DIRECTPROCESS

WAGO

Big Data for Big Ships
Maritime 4.0 – Opportunities and Challenges

SAFELY ON COURSE IN THE BINARY SEA

"ANYONE WHO TALKS ABOUT MARITIME 4.0 HAS TO DO THEIR HOMEWORK"

REDUNDANT AND YET NOT SUPERFLUOUS

FROM THE BRIDGE TO THE BILGE

WAGO's Automation solutions meet virtually any maritime challenge – from shipbuilding to offshore systems

- Covered from the Bridge to the Engine Room with the "Compass" Certification (BSH)
- Alarm monitoring systems, tank ballast and cargo management
- Cabin automation, energy supply and propulsion control
- Media redundandcy for ETHERNET communication

www.wago.com/ship

WE INNOVATE!

WAGO

EDITORIAL
FREE RESOURCES REVOLUTIONIZE THE MARKET

Dear Reader,

Let's be frank: For the majority of stakeholders in maritime construction and operations, the first two quarters of this year were less than optimal. The first half of 2016 was only notable because it holds the record for the lowest rates of new orders in years and the lowest shipping levels since 1981. These developments are generating strong pressure to consolidate shipping companies and shipyards – in all probability, this will affect suppliers within the next two years.

With the shipping industry stuck in the doldrums, is it time for despair? Absolutely not! Instead, this is an opportunity to change course and try different options. If you cannot maximize your resources, then you have the opportunity to look beyond the horizon and question the conventional methods. Now is not only the right time, but it is also necessary for the traditionally conservative maritime construction sector to embrace innovation. Several promising technologies, ideas and approaches are waiting to access the maritime sector: many technological "saviors," like the Internet of Things (IoT) and big data, have the potential to revolutionize the market if they could gain traction in the shipping industry.

Consider for a moment the vast quantities of data produced by drive units, alarm and monitoring systems alone, and how this could be used to reduce freight costs! Is it possible that our ideas might overturn traditional business models? Good! Our ideas will also bring new opportunities – the same way that the "power per hour" business model embraced by the engine manufacturers proved itself in aviation.

However, the overflowing bookings of cruise ship lines and tourism companies have encouraged us to focus on the opportunities presented by cruise ships. And regardless of whether "Maritime 4.0," or another less-autonomous system, will be incorporated into cruise ships and other marine applications, there's no doubt automation will play a significant role in the growth of all expanding maritime sectors. This is because automation is ultimately an essential component in both IoT and big data.

Seeing this, WAGO has entered the race with our flagship: the robust, high-performance PFC controller family, which carries all the necessary maritime certifications and approvals for use in hazardous areas. We believe that this family of controllers is ideal for future maritime developments, as these Linux©-based controllers not only represent a solid long-term investment, but they also provide integrated security mechanisms to prevent cybercrime. Security is an important prerequisite for ship-to-land communication, as well as for data recording, controlling, monitoring and networking on-board subsystems.

Take the time to read about what we can offer you today, and think about what we can create together.

May you find inspiration in your reading,

Norman Südekum

COVER STORY

Maritime 4.0 – Opportunities and Challenges

Under Maritime 4.0, big data will check in on large ships within commercial shipping. While Industry 4.0 continues to adopt specific forms for process automation, the first cyber-physical systems and cloud-based network structures, which will ultimately optimize maritime operations, still have a long way to go before they are ready for sea travel. It is primarily German maritime equipment suppliers that are convinced Maritime 4.0 will enable them to achieve enormous gains in commercial shipping efficiency. Is this merely a rosy outlook on the part of German industry? After all, they lead the global list of suppliers according to VDMA statistics. What does big data actually offer the maritime sector, and what new challenges are linked to these massive data sets?

CONTENTS

Modular control technology enables task-related growth.

SAFELY ON THE SHIP AND OFF AGAIN

TTS Marine from Gothenburg is widely regarded as the world's top provider of stern and bow ramps, movable car decks, door systems, freight elevators and gangways for ships and ferries. In conjunction with WAGO, the Swedish company is developing a new control system for cargo doors and gangways. The solution's open design is focused on maximum operating safety, and its modular structure will be ready for modernizations, updates and expansions.

Fast and safe: Ramps connect the ship to the quay.

Dock, unload, load, undock: Time is money in ferry travel and schedules are tight. To minimize loading times, RORO ferries rely on high-performance ramps from TTS Marine. The company provides the world's leading shipping fleets and shipyards with ship-side and land-based systems that provide the trouble-free loading operations of passengers, vehicles and goods. For the past three years, the Swedish subsidiary of Norway's TTS Marine AS Concern has relied on the WAGO-I/O-SYSTEM 750 for the central control system. The decision to use WAGO automation solutions followed comprehensive benchmarking in which the architecture of the control system, its quality, reliability and above all, its approval for use in the maritime sector played essential roles.

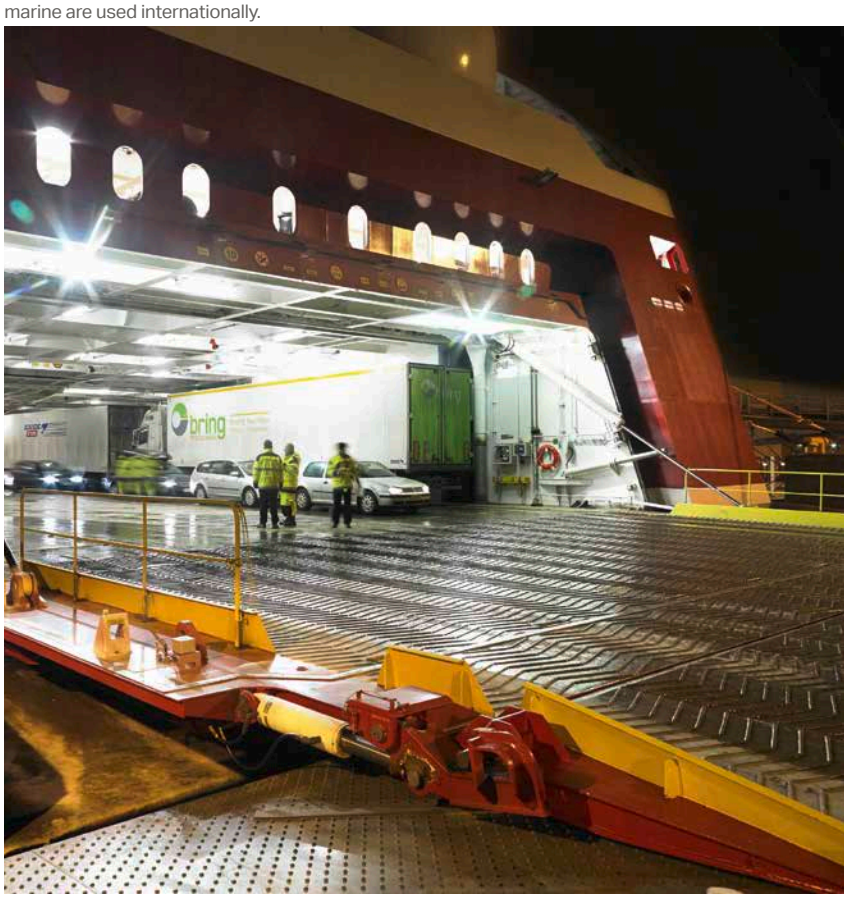
"We wanted a flexible control system that we could easily update later, and a vendor with a global presence," explains Tobias Ahlberg, Sales Manager at TTS Marine AS. "Our loading systems travel around the world and have an average service life of 25–30 years, so it is important that the products we use are also robust." And reliable, as Ahlberg adds, because failures or incidents cannot be allowed in the TTS systems – they are key points in ship security.

Step-by-step to the perfect solution

"When we considered WAGO's solutions, we quickly decided to incorporate them because they have several different certificates from

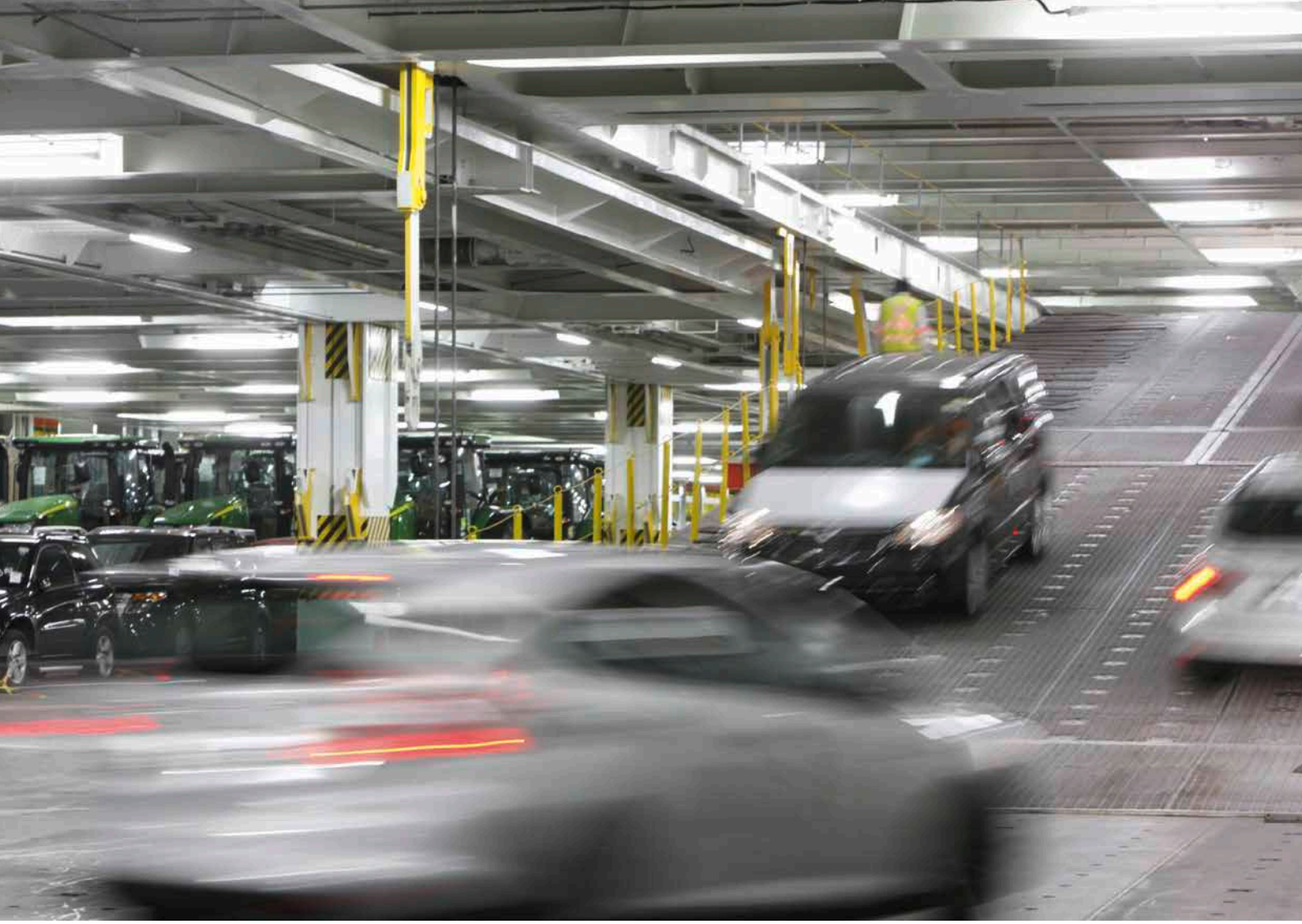
»We wanted a flexible control system that we could easily update later, and is backed by a vendor with a global presence«

Loading ramps from TTS marine are used internationally.



maritime standardization committees," explains Ahlberg. However, the Swedes did not want to convert the entire system at once, recalls Ahlberg. "And WAGO did not encourage us to do that, either."

In order to gain a mutual understanding of which components were best suited for each task, TTS Marine AS and WAGO initiated the technical system conversion in small increments. "Initially, we decided not to exchange all components for WAGO parts," states Martin Andersson, Design Engineer at TTS. Andersson is essentially responsible for everything: from developing electrical systems and component specification, on through to the writing of all programs for the programmable logic controllers, up to implementing acceptances. "Because there was absolutely no pressure to specify WAGO, we could concentrate



The interior of large RORO ferries can be compared to a multi-story parking garage.

on one aspect of the conversion at a time. We gradually expanded our inventory of WAGO components, including the TOPJOB®S Rail-Mounted Terminal Blocks and relays.

Conquering the maritime sector together

Ultimately, Andersson found that WAGO's system is an excellent fit for this type of approach, because it can be modularly expanded with ease, and can grow in unision with the customer's needs. "The open architecture of WAGO's controllers will allow us to integrate new components in the future via simple updates," states Andersson, who is excited that the Linux® based controllers can be freely programmed. They are also approved for control tasks on the bridge. This is vital as the need for resistance to interference and the demand for low interference emissions are particularly high, because failures of sensitive systems, like radio or navigation, must be safely prevented.

More than anything, Andersson values that, "WAGO knows what technology we need for developing control systems so that we can be just as successful with future projects as well." The collaboration of the last few years has opened new doors within the maritime industry for both companies.

