2016 VOLUME 1

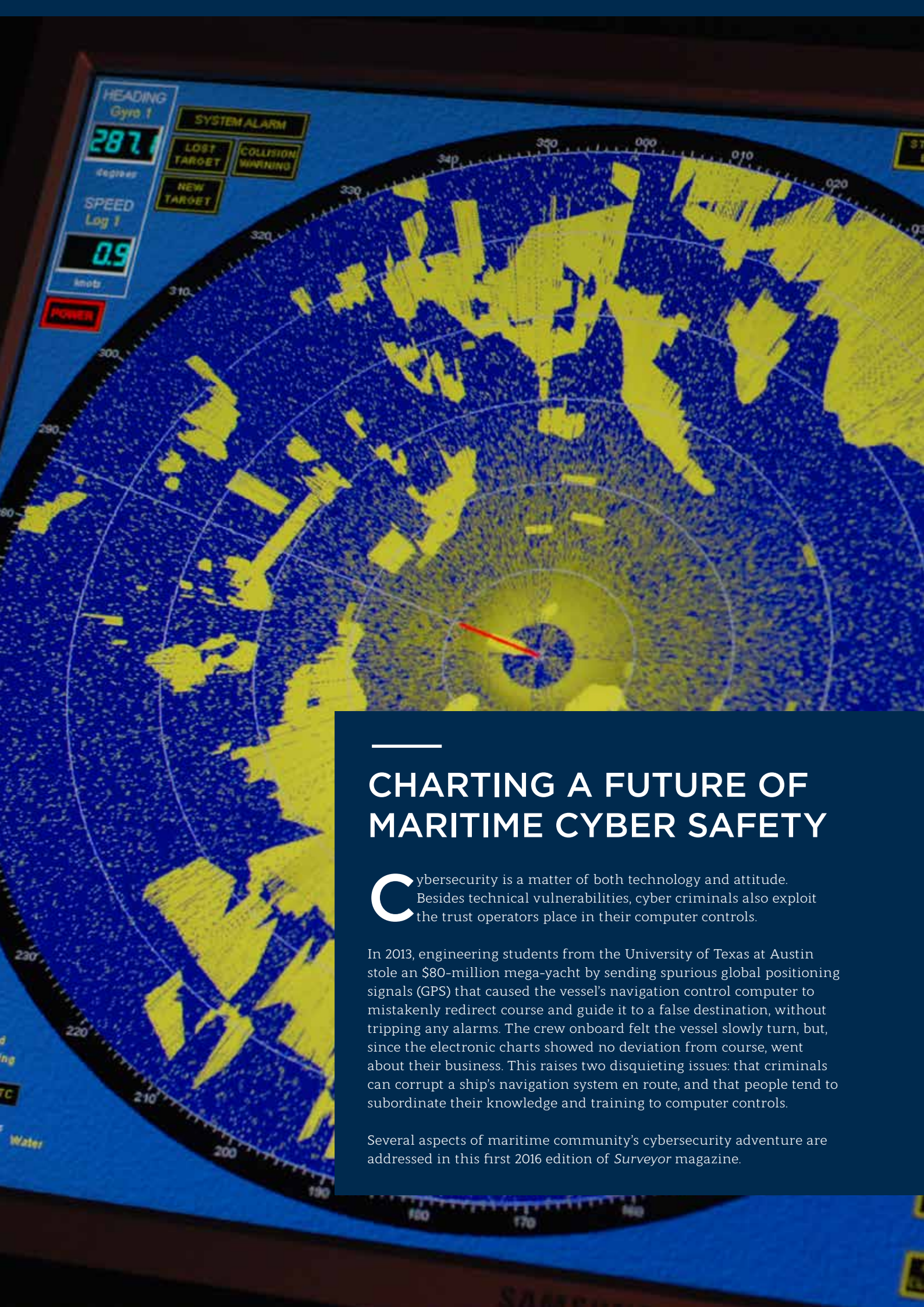
# SURVEYOR

AN ABS MAGAZINE



## THE CYBER ISSUE

ABS




# CHARTING A FUTURE OF MARITIME CYBER SAFETY

Cybersecurity is a matter of both technology and attitude. Besides technical vulnerabilities, cyber criminals also exploit the trust operators place in their computer controls.

In 2013, engineering students from the University of Texas at Austin stole an $80-million mega-yacht by sending spurious global positioning signals (GPS) that caused the vessel's navigation control computer to mistakenly redirect course and guide it to a false destination, without tripping any alarms. The crew onboard felt the vessel slowly turn, but, since the electronic charts showed no deviation from course, went about their business. This raises two disquieting issues: that criminals can corrupt a ship's navigation system en route, and that people tend to subordinate their knowledge and training to computer controls.

Several aspects of maritime community's cybersecurity adventure are addressed in this first 2016 edition of *Surveyor* magazine.

2016 VOLUME 1

# SURVEYOR

AN ABS MAGAZINE

## FEATURES



Published by ABS
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA
Tel: 1-281-877-5800
Fax: 1-281-877-5803
Email: abs-worldhq@eagle.org
Web: www.eagle.org



**Editorial**
Joe Evangelista

**Graphics**
Christopher Reeves

Paige McCown, Director



## Photo Credits:

Cover, 2, 4, 6, 12, 15, 17–20: Shutterstock; IFC: Joe Evangelista; 3: USMRC; 4: LISCR; 5: Cybrex LLC; 7–9, 15: Wärtsilä; 10–11: Rolls-Royce; 13: Project MOSE; 14: ABB; 17 (bottom): US Coast Guard; 19 (bottom): ABS.


# GIRDING FOR BATTLE IN THE CYBER ARENA

Early last year, the data breach investigation team at Internet service provider Verizon reported that one of its clients, a major Middle Eastern shipping company, experienced an unusual piracy incident involving the theft of millions of dollars in jewelry, diamonds and other valuables from one of its containerships. The odd thing about the theft was that the pirates were on and off the vessel in only 90 minutes, during which time they precisely targeted the few containers – out of the thousands onboard – that held the valuables. The investigators looked for company insiders who might have provided confidential shipping information to the invaders, but found instead that the data breach had an even more disquieting source: the pirates had collaborated with cyber criminals to steal data from the head office that left the ship open to a seaborne attack. Shipping's oldest enemy and its newest foe had finally joined forces.

The cyber cadre exploited a weakness in the shipping company's computer architecture to hack its content management system (CMS), the place where important documents such as ship manifests and bills of lading are stored. Using malicious software known as a 'web shell', they were able to find and download not only shipment information, but also the company's GPS vessel tracking data. They passed this along to the pirates, who then knew which ships held something they wanted, where on the ships the booty would be, and when the ship would be in a vulnerable location. Further, in resolving the issue, investigators discovered that the CMS had been compromised months earlier, and that several prior instances of apparently 'normal' piracy on the company's ships could be linked to downloaded documents.

