risks and documentation work of newbuild projects

We are fortunate to be the preferred class partner major suppliers choose to work with on type approvals. They value us as a discussion partner based on our experience and expertise. We take the process very seriously as it reflects our brand value.

In addition, when vendors choose to get a system type-approved by us, it will reduce risks and uncertainties of newbuild projects, as well as reduce the documentation that each vendor needs to provide for each vessel. Detailed cyber security documentation is something that a supplier would like to limit the distribution of, hence a type-approval certificate plays more than one role.

We encourage all yards and vendors who are in doubt over what the upcoming IACS URs will mean for them and what to do to reach out. Whatever challenges you are facing, I am 100% certain we will be able to support you.