TEXT FREDRIK HEDRÖD | TTS MARINE,
STEFAN WALL AND URBAN WASE | WAGO

PHOTO WAGO

Heeling systems from BESI, in Bremen, Germany keep ships stable on the water

1.5 KILOTONS ON THE HOOK – WHILE AFLOAT

The stability of mobile cranes on land is comparatively easy to ensure; a suitable counterweight is set based on the load, and a few minutes later, hydraulic supports extend several meters out for balance. However, it is commonplace that bulky and especially heavy loads are usually transported via water to their destinations. This raises the question as to how stability is ensured for onboard cranes – water is an unstable surface. Systems made of pumps, valves and ballast tanks hold cargo and commercial ships upright. Often called “heeling pumps,” these systems prevent listing of the ship’s body in the case of unevenly distributed loads. To control them, the specialists at BESI rely on PFC200 Controllers from WAGO, in combination with the I/O-SYSTEM 750 for Ex and Non-Ex areas.

MPV Heavy Lifters, like the BBC AMBER, are designed to transport bulky and heavy cargo. Heeling systems ensure stability.

Vessels which can be identified from afar are called “MPV Heavy Lifters” – as they have at least two large cranes on deck. These multi-purpose vessels are designed specifically for handling bulky and heavy cargo. According the Michael Borchers, Chief Technical Officer at BESI, their cargo has included rocket parts, turbines and even entire trains. In a current new construction project, the two cranes of one “MPV Heavy Lifter” can exceed more than 1,500 tons of lifting capacity. The heeling compensation systems on such ships have to be configured with corresponding abilities.

“The ship has compensation tanks distributed across the entire stern, which our system can quickly and precisely empty or fill with ballast water,” explains Borchers. This is the only way for the ship to maintain its balance during loading and unloading. Lifting the cargo and compensation by the pumps is performed in parallel. Consequently, the loading process can only move as fast as the heeling pumps are able to create weight compensation using ballast water – nevertheless, this should function as fast as possible to maintain short logistics times, according to Borchers.

However, the heeling compensation system must function reliably, above all, regardless of the time demands. “If one pump suddenly fails, then an entire ship can turn extremely fast,” states Borchers. By this, he means that the boat will capsize, or “turn turtle,” as it is colloquially known. “If the heeling system is interrupted, then the crane operator cannot react fast enough to lower the load at the correct time when threading heavy loads onto the deck.”

»We can use one system to operate in both areas, and that system is identical in function and programming, making our lives significantly easier.«

Dropping the load from the hook in an emergency is still possible from the quay, because the ship can use the quay itself as a counter weight; however, this is impossible from the sea-side, because the load would crash onto the ship.

Redundant industry standards

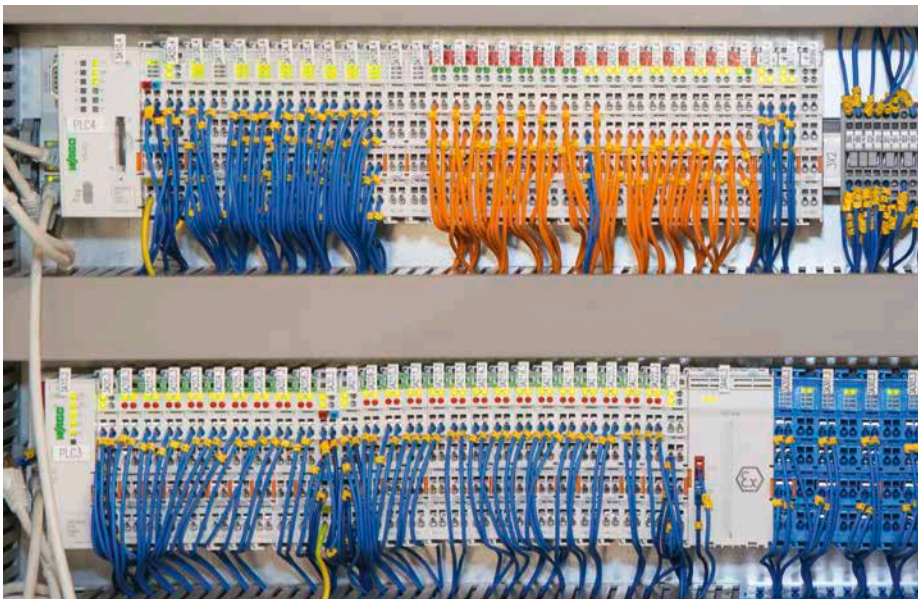
This is a scenario that explains why BESI relies on exceptionally reliable technology and equips its systems with sufficient redundancies. To control the "flow management" process, the company from Bremen uses WAGO PFC200 controllers – and in a redundant and spatially distributed function network configuration. BESI groups the heeling system, as well as the measurement, control and monitoring of tank contents under flow management. Due to the high fuel consumption in large commercial and container ships, fuel and ballast water must be regularly transferred during travel so that the ship retains a stable trim that's optimized for energy efficiency. When ships are in a harbor, the heeling systems can engage automatically on the basis of tilt sensors; at sea, the weight compensation between fuel and ballast water is executed manually. "No automation system is able to compensate for wave amplitudes 100 % of the time," explains Borchers, "because they constantly change and are unpredictable." Automatic operation of an electronic heeling compensation system is therefore forbidden while at sea. This is why cruise ships mechanically stabilize the body of the ship during heavy seas by extending stabilizing fins, which provide more inertia based on their resistance.

Michael Borchers is the Chief Technical Officer at BESI in Bremen.

One system also includes the Ex areas

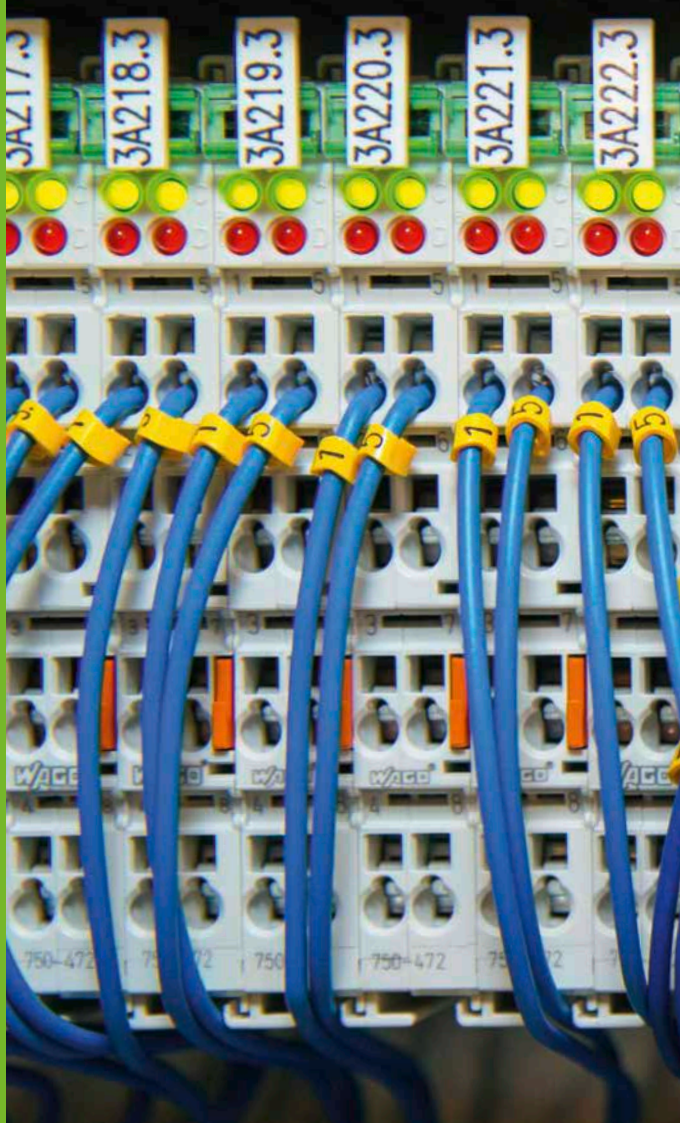
Tanks, pipelines, pumps, valve fittings: the flow management components from BESI penetrate cargo and commercial ships like a main artery running from stem to stern. Due to this fine-grained distribution, subsystems may also be installed in areas which fall under explosion protection, so BESI must use intrinsically safe components with Ex-i approvals in their automation. "Areas are classified depending on what is in the vicinity of the wiring installation, for example, fuel tanks," explains Borchers. Within the I/O-SYSTEM 750, WAGO offers a special variant that is visually distinguished from standard modules thanks to its blue housing. And while these blue Ex-i modules are designed for use in potentially explosive areas, their functionality matches that of the standard modules. This means that there is no difference in their programming. "We can program the control

Omitting Zener barriers enables a space-saving control cabinet design.



An Open Path for Networking

Using a combination of WAGO PFC200 Controllers and the I/O-SYSTEM 750, BESI installs an open network structure with distributed intelligence and decentralized I/O nodes in ships. This architecture provides a path for integrating other systems. Integration has already begun: the ventilation and air-conditioning systems have been linked to WAGO's control technology, which then functions as a data collector and ETHERNET gateway to bundle the information and forward it to the control level of the ship via ETHERNET. This means that the necessary control cabinets can be designed to be smaller and more flexible.



technology in both the Ex and Non-Ex areas with the software environment that we prefer, without having to establish complex links between different systems," according to Borchers. This means that BESI's engineers do not have to set up secondary or tertiary systems, and can consistently program all modules in one pass – and they can use the standardized languages from IEC 61131-3 (CODESYS) to do it. The advantage of this consistency for BESI is that the software engineers do not have to consider whether components of the heeling system are installed in a hazardous or non-hazardous area. Borchers emphasizes that, "We can use one system to operate in both areas, and that system is identical in function and programming, which makes our lives significantly easier." This is in addition to the fact that the WAGO components that are important for BESI have relevant international approvals for maritime use.

Extra space by omitting Zener barriers

The consistency of the WAGO I/O-SYSTEM 750 also saves time during wiring. Because the intrinsically safe sensors, like level gauges, or the actuators, such as valve relays, can connect directly from hazardous regions to the blue I/O modules, isolation amplifiers – which would otherwise be required – can be omitted. Isolation amplifiers are used in hazardous areas to limit the energy in the electrical circuit, essentially preventing ignition of the explosive atmosphere. Since BESI can omit the Zener barriers, there are not only fewer components in the switch cabinets, they also require less of the valuable onboard space. The Chief Technical Officer contrasts WAGO automation to a less elegant solution, "If we were to connect, for example, 50 devices from the Ex area to the I/O level, then I would need almost one entire control

cabinet just for the isolation amplifiers." Sufficient space is, however, never available – even in new construction – at least for technical equipment. Borchers understands that, even though the level of automation is increasing, space is only grudgingly provided for it. Ultimately, ship designs are optimized to devote as much free space as possible for cargo. "That is why compact automation systems with high degrees of integration are so important."

TEXT JÖRG SCHOMACKER | WAGO

PHOTO WAGO

Visualization of the heeling system which allow ships to be optimally trimmed in the water.

»ANYONE WHO TALKS ABOUT MARITIME 4.0 HAS TO DO THEIR HOMEWORK«

Interview with Professor Karl-Heinz Niemann,
expert in IT security at the University of Hannover.

In the film, "Tomorrow Never Dies", terrorists divert a military ship from its course by manipulating the GPS signals. What was part of the fantasy world of British filmmakers in 1997 – the theatrical release date for the eighteenth James Bond movie – is a real threat a mere 20 years later. "GPS spoofing,"as it is known to the experts, is real, and researchers from the University of Texas provided impressive proof in 2013 when they diverted an $80 million dollar luxury yacht from its course without its crew noticing. What is wrong with IT security in the maritime industry? Ship builders, system integrators and shipping companies are enthusiastic about the new opportunities that Maritime 4.0 offers. To find out if the sector ready for this, and what still needs to be done, we spoke with Professor Karl-Heinz Niemann from the University of Hannover.

The device, which the Texas researchers used to trick the navigation system of a luxury yacht, was about as large as a briefcase. The 65-meter long yacht had two GPS receivers, and was still spoofed. The Texans simply generated a GPS signal and increased the signal strength until the receivers on board switched to the transmitter. What does this scenario mean for you as an expert in IT security?

» That there is much more work to be done. There is still a lot of ground to make up in IT security in automation. While everyone else is thinking ahead to Industry 4.0, we still have to do the homework assigned for Industry 3.0 – existing systems need to be toughened up. «

You are talking about automation technology. In your opinion, is there a difference between industrial automation and the automation aboard ships?

» I think that the maritime sector is set up just as well, or poorly, as any other sector when it comes to IT security. Your example of the luxury yacht finds many parallels in other sectors. Off the cuff, I can think of a blast furnace, which was idled by a cyberattack. Blast furnaces are process technology systems that usually run for several years without any interruptions. The externally initiated stoppage ultimately caused a complete loss. The effects of cybercrime are serious everywhere they appear. To this end, I see no sector differences in the current level of implementation of IT security – there is also no difference in that it's vital to deal with the topic and the risks that arise from it. «

What can companies do to ensure IT security? What homework would you assign?

» It is imperative that operators prevent attackers from simply linking into a network. They should, however, consider that not all external connections are bad; they simply have to secure them

correctly. In this context, it's undoubtedly a question of settings. «

What do you mean by that?