That level of infiltration recalls a major cybercrime in the Port of Antwerp that authorities exposed in 2013. In that case, a drug-smuggling ring hacked into computer

systems controlling container movement and location, stealing data that enabled them to lose containers and send trucks to quietly pick up the boxes in which their confederates had hidden the contraband. The hack started with deceptive emails to port staff containing malicious software, which enabled the thieves to remotely access sensitive logistics data. Later, they broke into company offices and installed small data interception devices, known as key loggers, disguised as computer cabling; these record all keystrokes and, thus, all passwords and system commands. The criminals were inside the port's computer network for two years before detection.

"INTERVIEWS OF CREWS, PORT CAPTAINS, PORT ENGINEERS AND SENIOR MANAGEMENT INDICATED VERY LIMITED AWARENESS AS TO THE IMPORTANCE OR PRIORITIZATION OF CYBER AWARENESS, SECURITY, SAFETY, AND SECURITY PRACTICES."

Since then, the International Maritime Bureau has warned that shipping could become "the next playground for hackers," and at least one insurer reported discovering that what appeared to be petty-theft break-ins at shipping company offices were actually cyber espionage operations in which spyware and devices were installed on office computers.

Besides such targeted cyberattacks, there is also a growing number of reported incidents caused by normal vandalism-oriented malware floating around the Internet, like the ship that was delayed in port two days due to a virus infection in its electronic chart display and information system (ECDIS). The infection was so difficult to remove that the operator had to bring paper charts onboard in order for the vessel to get underway.

Taken together, incident reports like these indicate that cybersecurity, like safety at sea itself, involves both individual and group responsibilities. While shipboard and shoreside staff must be "cyber educated and aware" and maintain good digital safety practices, the company itself must enshrine cybersecurity in its processes and procedures to prevent malicious attacks and accidental infection.

**Captain Alexander Soukhanov,** Vice President, USMRC

Such is among the conclusions of the Maritime Cyber Assurance research program conducted by the United States Maritime Resource Center (USMRC), a non-profit research group, and its partner, cybersecurity firm Cybrex. The ongoing effort went operational in May 2015 after partnering with the Liberian Ship Registry and shipowner group BIMCO, and has since expanded to add marine terminals to its assessments.

"Interviews of crews, port captains, port engineers and senior management indicated very limited awareness as to the importance or prioritization of cyber awareness, security, safety and security practices," says Captain Alexander Soukhanov, vice president, USMRC. "In many cases, what we discovered was determined to present a very high severity of risk."

These risks raise "significant potential for disruption," he says, such as malicious takeover of engineering controls and corruption of electronic navigation charts. Some of the maritime industry's chief cyber vulnerabilities, as exposed during the research, were:

- Little to no evidence of cybersecurity policy
- Little to no cyber awareness among the crew
- Unsupported/obsolete operating systems, even in some newbuilds
- Many unpatched systems
- Many systems without anti-virus software or updated anti-virus definitions
- Unauthenticated or bypassed workstation or system access


- Dangerous modifications by crew (to software or systems) and evidence of ad-hoc networking by the crew
- Small office/home office IT infrastructure, which is inappropriate for an industrial environment
- Removable media access on shipboard PCs
- No cyber auditing occurring as a shipboard and ship management safety procedure
- Internet-connected Industrial Control Systems
- Critical systems connected to the Internet without protections or segregation
- Many systems Ethernet-connected and Internet-ready, but not protected.

One of the study's main sponsors was the Liberian Ship and Corporate Registry (LISCR), which, among other duties, identified ship operators and vessels for the assessments. During the invitation phase of the project, the organization discovered one surprising result even before any data was collected.

**Stephen Frey**, Vice President, LISCR

"In some cases, clients told us they had experienced cybersecurity problems already," says Stephen Frey, vice president, LISCR. Most of those incidents were what he refers to as "small issues" generated by the same "normal" menaces that computer users around

the world face every day: a computer stops working due to accidentally downloaded malware, for example, or a system develops problems because an infected device was plugged into a USB port.

Millions of people in all walks of life engage in risky cyber behavior, such as paying bills online via public Wi-Fi, accessing secure sites on hotel desktops, opening mysterious links in e-mails and plugging thumb drives of unknown origin into their personal computers – and the potential for an unwanted cyber event increases daily. You don't even have to be online to be at risk; researchers from the Georgia Institute of Technology once demonstrated the relative ease with which a hotel iPhone charging station could be rigged to install malware onto smart devices. Threats can come at a ship from many angles.

Average risks plus special vulnerabilities mean that cybersecurity requires an expanded level of vigilance from the shipping community. Even if the problems are only minor inconveniences, malicious programs exist in such great numbers and diversity that, taken together, they represent a serious threat of disruption to vessel operations.

"These small issues can be just as damaging as a major attack; plus, they are random problems. For every malicious act, you can expect to see hundreds of random problems," Frey says, adding that a virus can board a ship as easily as it enters a home computer. "All USB ports look alike," he explains. "Chances are good that somebody on the bridge with a tablet or smart phone to charge will plug it into a USB port without looking to see if that port is part of the ECDIS or the navigation system – and without any way of knowing if the device is leaving something behind. Protection of systems onboard is pretty low right now."

According to the USMRC, the most likely infections onboard a vessel would be light to moderately disruptive events that originate in such incidental sources. Deliberate attacks or exploitation by an organized adversary appear to be less likely, simply because there is currently little evidence to suggest otherwise.

"We know of incidents where cyber sources were attributed to significant operational disruptions that delayed vessels and required lengthy restoration processes, but the origin or nature of the adversary was not determined," says John Bos, president of Cybrex LLC. "While the nature of the potential adversary is a substantial part of the risk equation, common vulnerabilities across industry sectors exist in such quantity that high adversary skills are often not necessary to achieve the desired effects. Cybersecurity and preparedness across the maritime industry is inconsistent and generally low, both afloat and ashore," he adds.

**John Bos**, President, Cybrex LLC

"With cyber issues, you have to continuously protect every vulnerability you discover," notes Frey. "Malicious programs can float around the Internet forever, looking for unprotected computers. This means you have to look after all the old issues as well as the new issues; with each new system you bring online, you're adding to the area, or footprint, of what you have to protect. It's a constant process in which the threats keep expanding."

All of which leads Soukhanov to suggest a few urgent first steps for shipping companies starting out on their cybersecurity journey:

- Invest in a cyber assessment now. The cost of a cyber disruption could be far beyond what you save by doing nothing, or what you spend on preparedness.
- Take responsibility for your vessels' IT and cybersecurity. Physically survey, understand and document your vessels' IT networks.
- Undergo an independent cyber research assessment by experienced professionals who understand the maritime domain and can clearly explain the potential impact of highly technical vulnerabilities to the master and CEO.
- Amend your Safety Management System with an initial cybersecurity policy for your operations. Basing this on your cyber research assessment is even better, as it will be evidence-based. Don't wait.
- Train and educate everyone, from the C-Level to the deck plates, without exception.