» There are always people who want to explain to you that their system has no connection to the rest of the world and that IT security thus has no relevance for them. Do not believe them. There is always a connection somewhere. The more comprehensive homework, which we have to complete in my opinion, is establishing a sensitivity for the relevance of IT security for different parties in the maritime industry. At what points in daily life do these professionals come into contact with security breaches, and which do they generate unintentionally. «

Do you mean, for example, the common practice on container ships, where a cargo master enters his or her cargo data into the ship's system using a flash drive written on land?

» That is the exact type of case. Flash drives should never be used. Despite this, the practice is routine, even though it is an obvious weak point in security – at least if there is no quarantine area for imported data. «

Is IT security a problem that only the ship's crew should deal with? Who is responsible, in your opinion?

» The people in operations on board are, without doubt, potential weak points for any IT installed on board; unfortunately, they usually have no ability to recognize the sophisticated attacks on their systems. Therefore, it is important that shipping companies establish processes and methods, and then formulate a commitment to managing IT security. With regard to the container ship in your example, a protocol would be established for the next time that someone stands on the bridge with a flash drive in hand. «

Then you see management as responsible.

» True. In terms of IT security, we deal less in terms of methods than with a corporate strategy which trickles down from management – and everyone has to be prepared to expend some effort on this. It is imperative to define authorizations, monitor accesses and establish emergency plans in the event of a complete data loss. It no longer suffices to lock switch cabinets against unauthorized access using a square key. What we need is defense in depth, like a knight's castle. First, the fence protects the facility property, then there are access limitations on specific rooms, followed by regulations regarding specific cabinets. «

A castle is, however, quite stationary. So you see the need for special measures regarding ships?

» Compared to land-based applications, there are indeed new challenges and points of threat for ships – particularly due to the additional electronics that are on board. These include, for example, navigation, tracking and collision warning systems. This is equipment that is necessary for the ship's safety. In addition, no ship is an island, regardless of what anyone thinks. Indeed, many of these additional systems establish external connections and thus offer attack points for manipulation. Just like the scenario you described at the beginning of our discussion. «

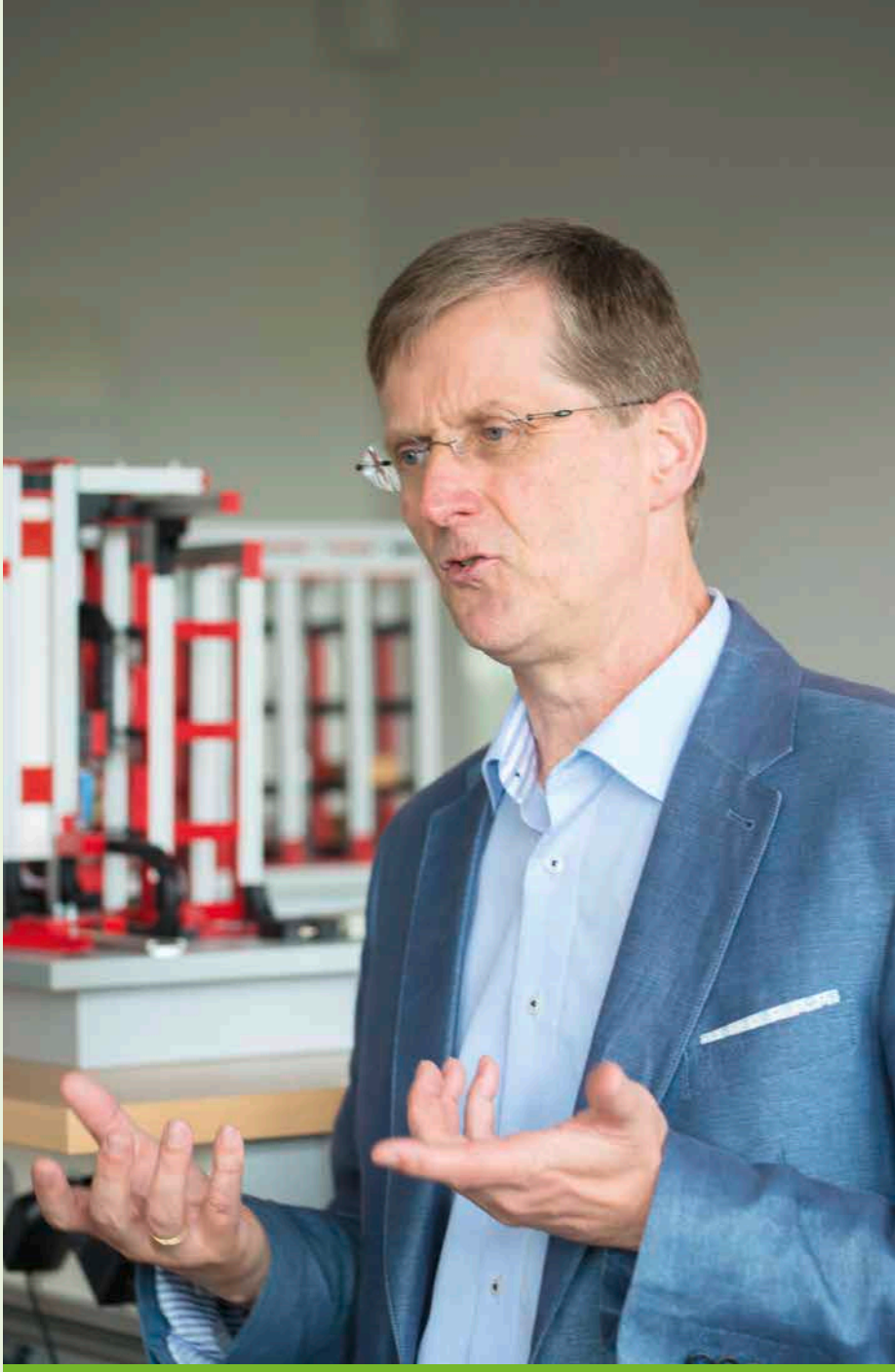
This sounds as if the advancing digitization on board is presenting a host of new problems for IT security.

» That is also true! Industry 4.0 is establishing additional communication links, because companies are configuring their data flows to be consistent. Due to the horizontal and vertical integration, extant isolation concepts as a component of in-depth defense, are no longer sufficient. The new demand is for "IT Security by Design." This is when functions of IT security are integrated from the start into the configuration of a layer-based security architecture in the controllers. «

Does this path impact approvals for maritime technology? Do the classification agencies need to consider IT security in their certifications based on the explosive nature of the problems you have described?

» I am convinced that those agencies are already working on this topic – especially as there is a need to catch up with regard to IT security in the maritime sector. As I said, to create a functional defense in depth, we have to complete our 3.0 homework -- for me, this is a compelling prerequisite in order to implement the ideas that are under development for Maritime 4.0. «

Professor Niemann, thank you for the conversation.



Professor Niemann researches and teaches in the Department of Electrical Engineering and Information Technology at the University of Hannover. He represents the academic fields of process information and automation technology, as well as lectures on integrated automation, industrial bus systems, process interfaces and energy efficiency.

His core research focuses on IT security in production systems, particularly in the context of Industry 4.0.

In addition, Professor Niemann leads a think tank on IT security at the SME 4.0 competence center for Lower Saxony and Bremen (http://mitunsdigital.de), and is active in various working groups for the Profibus Users Organization and the Association of German Engineers.


KELVIN HUGHES

BIG DATA FOR BIG SHIPS

Maritime 4.0 – Opportunities and Challenges

Under Maritime 4.0, big data will check in on large ships within commercial shipping. While Industry 4.0 continues to adopt specific forms for process automation, the first cyber-physical systems and cloud-based network structures, which will ultimately optimize maritime operations, still have a long way to go before they are ready for sea travel. It is primarily German maritime equipment suppliers that are convinced Maritime 4.0 will enable them to achieve enormous gains in commercial shipping efficiency. Is this merely a rosy outlook on the part of German industry? After all, they lead the global list of suppliers according to VDMA statistics. What does big data actually offer the maritime sector, and what new challenges are linked to these massive data sets?

It is said that you are in God's hands when you are on the high seas and in court. This adage has lost nothing of its significance in the 21st century. There is always an amount of uncertainty in the courtroom as to how the legal situation will be resolved, and similar uncertainties prevail on the high seas. Even when ships are following defined routes, they remain exposed to the forces of nature, the reliability of the technology or even pirates. While some discuss redundancies and reliability, others contemplate autonomous ships that could alleviate the risk of pirates, since pirates are more interested in the ransom they can extort for hostages than they are in the cargo itself. Will driverless transport systems, which are already used for logistics on land, change the image of the global seas?

Sector experts are convinced of the enormous potential of big data

Remote-controlled cargo ships on international waters are currently only dreams; however, they are approaching reality as automation is increasingly incorporated into ship designs and enables that which was inconceivable a few years ago. Examples include the networking of subsystems, which allows the linking of systems for finer tuning and significantly more efficiency; or remote access from land to read ship data or engage in the ship's operation to control specific functions. Whether or not people remain on board, sector experts like Hauke Schlegel, director of the VDMA

Today, large-format monitors, rather than the view from the bridge, direct commercial and passenger ships.

"Marine Equipment and Systems" department, are convinced that, "an unimaginable potential is concealed" in big data. The maritime sector, with the German maritime economy as the leading global supplier, stands to profit from big data – a fact that pleases Schlegel immensely. While it appears that in the foreseeable future China, Japan and Korea will close shipyards due to overcapacity, the German mechanical engineers and system designers are traveling in calmer waters. And while their future may not be rosy, it appears to be stable. In 2016, sales are expected to exceed 12 billion euros. And now the digital revolution offers further opportunity? What can ships and shipping actually get from this new technology? Let us examine efficiency, environmental protection and security in the shipping industry more closely.

Cost reductions due to unmanned shipping

In general, cargo services suffer daily from high and ever-increasing cost pressures. The reason for this is simple: there is too much available shipping tonnage underway on the oceans – a result of speculation during the boom years between 2004 and 2009. Overcapacity and ongoing price erosion are the end result. Transport services are therefore attempting to retain their economic viability by reducing costs. And anywhere cost reductions are discussed, labor costs are always

under consideration – even for shipping companies. For them, it specifically means a choice between quantity or quality. Companies either reduce the crew numbers on board, or the rely on a crew with lower electro-technical qualifications and correspondingly lower rates of pay. Both scenarios can be realized by implementing automation. Automated systems are capable of taking over many long-term tasks that were previously performed by humans. They also allow for remote functionality, which enables land-based experts to read a ship's data in order to oversee maintenance people at sea.

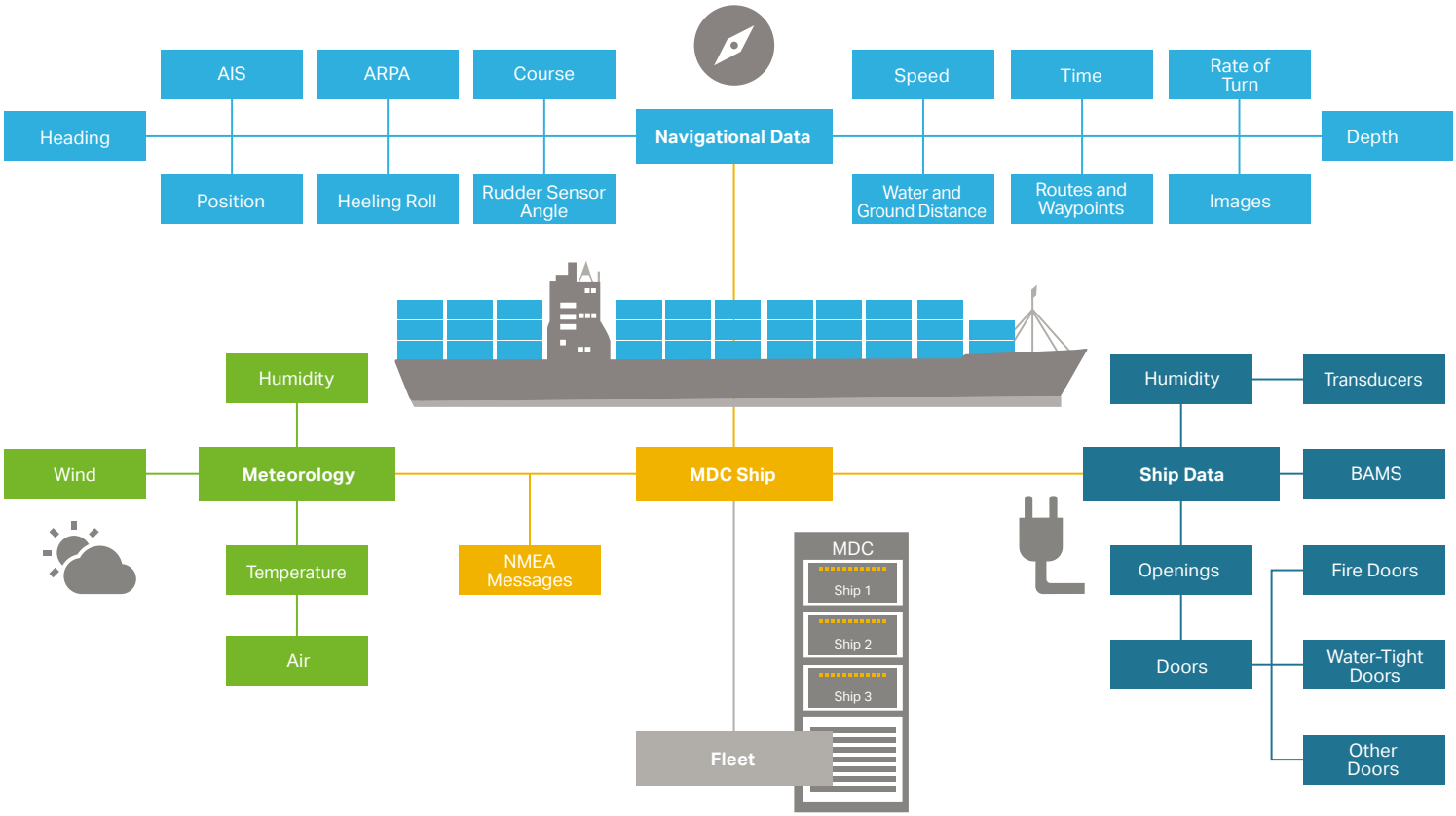
If the crew numbers on board fell to zero, there would be profitable benefit: small subsystems, such as, wastewater treatment systems, climate control and desalinization plants, would be eliminated if a ship were autonomously guided. Transport services could save approximately 10 % in fuel costs alone if they did not have to offer the amenities required to feed, house and entertain a crew.

Allocating costs according to their sources

With or without a crew: On a ship, there are many applications that could be operated more efficiently, aside from crew amenities. Measuring, evaluating, formulating remedies -- Maritime 4.0 holds tremendous promise for these specific areas. Consider building management for a moment: By employing data recording and networking, consumption and costs can be determined and optimized down to the individual room level. Comparable measurements do not occur on container ships. However, different containers contribute to different levels of transportation costs. This is due to the fact that, despite the standardized dimensions of a container, all cargo is not the same, which is abundantly clear when one considers "reefers."

Reefer is the term used for refrigerated containers, which must either be cooled using the ship-side cargo cooling system or have their own

From Oslo to Frederikshavn: in the narrow fjords of Norway, land-to-ship communication remains simple.



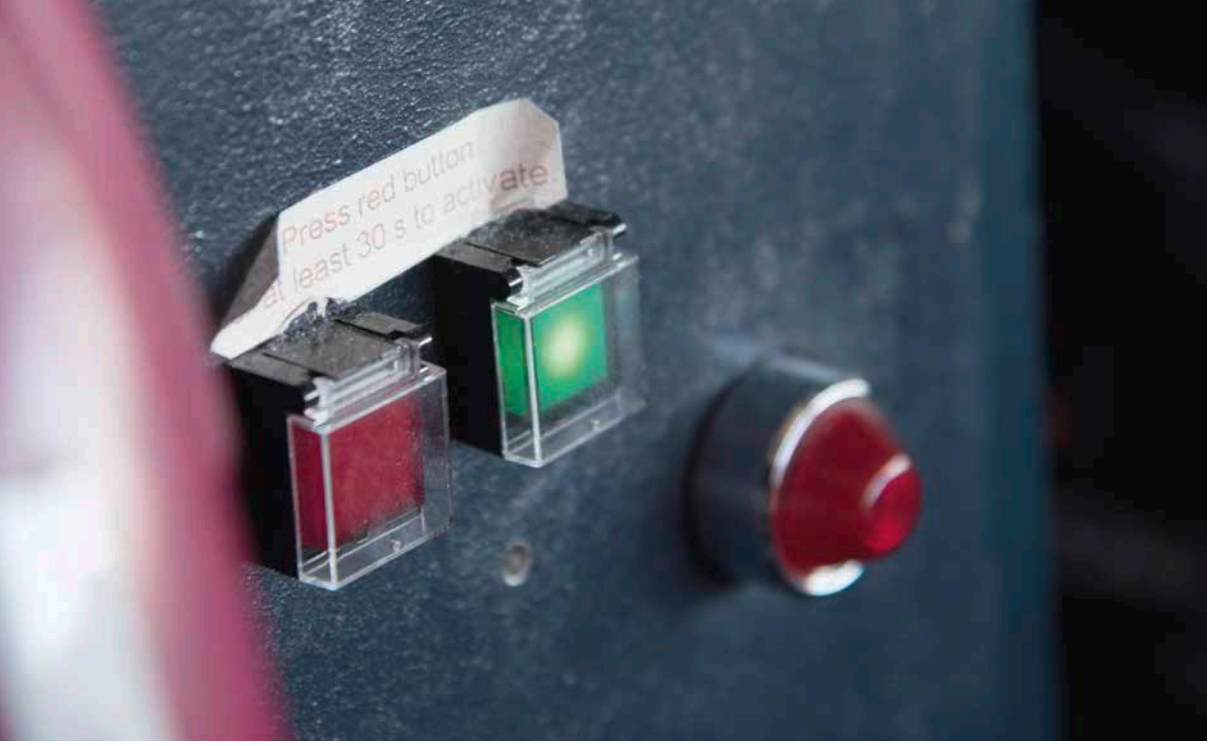
Everything is tightly linked. The chart illustrates how important big data and close-knit networks are for modern shipping operations.

cooling systems. These, in turn, draw energy from the onboard network. In both cases, the cooling directly impacts fuel consumption on the ship, because the generators have to provide electrical energy and the main engine consequently demands more output. It is obvious that refrigerated containers are responsible for higher shipping costs compared to other containers. In daily practice, however, infrastructure costs are uniformly distributed among all containers loaded on a ship. If integrative network technology could determine how high the energy demands of a reefer actually are, then the shipping costs could be allocated according to the source and individually calculated. Different cargo tariffs could be defined for different routes, because travel in the vicinity of the equator requires more electricity for cooling than cooler regions. Technologically, such tasks could be solved without a problem by currently available technology. WAGO's PFC200 Controller offers, for example, storage potential for monitoring data outside of the cloud in parallel to its own processor performance. Also, this monitoring is already required in order to document the uninterrupted cooling chain and thus the operational safety of a reefer.

Route planning instead of full steam across the ocean

Another example of the advantages that result from closer data networking can be measured in fuel consumption. If routes are plotted around low-pressure zones, for example, fuel is saved. Consequently, it is advantageous to evaluate weather data with more than safety in mind.

Additional processing of harbor information follows a similar path. Prof. Holger Watter, Dr.-Ing and president of the Technical University of Flensburg, recently enquired, "What is the use of traveling at full speed to a harbor, if I have to wait for a docking position?" When considering fuel consumption, it is substantially more efficient to adjust the traveling



Inconspicuous placement, but a serious outcome: if both buttons are pressed in case of a pirate attack, a comprehensive crisis management program will run in the background.

speed so that a cargo or container ship arrives punctually in a harbor that is logistically prepared to handle its freight.

Experts have estimated the monetary rewards that could result from optimizing fuel consumption and idle times to be so great that the EU has launched the "Sea Traffic Management" project. This initiative seeks to precisely synchronize shipping operations using communication, networking and big data. The basic premise of the project is that ships' data, which can be coordinated with one another, is provided in the cloud where other ships can access it. This opens the path for safely passing one another along shipping routes, and arriving punctually in harbors in a sequence.
The harbor operators would also profit from synchronized shipping. They could better prepare for the arrival of ships, which would thus lead to significantly less logistics space for intermediate storage and less capacity for transporting goods. Semis and trains wouldn't have to remain in long queues waiting for specific ships. Agreements of this type would pay off financially and environmentally. "In spite of this, it is not yet common in shipping," opines Proffessor Watter, who clarifies that in this context, it is still more important for ship operators to correctly interpret various scenarios. Watter wants ships' crews, "to be able to correctly read data and determine the correct measures," by which he means that automation systems need good human-machine interfaces.

Maritime 4.0 requires greater IT security

In this context, ships' bridges have long served as automation control centers where information flows together. This includes navigation, communication and cargo information, as well as administrative data, like registration documents and cargo declarations. With electronic maps and automated identification systems (AIS), it is apparent on the bridge that digitalization is increasing on the high seas. The trend speaks loudly, and the described potentials agree: big data for large ships? It would certainly be worth it! However, cost reductions, environmental protection and increased efficiency also have their price: significantly increased demands on IT security. The risk of data abuse and cybercrime increases alongside the digitization, networking and increasing land-to-ship communication. Anyone who talks about Maritime 4.0, has to discuss IT security – and this means much more than securing a ship against cyberattack, it also involves operational safety of the very ship. It is imperative, in order to protect ship, crew and the environment with suitable technologies, that data transmitted between land and sea are reliably encrypted. An example: access points and access times are regulated, or controllers are used that include "IT security by design" and can also function as intermediate storage if the connection between land and sea is severed for any reason.

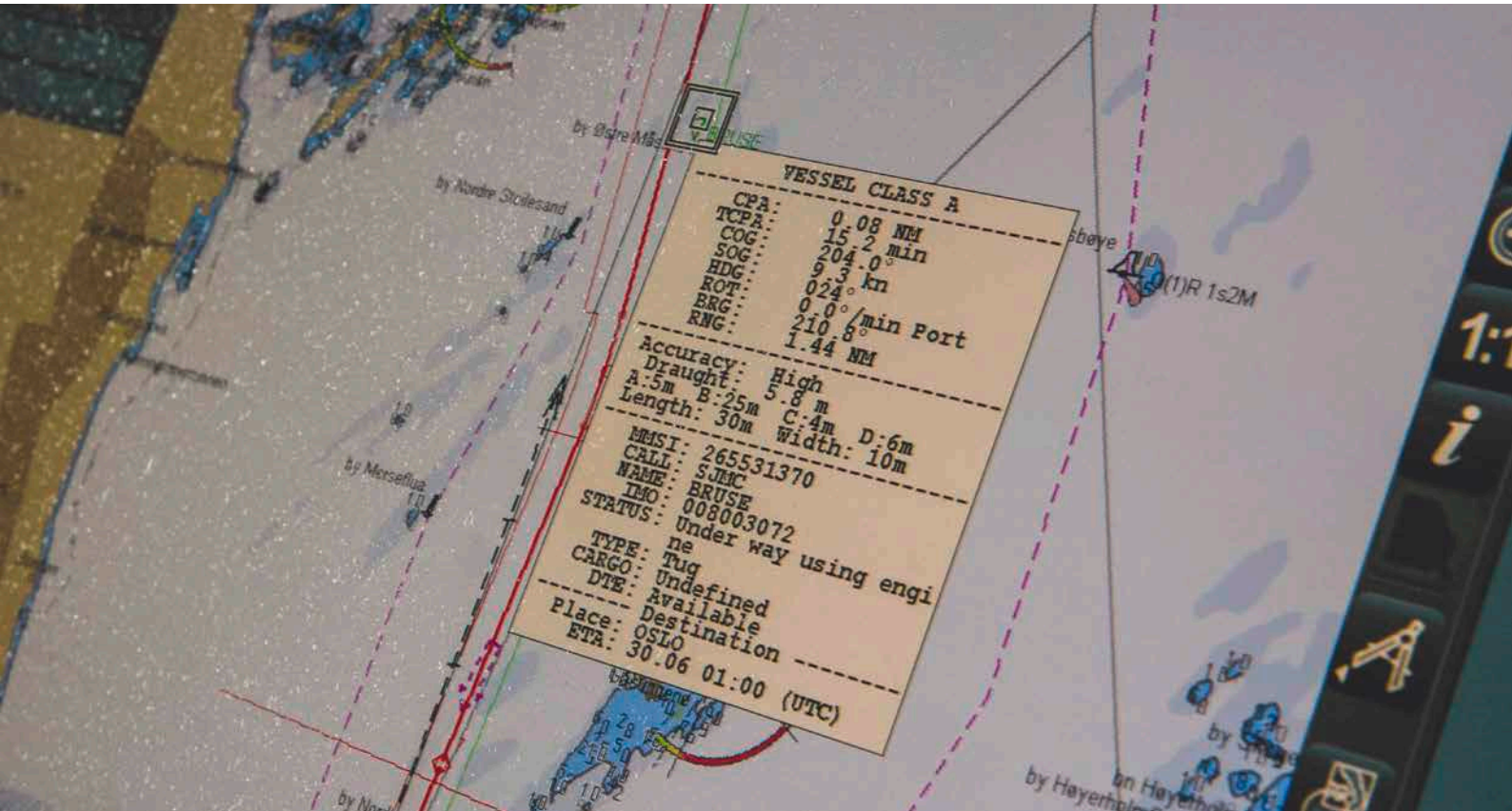
IT Security: an ongoing competition

In view of the serious effects caused by maritime accidents, it is surprising in this context that the current version of the IT Security Act does not include shipping operations among its critical infrastructures, which is a stark contrast to energy and water supply on land. Actually, IT security should be considered a "competition," which occurs between producers, hackers and operators. In order to flexibly react to new threats, an open operating system is the first choice because open-source products are not dependent on just one manufacturer. Rather, open systems are simultaneously used by many programmers who recognize security gaps more quickly and collaborate on improvements. Therefore, WAGO's PFC family is based on Linux® with real-time expansion, which provides common functions for IT security as defaults, regardless of manufacturer, and offers future possibilities for expansion.

TEXT THORSTEN SIENK, NORMAN SÜDEKUM, AND EVA BANHOLZER | WAGO

PHOTO THORSTEN SIENK | WAGO

The AIS provides information about key data from other ships on the route.