For Frey, the best protection is prevention through education. "Training and education in cybersafety is part of the answer to these kinds of issues – not just for the crew, but for everyone ashore as well," he says. "Another part of the equation is establishing the right safety protocols, restrictions and firewalls. Putting such protections in place is like putting locks on your door. If you leave your door poorly secured, anybody can walk in." ■

# PUTTING BIG DATA TO WORK


A kind of mythology seems to be building around big data and big data analytics, terms referring to the astounding amount of rapidly accumulating information in cyberspace and the analysis techniques that make use of it. At present, news media and international fora alike are overflowing with praise and prediction for big data as a deep well from which will be raised such benefits as better decision-making, improved industrial efficiencies, more effective marketing of goods and services and enhanced crime fighting and anti-terror capabilities – in addition to adding billions of dollars to national economies. As can be expected, much of the excitement is generated by companies selling big data services, but, unusually, there is also much truth and great promise beyond the hype.

Data is, quite literally, coming from all directions in all varieties and at an inconceivable rate, generated by computers, smart devices, robots, machines, sensors, industrial controls, security cameras, transmitters and any device that measures, observes or records something – to name a few sources. According to IBM, 2.5 quintillion bytes of data are produced every day, and 90 percent of all data in the world has been created in the past two years. This ever-growing cyber hoard is now widely viewed as a treasure chest of potential insights into just about anything imaginable, with analytics as the key to unlocking it all.

Among the alluring possibilities of big data manipulation is the potential to predict the future of things and people based on patterns and trends from the past – for example, determining when equipment is most likely to need servicing, or what actions people are most likely to take under a given set of circumstances. The New York City Police Department took an attention-getting step in people prediction several years ago when it teamed with Microsoft to develop the Domain Awareness System, a crime-recognition machine that integrates information from police databases, street cameras, radiation sensors, license plate detectors, public data streams and other sources, with the goal of predicting potential crime "hot spots" needing a boost in police presence. Meanwhile, online retailer Amazon received a patent for "anticipatory shipping", a process that tries to anticipate customer purchases before orders are placed so the items can be moved to nearby depots for rapid delivery.

The excitement over big data is such that the 2012 World Economic Forum in Davos, Switzerland, declared data to be "a new class of economic asset", like currency or gold. Still, when analysts talk about it, data itself sounds less like currency and more like sand: absurdly plentiful and barely useful unless you know what to do with it. Just as sand can be turned into glass and concrete and used to build a skyscraper, or poured into sacks and be little more than dead weight, big data can be used to revolutionize a business or bog it down in senseless correlations. Success or failure in the analysis of data, big or small, depends on the quality of the analytics and the abilities of the analyst.

"THE MARITIME INDUSTRY IS JUST STARTING ITS JOURNEY INTO BIG DATA ANALYTICS, BUT THE EARLY ADOPTER SHIPPING COMPANIES APPLYING IT TO OPERATIONAL IMPROVEMENTS HAVE ALREADY REPORTED REDUCED FUEL CONSUMPTION EVEN AS THEY INCREASED THE AMOUNT OF FREIGHT CARRIED."

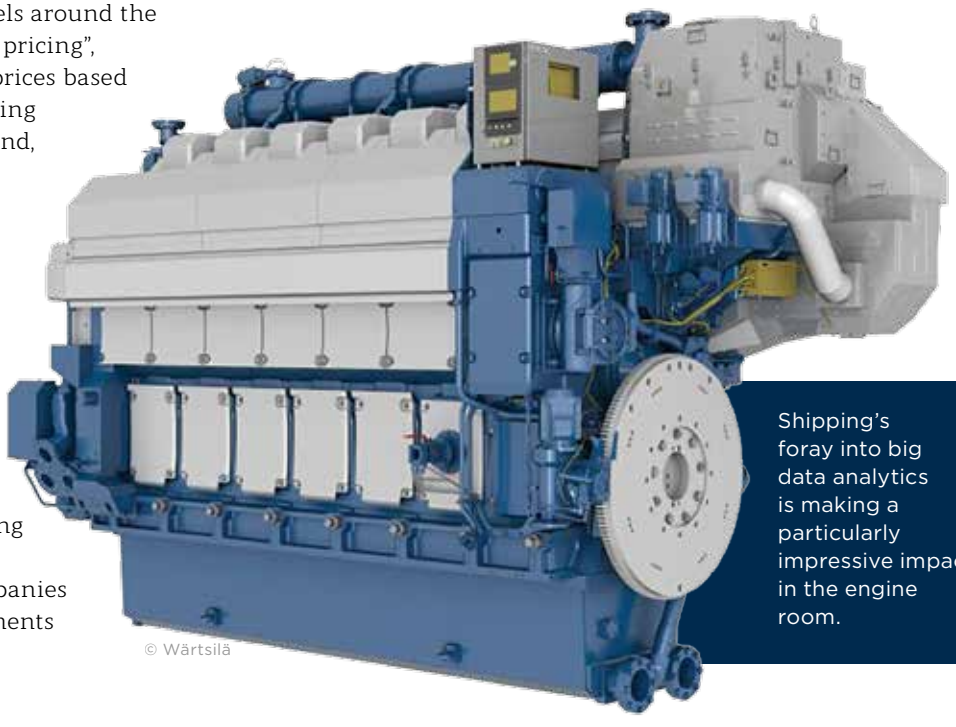
Successful applications of big data analytics have disrupted traditional business models around the world. Witness the rise of "dynamic pricing", whereby companies rapidly adjust prices based on a broad landscape of live streaming data that includes supply and demand, pricing by the competition, time of day and even weather conditions; a major U.S. retailer uses this for near-real-time price adjustment of some 73 million items. Dynamic pricing has changed the consumer experience in industries ranging from air travel and retail sales to professional sports and entertainment.

The maritime industry is just starting its journey into big data analytics, but the early adopter shipping companies applying it to operational improvements have already reported reduced fuel consumption even as they increased the amount of freight carried. One leader in this area, Maersk Line, cut fuel consumption by more than 13 percent between 2012 and 2014 while increasing the number of boxes carried by 11 percent, according to company records. Reported fuel savings during that time amounted to 1.35 million tons per year, equivalent to 1.5 million tons when the increase in freight volumes is factored out. Those are pretty small numbers in a world estimated to use some 90 million tons of fuel a day, but they promise a significant shift in global fuel consumption as similar techniques spread through the maritime and other industries.

Aside from fuel savings, shipping's foray into big data analytics is making a particularly impressive impact in the engine room, through condition-based maintenance, predictive analyses and remote support.

Remote support involves some science-fiction-like capabilities that have sparked stories circulating through the industry about engine makers taking control of ship engines en route and adjusting them without the client's knowledge. Such myths undermine the client's sense of cybersecurity and thus need dispelling, says Magnus Miemois, director of sales and service at Wärtsilä. While remote control of an engine is possible today, takeover is not what support technology was made for, he says.

"Remote support of ships today is about the people onboard being able to access expertise, share information and receive help over great distances in real time," Miemois says, "and we have a number of clients that have signed on for remote support as



© Wärtsilä

Shipping's foray into big data analytics is making a particularly impressive impact in the engine room.


The most futuristic element of remote support is something Wärtsilä calls the "virtual service engineer".




**Magnus Miemois,** Director of Sales and Service, Wärtsilä

part of long-term service agreements. But it is a reactive activity, always based on the customer asking us to become engaged and enabling us to connect with his system. The scenario where we detect a problem remotely, take action and then tell the customer in a by-the-way manner what we did to fix it is not part of our reality."

The first safety barrier for the client in the remote support process is that a session must be initiated by the vessel, somewhat like the way a personal computer user must grant a help center technician access to his desktop.

"The ship has a physical mechanical switch that only specific people can access, which needs to be put in the on position before we can engage in remote support. After that, the remote supporter sees the same screens as the crew and can assist with troubleshooting," explains Erik Ristiluoma, Wärtsilä's general manager for operations and maintenance.

"On our side, we can do many things during these sessions, such as trending analyses, but cannot control anything onboard. We can look at the history of a piece of equipment, see what has been happening and in what sequences, draw conclusions as to where the fault is most likely to be found, and suggest solutions," he says.

The predictive element of the process draws upon the vessel's condition-based maintenance (CBM) database. Under CBM, an onboard system delivers a daily dump of averages and parameters into the manufacturer's database, which technicians sift through for trends and anomalies, looking to catch potential problems or offer predictive maintenance tips. "Our CBM philosophy is that, based on the trending of parameters, you can actually predict the correct maintenance periods for any piece of equipment," says Ristiluoma.


**Erik Ristiluoma**, General Manager for Operations and Maintenance, Wärtsilä

The most futuristic element of remote support is something Wärtsilä calls the "virtual service engineer", a technology that uses augmented reality to simplify onboard problem-solving. It has the chief engineer aboard ship and the service engineer in the office wear optical head-mounted displays (similar to Google glasses, but not that particular brand) that allow them to communicate using video, pictures, voice and vision. The service engineer sees and hears what the chief sees and hears, which relieves the mariner of having to explain such things as the way gauge dials are pointing, the position of a manual valve, or a strange sound emanating from a piece of equipment; the service engineer, meanwhile, is relieved of having to verbally guide the client through a complex test or remediation task. Because the headset gives the illusion of presence, the remote service engineer can point a finger at things onboard that he sees through his glass and, as he does so, the chief sees where that hand is pointing through his own headset.

Such enhanced support technologies are changing the relationship between suppliers and customers, making manufacturers a more important part of the client's day-to-day business than they were even a decade ago. As service contracts become more comprehensive and involve more data-driven applications, they create a tighter relationship between supplier and customer, calling for a more intimate sharing of information between them to help resolve problems as they occur.

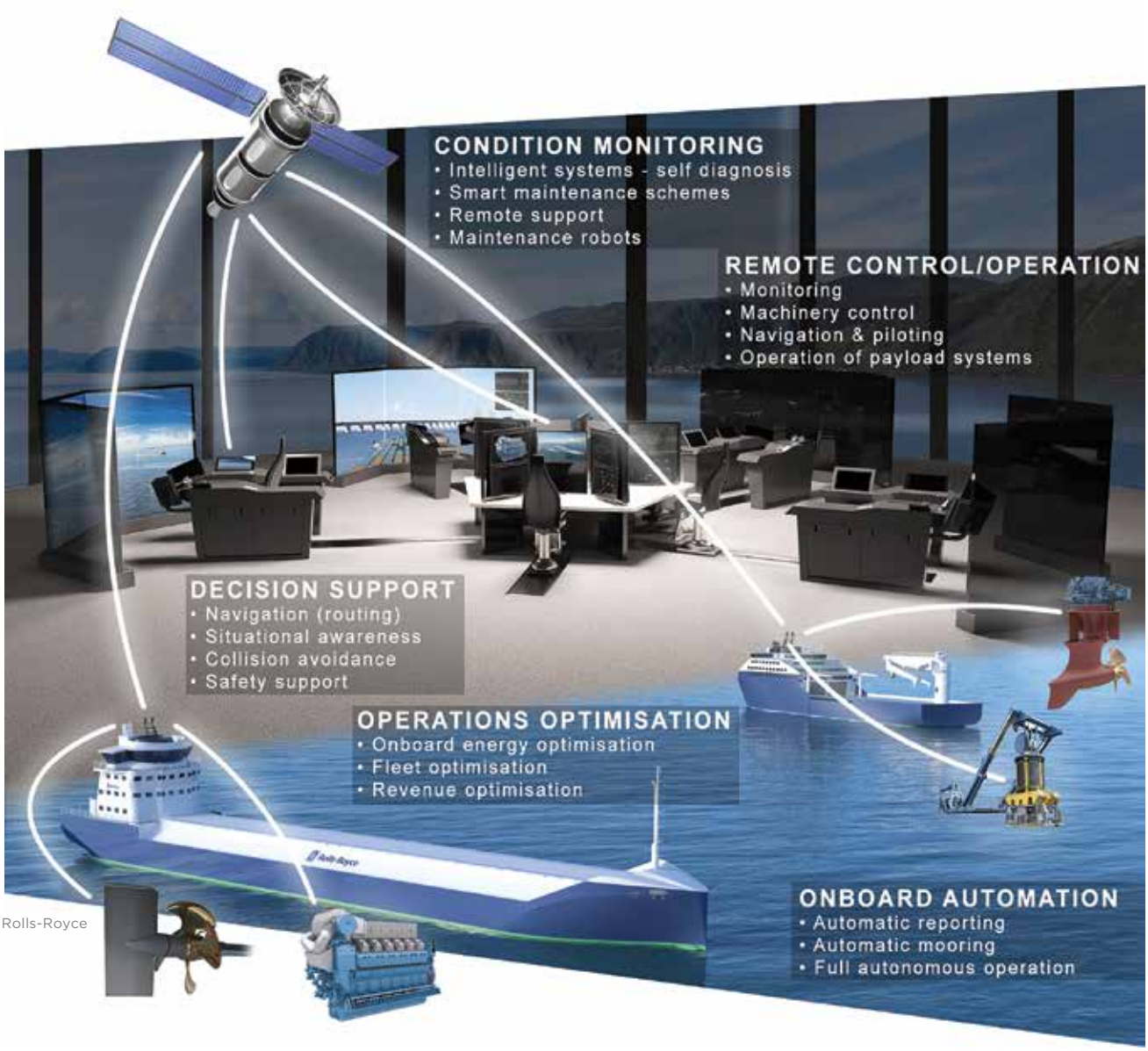
"We are seeing a clear trend towards more comprehensive, long-term service agreements," says Miemois. "Traditionally, service has been about calling for parts, labor, etc. as needed, which is a scenario of very little forward planning. Now the industry recognizes that, with such tremendous amounts of capital tied up in maritime assets, optimizing return on investment means optimizing uptime through, among other things, better forward planning. This means that service today is not just about delivering parts, labor and assistance, but also about doing so in a way that is synchronized with the operation of the vessel," he says. "The faster you can form an understanding of a situation, the better off you are." ■

# FROM SHIP INTELLIGENCE TO INTELLIGENT SHIPS

The unmanned engine room was a disruptive concept for the maritime industry when introduced 40 years ago, but was eventually embraced by all. The same may one day be said of the unmanned ship, if a handful of industry visionaries get their way.