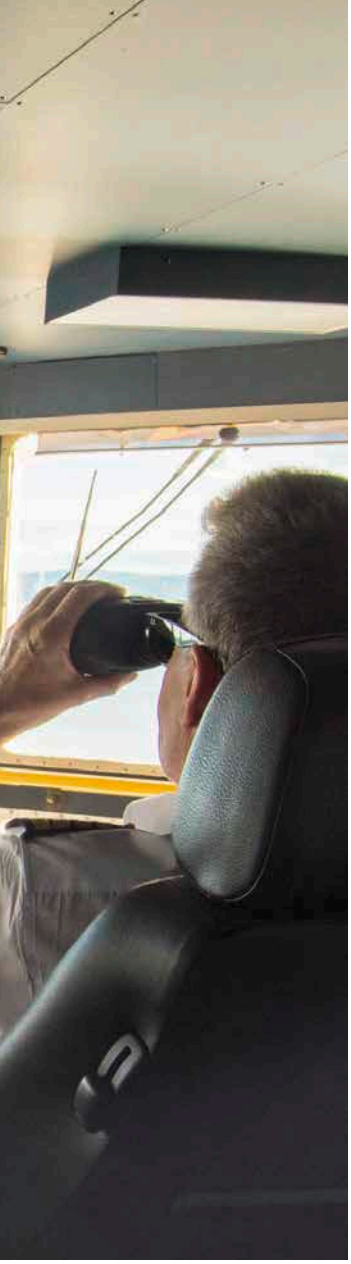


Regardless of the digitization level, the binoculars are always close at hand on the bridge.

IT security on ships

SAFELY ON COURSE IN THE BINARY SEA

With increased digitization and networking aboard ships, the risk for data abuse and cybercrime also increases. Anyone considering the possibilities of Maritime 4.0 must also consider the increased requirements for IT security – and more importantly, find suitable solutions for implementing it.



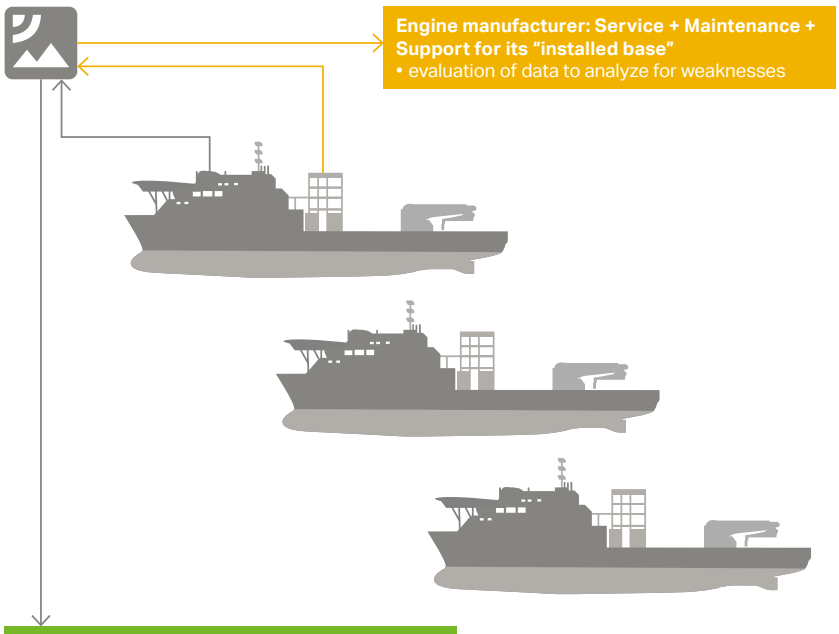
A ship's various intelligent subsystems ensure problem-free operation: from tank and ballast water management through drive control up to alarm and monitoring systems. They all function using industrial automation technology. At many points, advantages result from networking these subsystems – for example, when ship operations can run with greater resource- or energy efficiency.

The exchange of sensitive data also increases everywhere systems are networked. And yet this is not enough. In comparison to applications on land, ships have additional electronics like navigation, tracking and collision warning systems. They serve the safety of the ship; however, they also represent an additional threat, primarily because they not only increase the level of onboard networking, but also establish external connections. For these connections, Internet-based network technologies or mobile services are seeing increased use. And these communication paths provide access points for manipulation – particularly at the points between the ship and land.

Access to or the reading of sensitive data is a comparatively less important problem when compared with the effects caused by hackers introducing malware into the control systems of ships or drilling rigs, altering coordinates, or accessing a vessel's security-relevant subsystems. These acts don't just endanger IT security, they also impede functional safety, and ultimately the crew's safety. This is precisely why recommendations regarding IT security have increased along with the level of digitization and networking. The American Bureau of Shipping, the Baltic and International Maritime Council, Lloyd's Register Group, the UK Chamber of Shipping, and the European Union Agency for Network and Information Society have all published guidelines regarding IT security aboard ships. In general, they define processes, model approaches or technical measures for implementing IT security; for the most part, these align with the guidelines for automation technology.

As Reliable as the Tides

Long, unplanned idle times can be prevented in many situations by using technology with a high level of reliability and fast delivery of replacement parts. Although the business of replacement parts is of interest to BESI – and likewise other OEMs – the Bremen company places a great importance on the international availability of replacement parts. "If a ship owner is stuck somewhere off the coast of Africa and needs an I/O module from us, then every hour counts. If we have to fly to Africa ourselves, then our service-related costs would quickly outstrip profitability." In this case, it is substantially more logical to use standardized industrial products with a high market penetration, meaning that they can also be purchased on site. "No matter how profitable the replacement part business is, the systems have to start running again fast," agrees Michael Borchers, Chief Technical Officer at BESI. According to Borchers, the daily charter costs for ships the size of the CSCL Indian Ocean, which has a capacity of 19,000 standard 20-foot long containers, can exeed $40,000.



The reasons for remote access vary greatly between shipping companies and OEMs.

"IT by design" instead of "defense in depth"

There also seems to be agreement that additional communication relations are generated by Industry 4.0 or Maritime 4.0, providing an increasing potential for cyberattacks. What is more important is that isolation concepts are reaching their limits. This is because of the opportunities provided by networking, which both increases the frequency of outside access and allows much deeper penetration into the ship's automation systems than before. There is a completely transparent reason for this: by using remote solutions, shipping companies obtain the possibility for remote diagnosis of their ships, which allows them to optimize their fleets and remarket the recorded data. In addition, they can reduce labor costs if fewer personnel or a less qualified crew is used that can receive support from engineers on land for repairs. And finally, better networking of shipping companies and harbor unions improves the logistics at the docks and reduces fuel consumption for the ships. Simply preventing external access cannot be a solution for fixing security on ships. Defense in depth, however, which has previously been considered as state of the art, will soon become insufficient – even if it starts with access limitations, network segmentations and monitoring systems on the various levels of ship automation.
Security concepts are increasingly required that always function, regardless of the time or remote access point. The new demand is for "IT Security by Design," that is, functions of IT security that are integrated from the start into the configuration of a layer-based security architecture in the controllers.

"IT security made by WAGO" Minimize Risks – Repel Attacks

Tools in the PFC Family:

Security services

- Password protection, User administration
- SSL/TLS-1.2 encryption
- SSH – Secure shell client
- VPN (OpenVPN, IPsec)
- Firewall
- MAC whitelist

Integrated Linux® services

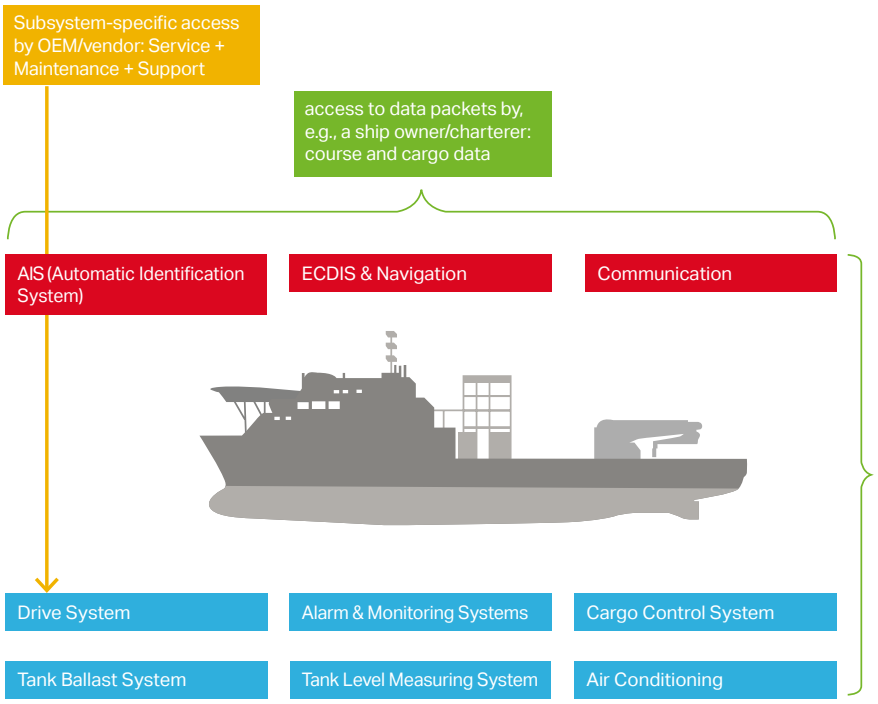
- Syslog
- SD card reader
- FTP, SFTP, SCP
- Optional: Rsync
- Optional: Virus scanner
- Optional: Fail2Ban

From the PLC to the cloud – securing the paths that data travels

Such technical possibilities already exist and are capable of closing gaps in security. For example, a reliable means of communication is the establishment of a virtual private network (VPN), based on OpenVPN and using SSL/TLS connections (Secure Sockets Layer, Transport Layer Security). These connections enable the transmission of encrypted data, even over wireless communication systems. WAGO establishes such VPN tunnels using OpenVPN or IPsec directly from the WAGO PFC200 Controller. The WAGO controller additionally records all relevant measurement and control data, encrypts it directly in the controller using SSL encryption and transmits the data as VPN. This means that no additional VPN tunnels have to be established by modems or routers, and, what may be more decisive, the line between the controller and modem is then directly encrypted as well.

TEXT NORMAN SÜDEKUM AND EVA BANHOLZER | WAGO

PHOTO WAGO



Typical systems on ships that use big data and have undergone increasing levels of networking.

Which switches provide which tools?

Security services

- Password protection, User administration
- SSL/TLS-1.2 encryption
- Bandwidth limitation
- Bandwidth monitoring
- MAC whitelist
- ARP inspection
- DHCP Snooping
- L2/L3 Access Control List
- 802.1X Port access control

Integrated services

- Log, Alarm (by email)
- SNMP v2, v3
- Backup & Restore settings

»WE ARE DOING TOO LITTLE WITH THE DATA WE COLLECT«

Interview with Andrea Grün, Senior Principal Engineer for Electrical Systems and Automation DVN GL

What would happen if there were a chance to deeply access the engine room level – even from afar? Completely new challenges for approvals and certification of components and systems have arisen for international classifying agencies because of this scenario. Agencies, like the Norwegian-German DNV GL must factor IT security for operational safety on board ships into their certifications. As Andrea Grün, Senior Principal Engineer for Electrical Systems and Automation DVN GL in Hamburg explains, remote access is the primary cause for concern.

In mechanical engineering, remote connections for remote maintenance, system optimization or streamlined maintenance cannot be wished away. From the standpoint of a classification agency, what do you consider important in network connections from ship to land?

» System manufacturers want to equip their systems with remote access because this eases maintenance and service. We have established corresponding guidelines for such tasks. We have considered, for example, that there should be no updates while a ship is underway. We are not the police; however, we do prohibit access from land to the systems when the ship is at sea. «

Why? In factory automation, optimization occurs during production.

» We simply cannot accept the risk. That is, the risk of setting systems to undefined states because the data have been incorrectly or incompletely transmitted. Imagine that this happens on the high seas beyond sight of land. There aren't any service technicians who can reach you. These types of activities belong in harbors, and not on the international shipping lanes. Therefore, we have also determined that systems must be capable of returning to the old software status after an update. Regulating remote access thus provides operational safety, from our point of view, and guiding these

Andrea Grün has worked for DNV GL for more than 25 years and is the Senior Principal Engineer for Automation in the Head Office of the Hamburg Maritime. The DNV GL is the leading global classification agency for the maritime industry. They promote safety in the global maritime sector and work to improve ship performance, energy efficiency and environmental compatibility.

Grün is the technical project manager for complex networks and innovative software systems, and is an expert and auditor for the MED (Maritime Equipment Directive) and ISO 9001, with an emphasis on the maritime sector.
She contributes significantly to the development of new regulations and international standards in automation and for the approval of software-based systems in the maritime sector.

initiatives is essentially why classification agencies like DNV GL exist. «

How would this type of remote access, which conforms to regulation, look aboard a ship?

» As I mentioned, connections are only permissible in harbors. As soon as the work is completed, the crew must verify that everything is in order and resume control of their ship – that is, sever the connection. There are clearly controlled hand-off and acceptance procedures. «

How does the crew deal with this type of remote access?

» Frankly, most crews are not really happy about this technology, but then, they were not pleased about the introduction of ship data recorders, VDRs, either.«

What is the crew afraid of?

» It's about control, or, more accurately, the loss of control, however you want to look at it. There are shipping companies that want remote access in order to maintain control during the ship's travel via network. It's one thing to read data, it's quite another to engage with the controls. «

The DNV GL is headquartered in the German harbor city of Hamburg.