The vision they are pursuing is one of autonomous robotic vessels sailing crewless on the open ocean, captained by an artificial intelligence that steers with precision and optimizes the voyage at every step of the way, until, approaching port, the "smart ship" hands over its helm to a human captain who takes command by remote control from a virtual bridge in a shoreside facility.

Realizing that vision is the shared goal of two current EU-funded research programs: the $3.5 million Maritime Unmanned Navigation through Intelligence (MUNIN) project in the UK, which began in 2014, and the $6.6 million Advanced Autonomous Waterborne Applications Initiative (AAWA) that started up last year in Finland. The former is dedicated to developing



new vessel and system designs, and the latter to exploring the economic, social, legal, regulatory and technological factors that need to be addressed before autonomous ships can become a reality.

"SHIPPING IS AT THE DAWN OF A NEW ERA, THE ERA OF SHIP INTELLIGENCE."

As a practical matter, it may be decades before fleets of oceangoing automatons crisscross the world guided by a digital brain, according to what a spokesman for the International Chamber of Shipping told the BBC when the MUNIN program was announced. Yet some science-fiction-like developments are already with us – pushbutton navigation and remote control of full-size ships, for example – and others are just a short step away.

"Shipping is at the dawn of a new era, the era of ship intelligence," says Oskar Levander, a leading proponent of smart ship development and vice president of innovation, engineering and technology at Rolls-Royce. A prominent participant in both MUNIN and AAWA, the company has been stumping hard since 2013 to promote the idea that an evolution towards autonomous vessels is inevitable.

"This digital revolution is driving a number of topics at the same time all over the world, such as the Internet of Things, big data analytics and, in the industrial sectors, the 'Industry 4.0' concept," Levander says. "For the maritime sector, we group these changes under the term 'ship intelligence', which we like to say has three pillars – asset management, optimization and decision support and remote and autonomous operation – supported by a number of enabling technologies such as object detection, communications, automation and cloud computing."

The key to making functional, commercial autonomous ships, he explains, is development of "situational awareness", a technology that promises to give a captain on land a better understanding of what's around his ship than he would have if he were standing on its bridge. This is to be achieved by combining numerous sensors and cameras to stream vast quantities of data to high-capacity computing and visualization equipment, which will then produce a live, unobstructed 360° view around the ship, supplemented by navigational and other decision-assist information. The ship control centers where

**Oskar Levander,** Vice President of Innovation, Engineering & Technology, Rolls-Royce

all this occurs will also be bases for remote vessel supervision and asset management.

"We don't want to replicate the bridge in the control centers, because the bridge only gives a restricted view of what's happening around a ship," Levander says. "What we want is more like a computer game – you can have a bird's-eye view of the ship's situation if you want, for example, because we are not limited to being inside the bridge. We can have a complete world around the captain, created using cameras, radar, lidar and sensors to create a condition of total awareness."

The heart of this development stream is "sensor fusion", the unification of many new and existing sensors into a new kind of system that can accurately capture the constantly changing physical reality around a ship. This sensor web will be joined to object detection technology, and the combined hardware network then linked to automatic navigational logic systems (technologies targeted for development by the two EU research projects). When finally assembled, the grand system will enable a ship to operate autonomously at sea and under remote control in port.

It sounds like a far-off goal, but, according to Levander, much of the technology exists today and some revolutionary steps forward are poised to happen. The first generation of smarter ships, for example, will use these advanced technologies to assist decision-making on the bridge and to enhance operational efficiencies.

"It's not as if we expect to jump from fully manned to fully autonomous vessels in one leap," he says. "There will be a lot of steps in-between, including the development of new ways of operating ships. The road map going forward starts with the smaller applications like ferries and coastal vessels."

Logical first adopters are road ferries that ford rivers or link islands with the mainland. They offer a good platform to prove the technology's reliability because their short pendulum routes are relatively simple to navigate, allow good observation from shore and put the vessels in port very frequently, sometimes on an hourly basis, where the systems and equipment can be examined.

Another reason why ferries are likely to be the first commercial vessels with intelligent assistance is that they are local vessels subject to local rules. Changing international legislation to accommodate these new systems for oceangoing vessels is likely to take some time, while changing national legislation for local waters is much easier to accomplish – especially if the maritime authorities are supportive.

"There are several flag States that are very keen on seeing this development happen," Levander notes. Asked to specify, all he will divulge is that the more forward-looking flag States can be found "in Northern Europe and one or two places in Asia."

The practical goals and promises of this new technology stream have aroused enthusiasm among shipowners as well as flag States. "Yes, some unmanned boats are already out there, but we are not aiming to produce another test subject; we want to have a commercially viable ship in operation, doing commercial work," he says, stressing that smarter ships have become an industry expectation. "We have customers that want these solutions, and would like to have them as soon as possible," he adds.

Levander believes one of the first live applications in the smarter ship revolution will be pushbutton ferry crossings, in which a captain on the bridge presses a button and watches the navigation system drive the vessel in an efficient, predefined manner. The next step, he explains, will be to have the ferry make its crossing with no one on the bridge, remote-controlled by a captain from a virtual bridge on land. In the final step, the vessel will make a fully autonomous crossing with only supervision from a control center. He does point out that operators of autonomous vessels carrying passengers may still want to have crew onboard to provide hotel services and aid the passengers in the event of evacuation.

Truly autonomous navigation remains a future goal, according to Levander, mainly because further development is needed in and around the areas of systems standardization, reliability and validation. Still, the first steps forward promise to be impressive.

"You will see automatic ferry crossings very soon," he predicts. "Automatic crossing with a captain on the bridge is something we could sell today – as is the next step, remote control by a captain that is not on the bridge."

That said, which vessel type or service will end up being the debut platform for these technologies, and in which country the opening bell of the automatic ship revolution will be rung, remain open to speculation.

"We are working with several different owners on several different cases, including coastal cargo ships, and all are pushing for increased automation, so it might just be a matter of who gets a vessel built first," Levander says. "But I do believe we are going to have one of these ships on the water before the decade is out." ■

Ferries are likely to be the first commercial vessels with intelligent assistance since they are local vessels subject to local rules.


# REAPING THE INTERNET OF EVERYTHING

Venice, Italy, is built on a lagoon that communicates with the Adriatic Sea, which throughout history has periodically damaged the city with severe floods caused by excessively high tides. Now, a decades-long effort to protect the historic city and surrounding communities from these deadly tidal fluctuations is set to come to fruition. Named MOSE (an Italian acronym for Experimental Electromechanical Module), the €7 billion project is an immense flood barrier system of breakwaters, navigation locks and 78 large underwater mobile gates installed across the lagoon's three inlets. When high water threatens, the boxlike steel gates, each weighing some 300 tons, fill with compressed air and swing into place in about 30 minutes, isolating the city from surges of up to 3 m (9.8 ft) in height. The most impressive aspect of the project, however, may be that the huge system will very nearly operate itself.

The electronic brain behind MOSE will manage data signals from some 50,000 devices and coordinate operation of the entire system, raising and lowering the barriers according to pre-set parameters based on the movement of the water at the inlets. Integrated into the computerized control is an electrical power automation solution that enables remote operators to control the power network and ensure stable electrical supply for the system. After 13 years of construction, MOSE is scheduled to be in operation this year, and when it is will stand as one of the world's most prominent best-use examples of the Internet of Things.

There are a several variations of the term "Internet of things". ABB, the manufacturer of the automation system that drives MOSE, calls it the "Internet of things, services and people"; others call it the "industrial Internet of things"; still others call it the "Internet of everything". By whatever name, it speaks of the same hope: that of making life better through automation, connectivity and computerized assistance.


The Internet of things (IoT) is a phrase coined some two decades ago to refer to the large number of devices that transmit or receive data over the Internet – by some estimates, 20 billion devices will be transmitting data over the Internet by 2020. As a concept, the IoT became particularly meaningful for society in recent years, when technology advances – such as the linking of thousands of computers to form clouds of tremendous storage and computing capacities – brought within common reach the ability to analyze and make use of that big data. Today, allied with the analysis techniques called big data analytics, the IoT is enabling organizations big and small to access vast data pools that can be mined, manipulated, organized and analyzed with the goal of finding new discoveries and generating insights that might help businesses

ABB Integrated Operations Control Center in Helsinki.

© ABB

perform better, help people make more informed decisions, and help improve the operation and maintenance of machines and industrial systems.

The union of the IoT and big data analytics has brought about a convergence of Information Technology (IT) and Operational Technology (OT), driven by interactive linkups between computers in the office and computerized controls on the factory floor. Industrial OT products, such as programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems, are integrating with IT infrastructure and applications to produce revolutionary changes in industries ranging from power generation to shipping.

One example is Bosch, a leading engineering conglomerate who put IoT at the center of its business strategy. Known for smart consumer products and automotive components, Bosch is also a leading manufacturer of micro-electro-mechanical systems sensors, and wants to use IoT technologies to connect its 250 factories around the world. The first of these connected factories, which produces hydraulic components for cars in Germany, has close to 5,000 systems linked together, and reports that the connected technologies have brought about a productivity increase of 10 percent. The general manager for IoT and Product Management at Bosch Engineering and Business Solutions, Uday Prabhu, told a Bangalore technology conference in May of one instance where, after analyzing data on some 600 variables at 16 assembly line stations, the connected plant was able to reduce scrap by 67 percent, saving some €2.4 million annually.

In some cases, products using the IoT have become product-service hybrids – Internet-connected, intelligent machines that send data to the manufacturer for analysis as part of an enhanced service contract. The maritime industry is seeing this in the evolution of the ship's main engine, the latest of which stream data to both the owner and the manufacturer for trending and analysis. Wärtsilä, for one, uses the IoT and big data analytics in a remote support service that allows in-house service technicians to confer live with a vessel's technical management and the engine crew onboard, and even digitally visit the engine room to instruct the crew in repair activities.

The rise of heavily instrumented ships and engines streaming data to vessel control centers monitoring fleet performance, and the resulting productivity improvements, show how the IoT and big data analytics are beginning to exert an impact on the maritime industry. So does the heightened role that manufacturers have in their customers' daily business – witness the three Integrated Operations Centers opened by ABB, which connect the company's service engineers to hundreds of vessels around the world fitted with its systems. Sensors and software aboard each vessel send equipment and performance data to a center via satellite link, enabling owner and manufacturer to collaborate in remote troubleshooting and make informed decisions about performance and maintenance plans.

Technology evolution on many fronts has enabled the IT/OT convergence; along with development of sensors, controllers, PLCs and SCADA systems that are both advanced and affordable, the proliferation of high-speed, high-capacity communications networks has let the data they generate be sent cheaply, rapidly and in vast quantities. Early adopters in this convergence have focused on improving operational efficiency and engaging in predictive maintenance practices. Many companies now anticipate equipment failures with greater accuracy and respond to critical faults more quickly than in the past, with resulting productivity gains from minimized downtime.

Rolls-Royce, for example, regularly logs data from some 10,000 of its gas turbines installed on airplanes around the world; among it uses for this immense performance database is to predict when one of the engines might need service. The company is now applying this process to its marine engines in developing data-driven vessel health management services, but has a much farther view in mind. Its vice president of innovation, engineering and technology, Oskar Levander, says the next steps in that direction include a move from monitoring equipment to monitoring systems – such as monitoring not only the engine, but also all auxiliary systems that might have an impact on engine performance – and then, applying the systems approach, to attaining a view of whole ship performance. From there the road turns upward towards an ultimate goal, a grand expression of the Internet of things: development of an autonomous ship. ■

# FACING THE CHALLENGE OF CHANGE


Ships and offshore assets have service lives measured in decades, while software rarely goes more than a year without significant updates, security patches, bug fixes or functionality improvements. As a result, vessels and rigs with high levels of automation and computer control can expect to undergo numerous critical software modifications during their lifetimes. This fact of life in the digital age is making the maritime industry pay growing attention to the discipline known as software management of change (SMoC), the practice of systematically describing, testing, vetting, and documenting changes to software applications or systems.

It is known that software installed in a complex system can interrelate in ways that are not always well-understood, even when the programs come from different vendors and perform unrelated tasks. This sub-rosa interaction means the possibility always exists that an improvement to one piece of software might cause a fault in another, or a cascade of faults in an industrial operation. That is why the extensive system integration typical of modern ships and rigs demands that software modifications be thoroughly reviewed and tested for functionality and safety with respect to not only the application being changed, but also to all linked systems.

The longevity of marine assets and the continual update and patching that their onboard control systems require gives SMoC special importance for the maritime sector, simply due to the potential damage

> "THERE IS BASIC KNOWLEDGE OF THE INHERENT WEAKNESSES OF COMPUTERS, BUT NOT AN UNDERSTANDING OF THE RISK TO OPERATIONS."

or downtime that can result from a major software failure or even a minor software glitch. Thus, from the military to the service sectors, the monitoring, management and control of software change is gaining recognition as an important part of both cybersecurity and asset integrity management – itself increasingly dependent on data collection, analysis and diagnostics.

For such reasons, most major equipment manufacturers have rigorous procedures in place to manage software change. Engine maker Wärtsilä, for example, puts all of its 18,000 employees worldwide through compulsory training in cybersecurity, complemented with specific modules on cybersecurity for field and technical personnel.

Without a mandate that software modifications be tested for negative effects in a vessel's particular configuration, there is risk that vendors with a lax

**Kim Eklund**, General Manager, Cybersecurity, Wärtsilä

software safety culture will unintentionally cause inconvenience to their clients, and beyond. Last year, for example, a ship was tied to the dock in Houston for two extra days because a vendor's software upgrade clashed with other onboard systems and prevented the vessel from getting underway.