How can a classifcation agency anticipate what is planned with remote access?

» During certification, we always ask about specific topics. Let's take an alarm system as an example, which now has diverse functions as an integrated automation-, alarm-, monitoring- and control system, and is extremely powerful. These systems can just as easily control as monitor, and they are connected to the entire automation network. During the approval process, we are given descriptions of these systems that list all of the functions. If we come across the designation "remote access" in the documentation, we investigate further with the company. In general, we then request further specifications and ask them to demonstrate why the function is necessary. «

What answers do you get?

» That depends completely on who answers the question. Shipping companies use remote access to call up travel, consumption or cargo data, for example, to optimize their logistics chain. Machine manufacturers or system designers require remote access to diagnose their subsystems, which also includes service. «

Are these the type of answers you can live with?

» It is what it is. Even if we consider remote access to be just as critical to the crew's safety on board as it is to IT security, we must also accept the fact that there are also inherently positive aspects of the technology. The systems aboard ships are becoming more complex – this trend can be compared with the automotive industry, where this has been the case for years. The proportion of IT and automation in vehicles has steadily risen. That's why repair shops are no longer looking for talented mechanics -- instead, they need mechatronics technicians who can operate a laptop and read the onboard computer. The career track of sailors is currently changing in the same way. The demands for technical qualifications are growing at a relatively low rate of pay. Support from land is becoming increasingly necessary under these conditions. In this respect, the answers as to "why" are completely comprehensible. «

There is currently a generational change playing out in the maritime sector – does this provide fertile ground for Maritime 4.0?

» Absolutely! The inspectors in the shipping companies are younger, on average, and they are natural technophiles. For them, there are attractive possibilities stemming from the rise of Maritime 4.0. Just consider what could arise simply from the ability to gather fleet-wide data and compare it. The person who knows, which ships in a fleet run best and the reasons behind this, can optimize the entire operation – from fleet fuel consumption up to an exceptionally well-tuned logistics chain. «

Where are we going, in your opinion?

» Basically, I think that we can use the technological developments within the context of Maritime 4.0 to leverage potentials: for example, to implement a perfectly tuned logistics system, for container tracking, for monitoring cooling chains or conserving resources and increasing energy efficiency. We just certified a network in which a ship's quarters function together with the fire alarm system. Such combinations are interesting – especially for cruise ships, because they provide cost savings. However, the demands on IT security will grow in conjunction with Maritime 4.0. From the perspective of IT security, it is extremely important in the case that I just mentioned that no passenger can penetrate the fire alarm system through the cabin network. «

What needs to be done?

» What still needs to be completed, in my opinion, is the targeted evaluation of data that we currently gather from everywhere. My impression is that we create immense mountains of data, and still do too little with what we collect. As this relates to remote access, which we have discussed in detail here, we need logical rules and technologies that support IT security. I'm thinking of an architecture or an authorization concept – for example, defined remote access at specific intervals that the crew would determine. As well as technologies, which would also protect the infrastructure if various points are accessed externally and extend from the control center to the depths of the engine room. «

Ms. Grün, thank you for the conversation.

The "Adèle" has been lauded as one of the most beautiful gems in the international yacht market.

Renovations for traditional sailboats

"ADÈLE" SAILS USING MODERN AUTOMATION

Classical lines, with carbon fiber rigging and a fast hull: "Adèle," built in 2005 by the Dutch Vitters shipyard is still a looker – even after ten years on the world's oceans. Swede, Jan-Erik Osterlund, commissioned the 55-meter-long yacht with an aluminum hull so that he could spend two years sailing around the world. Since then, "Adèle" has found a new owner – and a completely new automation technology based on the WAGO-I/O-SYSTEM 750. The Royal Huisman shipyard in the Netherlands won the contract for the refit.

Anyone who travels by megayacht generally has plenty of time. However, it also holds true that no owner wants to spend time stuck in a harbor because of malfunctions, no matter how well-appointed a marina's megayacht facilities may be. Therefore, owners invest in high reliability and correspondingly redundantly structured automation technology. This was the case during the refit of the 150-foot "Adèle."

Modern control and communication technology had been installed during the original construction of the two-masted yacht. At that time, data connection occurred via DeviceNet. The core of the automation system was formed by three controllers for communication, monitoring and lighting control. However, the multiple mutual dependencies between the subsystems increased malfunctions. So "Adèle" was never able to fulfill the high expectations of her owner.

Available due to decentralized automation architecture

A comprehensive retrofit ten years later sought to solve this problem. During her sojourn in the shipyard between 2015 and 2016, the yacht specialists at the Royal Huisman yard replaced "Adèle's" batteries for the electrical supply, updated the lighting to LED technology, modernized the HVAC technology, and expanded the drive train – including a general overhaul of the generator. The Dutch also replaced the old control technology with the WAGO-I/O-SYSTEM 750 and DeviceNet with ETHERNET. Because the network aboard "Adèle" must always work – even if individual components fail or the communication link is interrupted, Royal Huisman decided to integrate automation technology that is equipped with redundant Ethernet networks for communication.

The automation and communication technology from WAGO was selected because it has all of the necessary approvals for maritime use. In this specific case, certification was required from the largest global classification agency, DNV GL.

Her interior provides greater ambiance than a luxury hotel.

The drive to use internationally certified components reflects Royal Huisman's interest in complying with global standards in new construction and retrofits. And because ships like "Adèle" travel around the world, "a reliable and fast replacement part supply chain was relevant" for Royal Huisman, in addition to the certification, according to Pascal Koek. As Royal Huisman's Software Developer, Koek offers another argument in favor of WAGO technology.

»The type of communication structure, the flexibility of the system and its compact design make WAGO's automation solutions very attractive to us.«

Flexible technology for individual dream yachts

According to Koek, the flexibility of WAGO's system is particularly valuable in new construction. "Thanks to the modularity of the WAGO-I/O-SYSTEM, we can individually adapt and flexibly expand the automation to specific ships," he explains. "The type of communication structure, the flexibility of the system and its compact design made WAGO's automation solutions very attractive to us," Koek adds.

Attractive is just one word for the yachts built in Vollenhove on Ijsselmeer. "If you can dream it, we can build it," emphasizes Koek. Royal Huisman, a leading global shipyard for motorized and sailing yachts up to 90 meters, has earned its storied reputation by merging quality, service and innovation with traditional craftsmanship. "We make dreams into reality," states the software developer as he beams with pride. The dreams are made from majestically modeled aluminum using hypermodern technology, yet are built using traditional methods. It generally takes two to three years between the first sketches and construction before the owner takes delivery. "And despite all of our experience, we are always delighted and amazed every time a yacht leaves our shipyard, because every boat is different," Koek summarizes.

TEXT NORMAN SÜDEKUM AND JORIS VAN LIEMPT | WAGO

PHOTO WAGO

COMPLETE FLEXIBILITY, GREATER SECURITY

The new Industrial Managed Switches with maritime approvals

Ethernet's presence is growing aboard ships, prime examples include drive control, deck-based cargo lifts or alarm and monitoring systems. Therefore, cost-efficient, stable and redundant network solutions are necessary, which include components like WAGO's 852 Series Industrial Managed Switches.

The individually configurable Industrial Managed Switches reliably network all Ethernet nodes and ensure continuous access to machines and systems. The "Rapid Spanning Tree," "Dual Homing," "Dual Ring," "Jet Ring," "ERPS v1/v2," and the fast "Xpress Ring" protocols enable the creation of redundant network structures with short recovery times of less than 50 ms. This guarantees secure communication, even when connections are faulty. Every WAGO Industrial Managed Switch also features a redundant power supply for uninterruptible data communication (transmission rate up to 1 GBit/s). This value-add feature contributes to secure operation of machines and systems on board ships.

Comprehensive security functions

Industrial Managed Switches from WAGO support up-to-date security functions, such as "Mac Limitation," "Port Security," and authentication per IEEE 802.1x. Furthermore, "IGMP Snooping," broadcast and bandwidth limitation enable additional data flow control. The advanced security functions support these next-generation switches in protecting your systems against cyberattacks and accidents that can adversely impact people, machinery and the environment.

Industrial Managed Switches with DNV GL approval for use on ships are each available in two different versions: 8-port 1000Base-T and 4-port 1000Base-SX/LX models (852-1305), as well as the 8-port 100Base-TX and 2-port 1000Base-SX/LX models (852-303). All switches can be individually configured to meet the requirements of various network structures.

High-performance downtime prevention:
WAGO's new Industrial Managed Switches with ring redundancy, redundant power supply and industry-leading security features

Increase uptime using two parallel controllers

REDUNDANT AND YET NOT SUPERFLUOUS

The word “redundancy” stems from Latin, and means,“ to be present in excess.” One might believe that redundancy is not a concept that would be setting the stage for increased efficiencies and savings. Wrong! Particularly when redundancy supports uptime.

Technical systems in factories, buildings and on ships often have to complete their tasks without interruption. In order to achieve the required uptime for machines and systems, it is often necessary to double targeted functions of the automation systems in many applications, as well as in maintenance. Due to this redundancy, the automation system can compensate for any faults and ensure the continued operation of technical systems.

If an interruption does occur in the automation system – regardless of whether it is due to internal or external causes – it is imperative to detect it as quickly as possible, localize it and remedy it. Time is money and unplanned stoppages result in correction costs. On board ships, the fast procurement of replacement parts and the availability of system specialists are often part of the problem in such cases. This is why the demand for fault tolerance in automation systems is ubiquitous in this sector.

The correct redundancy for each application

An important system indicator for fault tolerance in automation systems is the switching time between the active and the stand-by automation functions. The switching time required determines which target applications can be operated using which automation systems. A distinction is made here between redundancy types: hot connects virtually instantaneously, warm requires several milliseconds and cold connections may take a few seconds to establish.

Time-critical technical systems, which engender high costs in the case of failure, are generally designed with hot redundancy solutions. Warm redundancy is preferably used in systems that are

not time-critical, like alarm and monitoring systems, or to control slow control loops. A general rule of thumb: the switching time to the redundant automation function must be lower than the system tolerance time of the system in question.

Taking system environments into account

In order to guarantee the reliability of the automation systems, the system environment must be considered in addition to the PLC. The voltage supply and the communication medium (e.g. ETHERNET) must also fulfill the technical system's uptime requirements. Another classification of redundancy types is by function: supply redundancies, communication redundancies and device redundancies. The need for different redundancy types must be evaluated in the design phase of the automation system so that the automation technology will contribute to increased uptime for the technical systems.

In maritime construction, a maximum fault tolerance of at least one is required. This means that a failure of the voltage supply or an interruption of the network cable does not impact operation of the technical systems, because it is merely a "single point of failure" (SPOF).

Supply redundancy

In general, voltage redundancy is designed as a hot redundancy by using a diode module for economically regulating two independent voltage sources. If one electrical supply fails, the second voltage supply is available through instantaneous switching.

Communication redundancy

An Ethernet network can be designed as a dual LAN network (two LAN cables with identical data traffic) or as a ring. The dual LAN network enables instantaneous switching, but is associated with increased cabling costs. A more economical alternative is the ring network protocol; however, these systems often have a longer switching times. Switching times for the known redundancy protocols of office networks (STP, RSTP, MSTP) are cold at best, in that they require more than two seconds. A standardized, manufacturer-independent ring protocol, which enables switching in less than 50 ms, is ERPS.

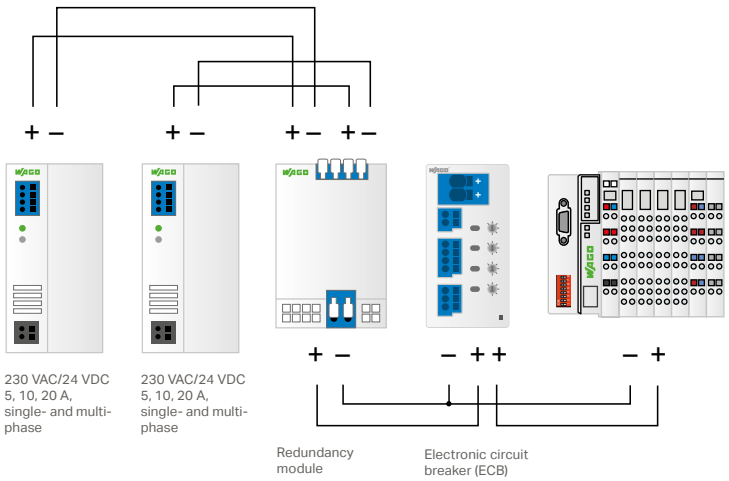
Device redundancy

There are likewise various switching mechanisms for the device redundancies of PLCs. The most expensive are hardware-controlled switches, followed by switching implemented by the operating system. A less expensive alternative is switching algorithms at the application level. It is imperative that the necessary system tolerance times for the technical systems match the selected redundancy type.

Redundancy by WAGO

Supply redundancy

When it comes to supply redundancy, WAGO provides the relevant hardware for a redundant electrical supply with devices from the *EPISTRON*® Series. It is important in this case, that the two current supplies have different sources, and that the cables are laid in different paths. This ensures the functionality of automation systems during an electrical failure of one power source.