For a ship, a delay can be as costly as damage if it makes the vessel lose its charter. The risk of software-spawned service interruptions and operational issues makes it essential that owners develop something along the lines of a software book or cyber inventory for their marine assets, in which every piece of operating software and its version history are documented. How this is to be done, and who will bear the administrative burden for keeping the records straight, are among the many questions each company will have to answer for itself as it follows its cyber journey.

Managing software change is just one part of a much larger challenge facing the maritime industry. Lack of cyber awareness is among the basic deficiencies identified by the Maritime Cyber Assurance research program, an ongoing program of cyber assessments on ships and terminals conducted by the United States Maritime Resource Center (USMRC), a nonprofit research organization, and its partner Cybrex LLC, a cybersecurity firm.

"Cyber is not well-understood across the maritime industry," says Captain Alexander Soukhanov, vice president, USMRC. "There is basic knowledge of the inherent weaknesses of computers, but not an understanding of the risk to operations. This applies to all ships we have assessed, old and new," he adds, noting that some form of software management is critical to managing cyber risk onboard.

"Cyber risk management cannot be implemented unless you know your systems and environments and how they are integrated, who your vendors are, and what remote accesses and controls exist. Currently this is inconsistent across the industry. Some companies are cyber aware and have policies and methods in place, but most do not," he says.

One important aspect of managing software-related operational risk is to have solid procedures in place for testing updates before activation, according to Kim Eklund, general manager, cybersecurity for Wärtsilä. "You always need to be context-aware; the basic principle in the industrial control system context is that, of the three key principles of security – confidentiality, integrity and availability, – availability is the overruling aspect to consider," he says, and draws an example from the company's work in the energy sector.

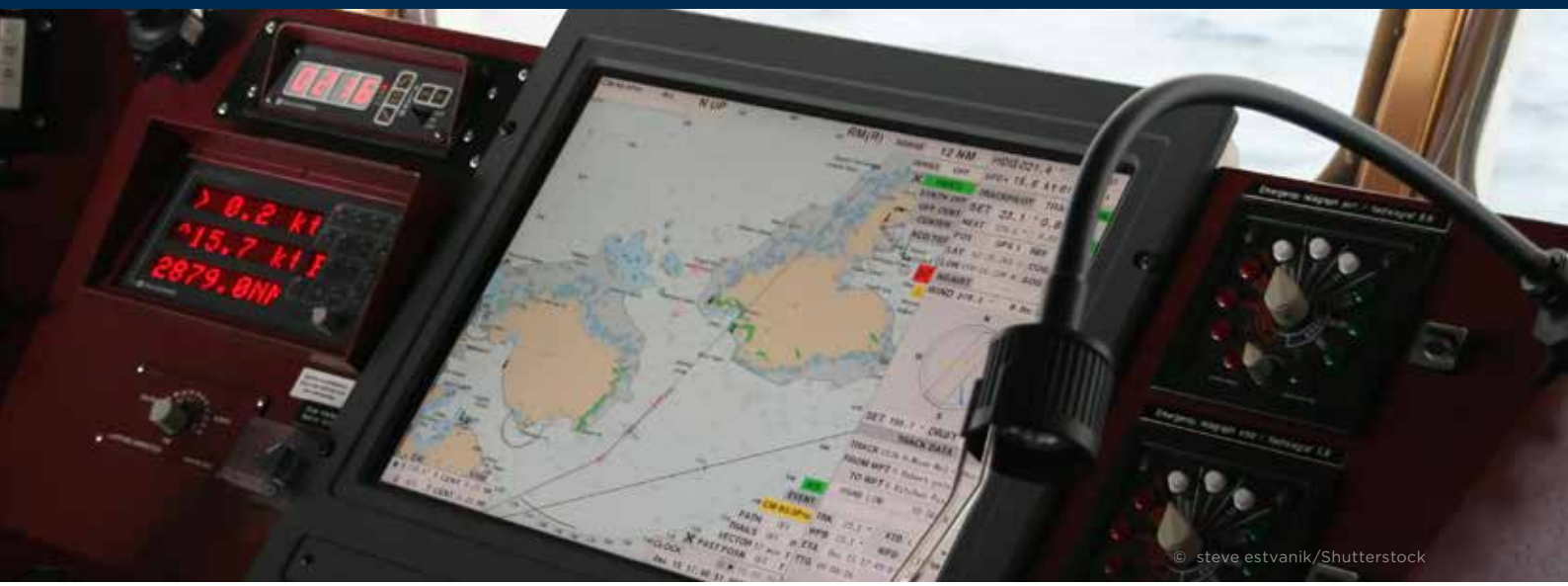
"For updates in stationary power plants, we recently launched a security patching service in which the basic principle is that, besides validating patch authenticity, you also need to validate how that patch is functioning in the operations technology environment," Eklund says. "For that reason, we have a 'virtual validation installation' whereby we can pretest any configuration or update prior to deployment. Other important aspects of software change management are remediation and recovery capability with rigid roll back procedures in place if needed."

At present, ships and rigs are conglomerations of software from a variety of vendors, and possibly the vendors to those vendors. This poses a special concern for the secondhand markets. Technology evolution happens so quickly that a vessel only ten years old might be running antiquated software that is becoming unstable, is no longer supported, or whose original providers no longer exist.

Apart from clear and present cybersecurity risks, the industry needs to prepare itself to deal with other, less definite, but equally threatening challenges from the cyber dimension as the world fleet ages. If the industry's legislative history is any guide, cyber issues are matters best addressed sooner than later, because software safety, in one form or another, will eventually find its way into the International Safety Management Code.

As in other industries, cyber risk management for the maritime sector involves multiple responsibilities and requires conscious effort and cooperation from all sides – owners, operators, vendors and regulators. For asset owners in particular, enshrining SMoC controls and permissions in their Safety Management Systems will be a cornerstone of reliable operations going forward, and an important part of SMoC will be the cyber inventory. After all, it is difficult to manage change in something you do not understand. ■

# CYBER IS A SAFETY ISSUE



© steve estvanik/Shutterstock

The U.S. Marine Transportation System (MTS) consists of waterways, ports and intermodal land connections that allow various modes of transportation to move people and goods to, from and on the water. It is a vast network that includes 25,000 miles of navigable channels; 238 locks at 192 locations; the Great Lakes and the St. Lawrence Seaway; more than 3,700 marine terminals and numerous recreational marinas; more than 174,000 miles of rail; some 45,000 miles of interstate highway supported by 115,000 miles of roadway and approximately 360 sea and river ports that collectively handle more than $1.3 trillion in cargo annually. Even more striking than its vast size and economic power is the fact that virtually all of it is vulnerable to some form of cyber attack.

In speaking to the House Subcommittee on Border and Maritime Security last October, Rear Admiral Paul F. Thomas, the U.S. Coast Guard's Assistant Commandant For Prevention Policy, noted that "Cyber risks manifest themselves as both safety and security concerns. As such, the Coast Guard is emphasizing the term cyber risk management, which also addresses how much the Maritime Transportation System relies on information technology systems to connect to the global supply chain. Vessel and facility operators use computers and cyber dependent systems for navigation, communications, engineering, cargo, ballast, safety, environmental control and emergency systems such as security monitoring, fire detection and alarm systems. Collectively, these systems enable the MTS to operate with an impressive record of efficiency and reliability."

**Rear Admiral Paul F. Thomas**, Assistant Commadant for Prevention Policy, USCG

He also cautioned that, "while these information technology systems create benefits, they also introduce risks. Exploitation, misuse or simple failure of information technology systems can cause injury or death, harm the marine environment, or disrupt vital trade activity."

"Cyber risks are an inherently global issue, and cooperation with international partners is an important part of our strategy," Thomas said. "Covert electronic surveillance by foreign ships visiting our ports is a long standing security concern, and cyber

technology certainly provides new avenues for such activity. Sound cyber practices by marine terminals can help minimize the likelihood that they might become victims of such activity, or of less nefarious activity that might still impact their business or operations. Failure to follow sound cyber practices may create as much risk as not conducting proper equipment maintenance or adequate crew training for conventional shipboard emergencies."

Recognizing cybersecurity as "one of the most serious threats to U.S. economic and national security interests," the U.S. Coast Guard developed its own Cyber Strategy and published it in June of last year. The document states that, "To fully ensure the Coast Guard is able to perform its essential missions in the 21st Century, it must fully embrace cyberspace as an operational domain. To this end, the Coast Guard will focus on three specific strategic priorities in the cyber domain over the next ten years: defending its own cyberspace, enabling operations and protecting infrastructure."

Defending its own cyberspace is described as protecting its information infrastructure and building a more resilient Coast Guard network.

© Greg K__ca/Shutterstock

Enabling operations means supporting those cyberspace operations, both in and out of Coast Guard information and communications networks and systems, that help detect, deter, disable and defeat adversaries. The underpinning of these operations – robust intelligence, law enforcement and maritime and military cyber programs – is essential to all Coast Guard operations in preventing and responding to malicious activity against critical maritime infrastructure. Protecting Infrastructure refers to protecting the MTS and its associated infrastructure, which are vital to America's economy, security and defense. In this context, that means protecting the cyber systems that support the MTS from all identified threats and vulnerabilities.

In the maritime industry today, most reported cyber problems result from human error rather than from targeted criminal attacks – someone clicking on a malicious link in an email, for example, or plugging an infected USB into a company network, or making an operational error by taking by shortcut around procedures. Acknowledging this, when Coast Guard Commandant Admiral Paul Zukunft unveiled the Cyber Strategy, he called attention to an important but often overlooked aspect of cyber self-defense: that the weakest link in any organization's cyber security chain is usually not technology, but the human factor.

"The human factor is critical to managing cyber risks. Many safety and security vulnerabilities come from people doing things like plugging their cell phone into a computer, or failing to apply regular software patches," the Admiral said, and noted that a critical piece of cyber safety "comes down to what I call cyber hygiene. We see that not just with the Coast Guard; we see that throughout every organization.

Zukunft also pointed out that cyber hygiene is critical not only to preventing cyber incidents across all three priority areas of the Coast Guard's Cyber Strategy, but also to maintaining cyber self-protection for any individual or organization in the public and private sectors. That is one reason why the Coast Guard's Cyber Strategy emphasizes the role of people in the cyber safety chain, and particularly stresses the importance, for any organization, of leadership support for its cyber safety programs and its cyber defense team.

Applying its experiences and expertise to the broader maritime cyber landscape, the Coast Guard has been working closely with the Department of Homeland Security and other government agencies to help the maritime industry identify cyber risks, and with the International Maritime Organization to incorporate cyber risk into the Safety Management Code and the International Ship and Port Facility Security Code. ■


VIEWPOINT

# CYBER ISSUES AND HUMAN FACTORS

Howard Fireman

**Howard Fireman**, ABS Senior Vice President and Chief Technology Officer

Marine ships and offshore units are becoming increasingly dependent on Internet-connected computerized controls that often leave them vulnerable to cyber accidents or attacks. Because these assets are isolated at sea and have to survive alone against storms and other environmental hazards, an interruption in the operation of an asset's equipment – for example, a malfunction in navigation, propulsion or ballasting systems – could potentially cause a threat to life, property and the environment.

As the maritime industry grapples with the ever-expanding challenges of cybersecurity, it is becoming clear that most cyber incidents occur not due to technology failures, but due to some form of human error. This makes the human element as important as the technological element in an organization's cybersecurity.

Up to now, the human element in cybersecurity has typically been considered in terms of limiting intrusion into computer systems through safe online practices and equipment use. While good personal user habits will always be critically important to the cybersecurity of an asset, there is another aspect to it that involves the responsibility of the organization's decision-makers to the asset's system architecture. Simply put, to maximize an asset's cybersecurity, its cyber environment must be developed through deliberate decisions by the owner or operator about the automation controls and software to be installed onboard.

Cyber technologies onboard an asset exist to multiply the capabilities of the crew and help the asset operate with greater safety and efficiency. Along with these

benefits they bring a new challenge in the form of new vectors, or sets of considerations, that must be taken into account from the start of the design.

To correctly engineer the cyber component of an asset, every piece of it must be the result of conscious, deliberate decisions made during the design, architecture, build and operation phases of an asset's life. The key to it all is understanding what the asset's proposed cyber systems are intended to do and how they will do it, applying user process development, failure mode analyses and the related event and fault trees, then incorporating that knowledge into the asset's systems engineering and construction.

Proper systems design helps the operator avoid potential errors, thus reducing possibilities for unexpected events or system problems. It is as important to consider how the asset's systems will be used – incorporating the human interfaces, use elements and processes – as it is to develop the product functions. Failure to take control of these matters from the start means abdicating these important decisions to third parties, such as equipment manufacturers or vendors; their cybersecurity choices, while possibly correct according to their point of view, will certainly not be correct according to the unique needs of the owner, operator and the specific asset.

This is one reason why ABS is developing its ABS CyberSafety™ program, which is aimed at building the cyber capabilities of an organization by building knowledge and ability in its staff. The goal is to make maritime companies cyber resilient, or able to anticipate how their systems will function and to recognize and address cyber problems as they arise.

Too many maritime organizations today do not deeply understand the cyber-physical and cyber-enabled systems aboard their vessels and, therefore, do not see the full set of new cybersafety concerns that need to be considered in an asset's design phase and throughout its service life. The ABS CyberSafety program proposes to help these companies develop habits, practices and procedures that will prevent both accidental and deliberate cyber events from endangering the safety of life, property and the environment at sea. ■

© GlebStock/Shutterstock

**WORLD HEADQUARTERS**
16855 Northchase Drive
Houston, TX 77060 USA
**P** 1-281-877-5800
**F** 1-281-877-5803
ABS-WorldHQ@eagle.org
www.eagle.org



ABS