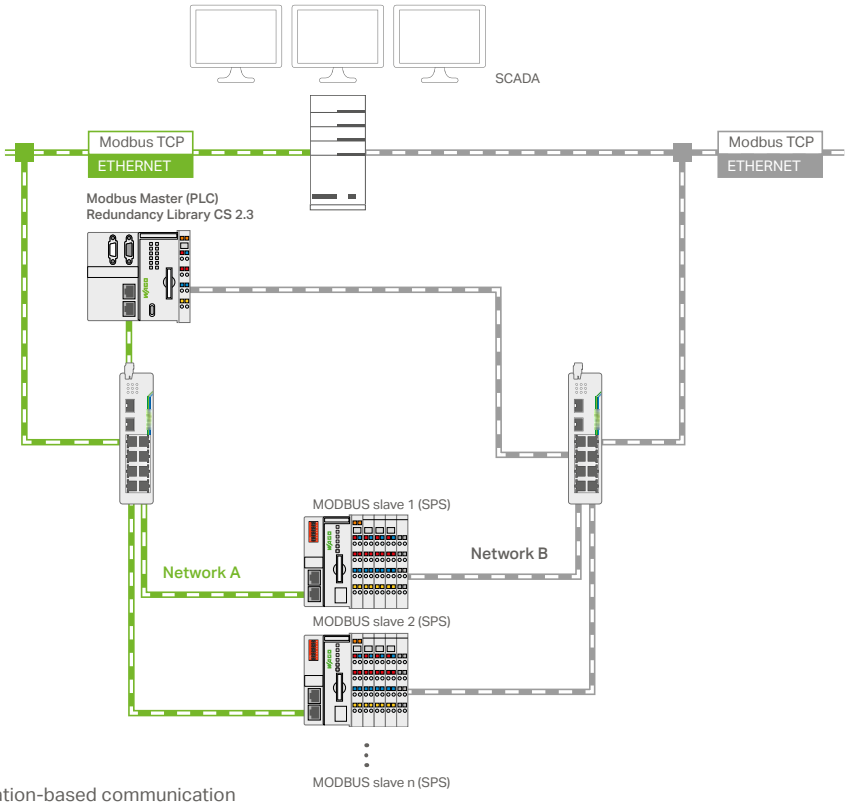


Supply redundancy

Communication redundancy

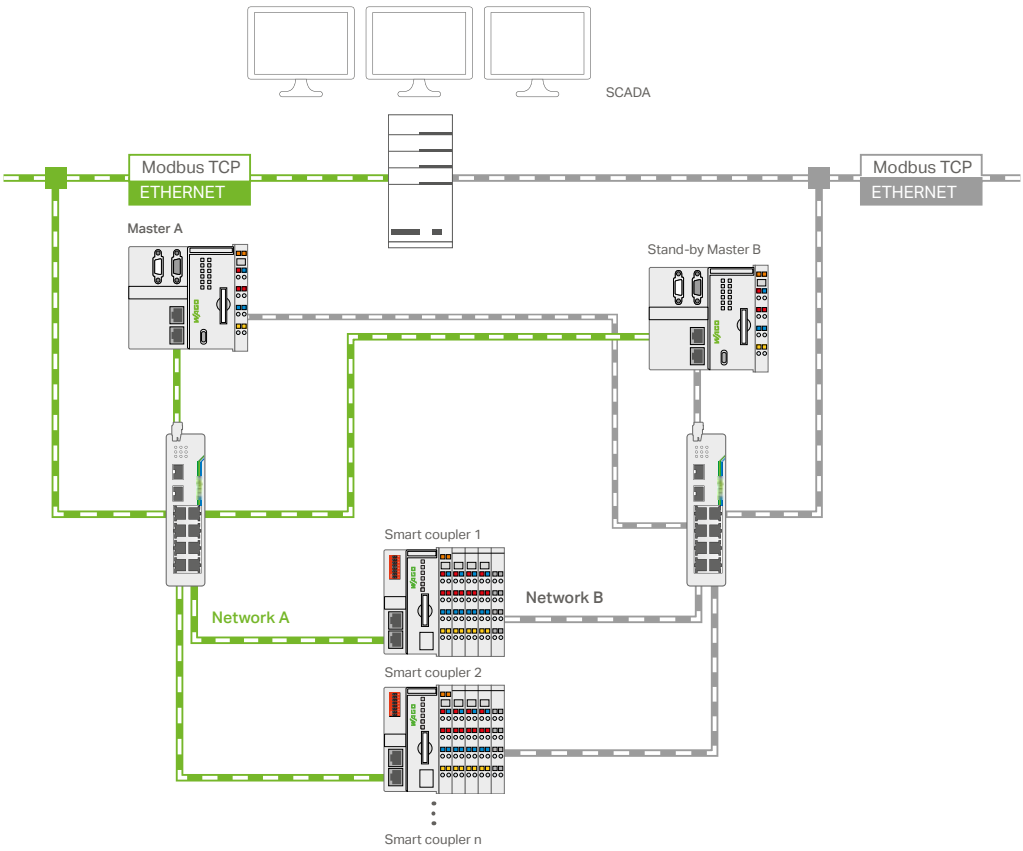
Regarding communication redundancy, WAGO offers a proven application-based redundancy concept. By using selected hardware in combination with the media redundancy library in CS 2.3, the necessary fault tolerance for Ethernet-based communication can be achieved using the Modbus protocol. In this redundancy concept, all data packets are transmitted over two different paths from the transmitter to the receiver. As soon as a message has been successfully transmitted to the automation system, the automation task is executed. This application-based communication redundancy is also instantaneous.

Application-based media redundancy (dual LAN)



Application-based communication redundancy

Application-based controller redundancy



New concepts for application-based controller redundancy

WAGO likewise provides its maritime customers with an application-based redundancy concept for controllers.

Based on the Modbus-TCP protocol, this solution is already used in alarm and monitoring systems. What makes this redundancy solution special? Extremely simple commissioning of the entire system using WAGO's standard hardware. For WAGO customers, this represents tremendous costs-savings during the system integration of their automation system.

WAGO's ***e!****COCKPIT* engineering software tool is used as the programming environment for the controller. The multi-node programming environment can easily transmit the PLC program to both PLCs. In order to use the application-based controller redundancy, a software library with the necessary synchronization functions muyt be linked into the master PLC. The library also offers the opportunity to redundantly link subnodes with a dual-LAN. The subnodes, also known as smart couplers, do not have to be programmed; they can simply be booted from an SD card and then configured using an integrated webserver. Analog and digital bus nodes are automatically recognized by the smart coupler, and the process mapping is likewise automatically provided to the higher-level master PLC. In addition, the master PLC can communicate with higher-level SCADA systems via the Modbus-TCP protocol. The redundant connection is carried out over two separate networks.

Alarm and monitoring systems are particularly well suited for using application-based controller redundancy. The solution design corresponds to an SPOF-tolerant system, which means that any occurring fault – like a voltage supply failure, the LAN connection, switches, or controller – can always be compensated for. Doubling the Ethernet topology and the redundant message transmission enable instantaneous switching during a fault in the network. Typical switching times after the failure of a PLC are easily below the requirements of DNV GL when used in traditional alarm and monitoring systems.

TEXT INGO SULECK AND NORMAN SÜDEKUM | WAGO

PHOTO WAGO

Ferries and cruise ships use innovative technologies to chart more efficient courses.

SAVE THE ENVIRONMENT – SAVE MONEY

When large shipping companies like Stena Line proudly report that they have once again been able to reduce fuel consumption in their fleet, then CATC from Gothenburg can also enjoy this success. The relatively young corporation from Sweden primarily specializes in reducing energy consumption in the heating, ventilation and air-conditioning systems used aboard ships. CATC, in close collaboration with WAGO, takes on complete system upgrades from the electrical design through programming and project management up to commissioning and future service.

The “hotel operations” of cruise ships offer significant opportunities to reduce operating costs through energy efficiency.

As early as 2005, the Stena Line shipping company consolidated their shipping division into an “Energy-saving Program” (ESP) to reduce energy consumption. The goal was an annual reduction of 2.5 percent, which they exceeded in 2015 with a reduction of 2.8 percent. “By 2030, we plan to reduce our CO_2 emissions by 35 percent per nautical mile,” explains Erik Lewenhaupt, Head of Sustainability at Stena Line. “Within the context of ESP, we assess various points for saving energy, from the ship’s propeller up to the lightbulbs. In addition, we rely on digital solutions for our fuel management system in order to optimize on-board operations using the data that we record from our ferries.”

Tuning the subsystems reduces energy needs

In applications like these, the systems from CATC prove their worth. On cruise ships and ferries, they optimize pressure and temperature from fans, air-conditioning devices, and boilers such that, “the energy costs for a ship can be reduced by up to 40 percent,” explains Jens Stjärna, one of the founders of CATC. The need for electrical power can be substantially reduced by primarily monitoring the systems of the “hotel system” (passenger and crew quarters) on ferries or cruise ships with the aid of the WAGO-I/O-SYSTEM 750, synchronizing the systems and controlling them simultaneously. And because all energy used on

board has to be generated by the hotel generator, called a gen-set, efficiency increases here also reduce fuel consumption, as well as particulate and CO_2 emissions. These changes in turn reduce costs per mile.

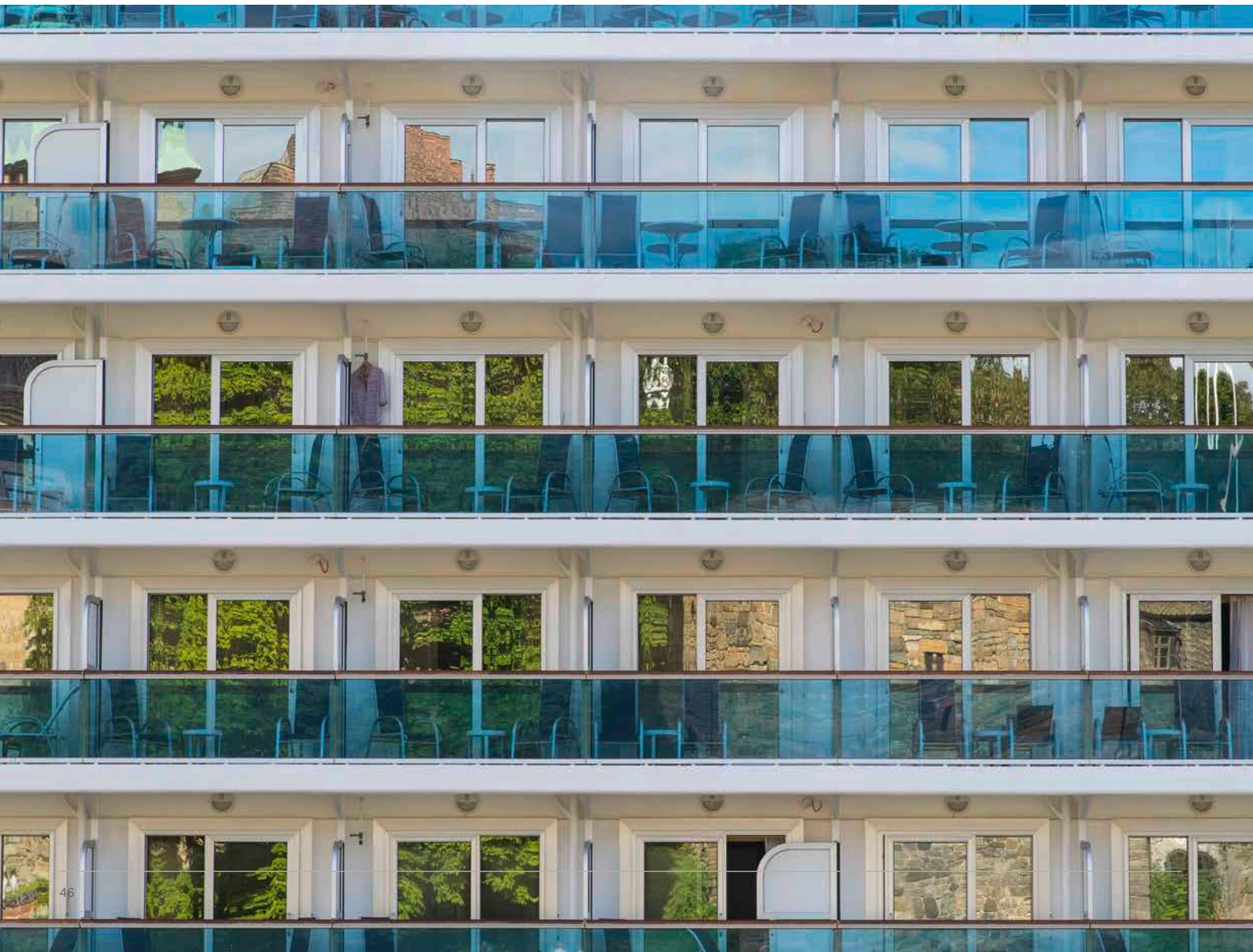
"Luckily, environmental consciousness is increasing," states Stjärna, who has found the maritime industry to be rather old-fashioned when it comes to issues of sustainability. This trend can be linked to the fact that cruise ships have been increasingly criticized because their exhaust creates smog in harbors and fjords. In addition, ships from the Stena Line, travel exclusively in ECAs (emission control areas), where specific environmental guidelines apply regarding emissions, as well as waste and wastewater disposal.

"At CATC, we anticipated the demand for more energy-efficient operation of ships, and today we are virtually the only ones dealing with such issues – this is naturally an advantage for us," states Stjärna.

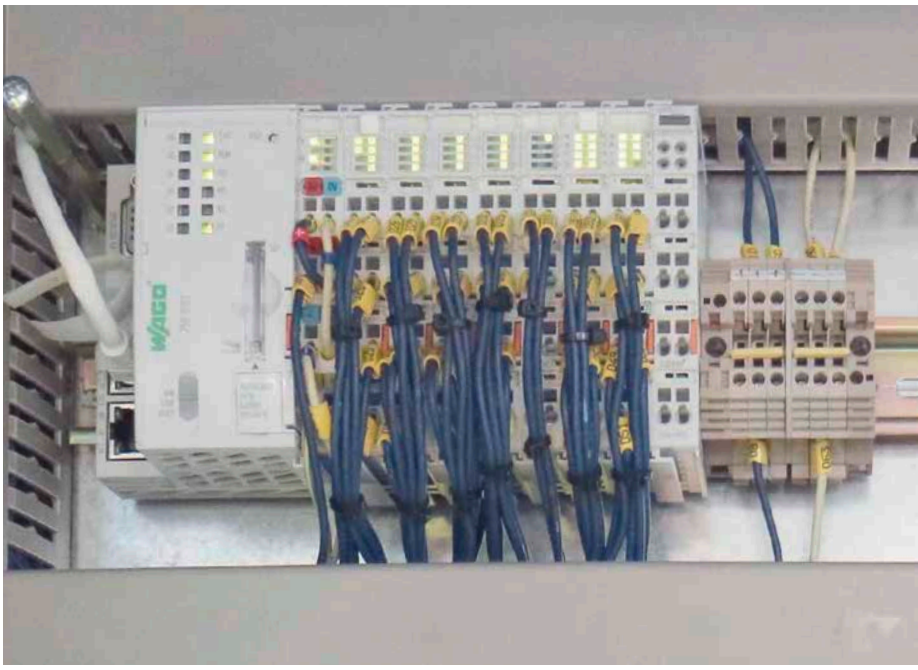
The Swedish firm combines its experiences in air-conditioning technology and ship automation with WAGO products that have the corresponding approvals from top classification agencies. Stjärna explains that, "The WAGO systems correspond to the relevant maritime standards. When we were selecting systems, this was a primary criterion, in addition to the compact design of WAGO's products. When all of the components that we use are certified, it is easier for us and makes dealing with new customers more successful."

Retrofit for a better climate

Most projects at CATC include the complete upgrade of the entire control system for the HVAC technology on board. If a system replacement is planned as part of the retrofit, then the work usually begins in the engine room. There, they install touch screens that enable the personnel to monitor temperature and air pressure, and control them individually. Comparable operating and visualization solutions are also used in areas where



With 3,500 guests and more than 1,500 crew members, modern cruise ships house an entire small town.



The WAGO-I/O-SYSTEM 750 is approved for maritime use.

passengers congregate, such as conference or dining rooms. “Our goal is to increase efficiency on board without compromising passenger and crew comfort,” clarifies Stjärna.
Since the upgrades occur while the ship is operating, the technicians from CATC have accompanied ships around the world. “It is a tremendous advantage to be on site while commissioning the new systems,” explains Stjärna. “This way, we gain direct feedback from our customers and can observe how the crew on board uses our systems.”
Stjärna explains that CATC recently completed a large project on one of the Stena Line ships that travels between Gothenburg, Sweden and Kiel, Germany. A completely new system was installed in both crew and passenger quarters, from the auto deck to the engine room. “The Stena Line employees, who work the auto deck, were especially happy about the retrofit,” says Stjärna, “because our system improved ventilation there, and reduced exhaust gasses.”

CATC’s retrofit improved the climate in two places at once – both in the ship and in the environment around it. This also makes financial sense.
“A system change can pay for itself within one to two years,” according to Stjärna. This is due both to the energy savings, and that on-board can work more effectively due to the new software. “In the long-term, our customers save money.”

TEXT JENS STJÄRNA | CATC,
STEFAN WALL AND URBAN WASE | WAGO
PHOTO WAGO AND THORSTEN SIENK

»WAGO’s systems are aligned with relevant maritime standards.«


SKARPENORD

Why standardized industrial technology offers so many advantages to the maritime sector.

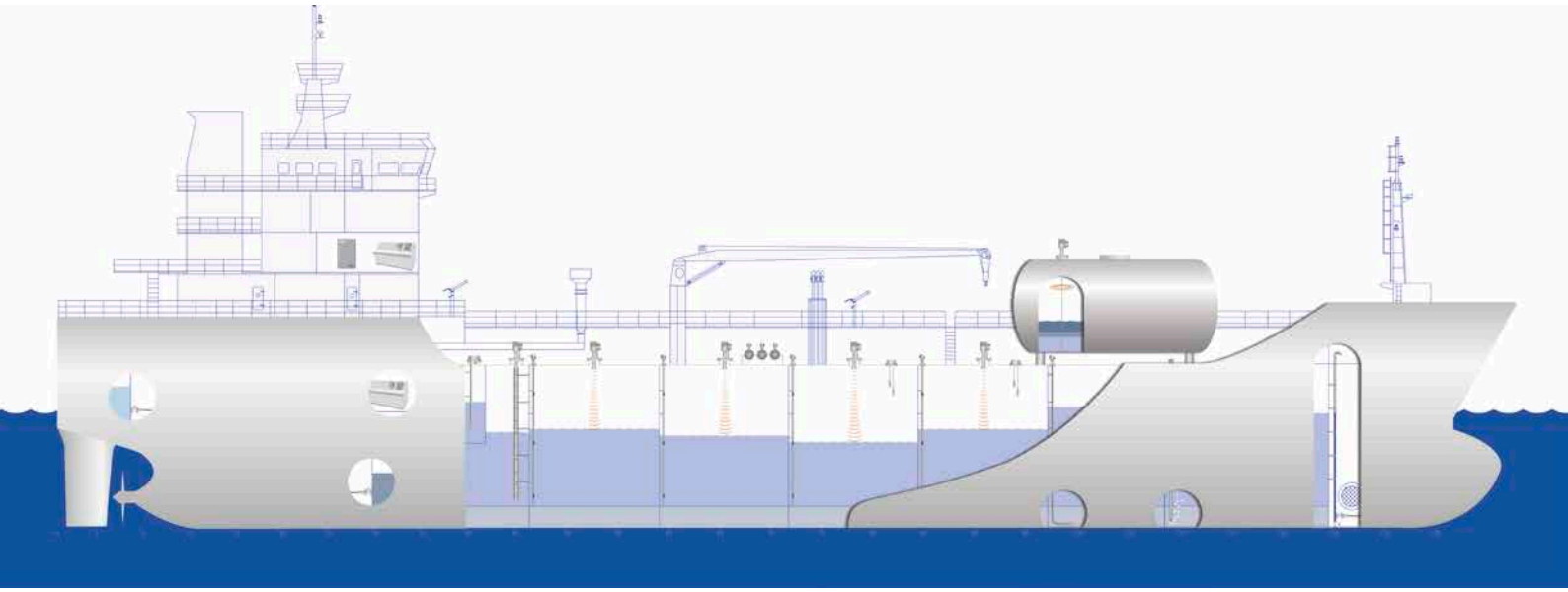
USING OFF-THE-SHELF PRODUCTS

While general cargo and container ships can easily count and add up the loads connected to their cargos for effective load management, precise level measuring devices are required for tankers. Krohne Marine from Norway is considered one of the global experts in this field, with more than 50 years of experience in designing load-monitoring and management systems for tankers. Krohne is using standardized control technology from WAGO in their new generation of "Cargomaster" systems, and replacing their proprietary electronics.

By using "Cargomaster," ships' crews constantly have the level of their tanks at their fingertips. The complete solution from Krohne Marine includes the entire monitoring system, from alarms, to visualization and connection to higher-level control systems, in addition to straight level measurement systems. Krohne uses their OPTIWAVE 8300 C Level Radar for the actual measurements at the load level. In addition to level measuring, the system – designed in Brevik, Norway – can also monitor pumps, conduits and the ship's draught. Until recently, the Norwegians developed most of the necessary electronics themselves – primarily with the assumption that this would maximize precision and uptime. Their innovation is reflected in an abundance of patents, among other things.

Standardized instead of proprietary

Krohne Marine is symbolic of proprietary systems, which function excellently; however, against a background of long operating times during freight travel, they also raise costs for product updating, replacement part inventory and service. These outcomes are typical for proprietary developments, particularly in control hardware. Therefore, within the context of upgrading "Cargomaster," Krohne went looking for a partner in industrial control technology, with whom they could perform maritime tasks with off-the-shelf products. The use of standardized components was possible because the Norwegians' expertise lies in the design and implementation of software, rather than the hardware, as the Director of Research and Development at Krohne Marine, Svein Henriksen explains. "Using off-the-shelf products currently allows us to reduce costs, primarily in development and production," adds Henriksen.



By using cargo-monitoring systems like the "Cargomaster," crews always have the fill level of their onboard tanks at their fingertips.

Optimal – in terms of price, performance and uptime

Prior to making the strategic decision to rely on WAGO's industry-proven, standardized control technology in their tank management systems, the Norwegian company compared diverse solutions from leading manufacturers. "We were looking for a supplier with products that could accommodate our requirements without long adaptation times – even in areas with extremely high demands, like explosion protection. In addition, the products that we use must have the corresponding approvals from the classification agencies," explains Henriksen, who manages the Service Department at Krohne.
From a functional perspective, the new hardware had to provide high performance – especially in communication capabilities. These criteria ultimately led to the decision to use the WAGO-I/O-SYSTEM 750. "With WAGO, we found a vendor that meets our needs," states Jon Anders Eriksen, the man in charge of process control technology at Krohne Marine. The collaboration functioned extremely well from the start – including intensive support in software engineering and training.

Unforetold options

The partnership ultimately led to a system in which the software was not merely implemented in the new control hardware, but instead was highly adapted for optimal interplay between software and hardware. This in turn led to a significant increase in performance compared to previous generations.
By deciding to stop developing their own hardware, and to begin using standardized modules, Krohne Marine was also able to tap into advantages for applications in the Ex areas. Background: The I/O-SYSTEM 750 includes modules for Ex and non-Ex areas. Functionally, these modules are not different; they are distinguished by their design and external color. Within the WAGO system, blue is the color for explosive areas.

»With WAGO, we found a vendor that meets our needs.«

This consistency in the product portfolio offers the Norwegians an advantage: they no longer need to consider whether a wiring installation falls under Ex-protection or not. From the perspective of the software engineers, only the functions are relevant because there are no longer any spatial restrictions. In addition, the blue I/O modules

eliminate additional components because Zener barriers are no longer necessary in the control cabinet. This detail not only saves space, it also makes the installation easier, as there are fewer components to be wired. This, in turn, increases operating safety due to the lowered risk of mismating or component failure.

More time for core competencies

For Krohne Marine, these points were exactly what drove their decision to use standardized industrial technology. Due to their large series production, which includes sophisticated production monitoring routines, Krohne Marine also benefited from reduced failure rates in the components used. The spring clamping technology in the WAGO-I/O-SYSTEM also contributed to reliability, as the high vibrations aboard a ship demonstrate the system's high performance.

Using off-the-shelf products pays off – even in the maritime sector. WAGO's standardized control technology also functions reliably in the harsh environmental conditions at sea. "We have not had a single complaint," emphasizes Henriksen. The cost reductions connected to the standardized products are visible in many areas at Krohne: fewer components and less inventory are needed, faster configuration and assembly, better availability of replacement parts and service around the world. "During development, we can now concentrate more on improving the functionality and user-friendliness of our systems," concludes Henriksen. The R&D Manager sees sustainable advantages that will significantly sharpen his company's competitive edge.

TEXT STIAN KARLSEN | WAGO

PHOTO WAGO

Because the WAGO-I/O-SYSTEM can connect applications in both normal and Ex areas using the same system, Svein Henriksen (left) and Øystein Johansen (right) can concentrate on their core competencies when designing their tank management systems.

KROHNE Marine

Krohne Marine is considered one of the leading manufacturers of tank monitoring systems aboard ships. Ballast, fuel or cargo tanks: Tailored solutions from the Norwegian company are installed in all types of ships – from small tankers up to chemical barges. Krohne Marine, which is headquartered in Brevik, has completed almost 1,000 systems since the company was founded in 1957. A digital milestone in the company's history was the 1997 development of the first level measuring system for ships that utilized electrical data.

WE INNOVATE!

Imprint
WAGOdirect process, September 2016
Editor: Eva Banholzer
(responsible editor)
Phone: +49 (0)571 887-44418
Fax: +49 (0)571 887-8418

Contact: Eva Banholzer, WAGO
We assume no liability for unsolicited manuscripts and photos.
WAGOdirect process is published periodically throughout the year.

WAGO Kontakttechnik GmbH & Co. KG
Postfach 2880 · 32385 Minden
Hansastraße 27 · 32423 Minden
info@wago.com
www.wago.com

Headquarters	+49 (0)571/ 887 - 0
Sales	+49 (0)571/ 887 - 222
Order Service	+49 (0)571/ 887 - 44 333
Fax	+49 (0)571/ 887 - 844 169

0888-0203/0216-6901 – WAGO DIRECT PROCESS 2/16 DE – 08/2016-00 – Printed in Germany