PORT TECHNOLOGY

EDITION 138 - 2024

THE E-JOURNAL OF PORTS AND TERMINALS

SAFETY AND SECURITY

In partnership with

Deloitte.

nexxiot

GREENTECH
FOR PORTS AND TERMINALS

POWERED BY PORT TECHNOLOGY INTERNATIONAL

THE ROAD TO NET ZERO

EARLY BIRD TICKETS AVAILABLE!

7 - 8 MAY 2024

BARCELONA, SPAIN

SAVE €300 NOW!

Join us at GreenTech for Ports and Terminals 2024 and be part of the solution for a sustainable future!

Explore strategies for developing green ports, highlight cutting-edge technologies that reduce operational carbon emissions, and discuss how collaboration can lead to easy wins in achieving sustainability goals.

FREE TO ATTEND FOR PORTS & TERMINALS!

FIND OUT MORE AT GREENTECH.PTIEVENTS.COM

SILVER SPONSOR

awake.ai

BRONZE SPONSORS

KALMAR

moffatt & nichol

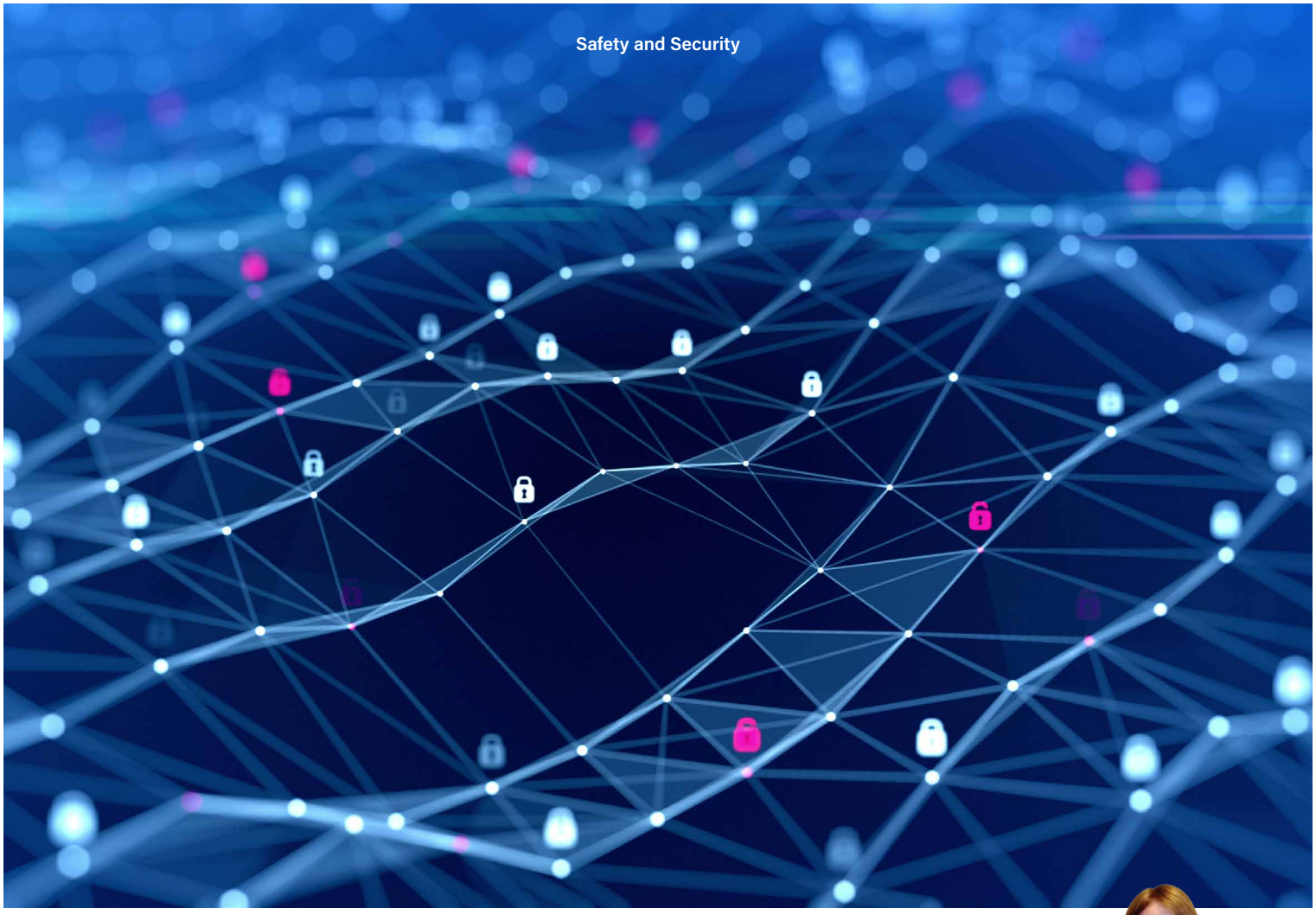
PORTCHAIN

RICARDO

spire | weather & climate

greentech.ptievents.com | #GT2024

www.ptievents.com www.porttechnology.org @PortTechnology PortTechnology



FROM THE EDITOR

Margherita Bruno,
Editor

Welcome to this month's edition of PTI e-journal, where we delve into the realm of maritime safety and security.

In today's interconnected world, ensuring the safety and security of maritime trading systems is imperative. Port security encompasses a wide array of topics, ranging from cybersecurity to efficient cargo handling, all aimed at fortifying overall security measures.

We are honoured to have our sponsors, Nexxiot and Deloitte, introduce their KYX solution for the global supply chain. Addressing challenges encountered by European ports, KYX integrates various factors such as infrastructure, environmental regulations, competition, security and digitalisation to enhance transparency, compliance and sustainability within the supply chain through real-time data insights and advanced cargo tracking and security technology.

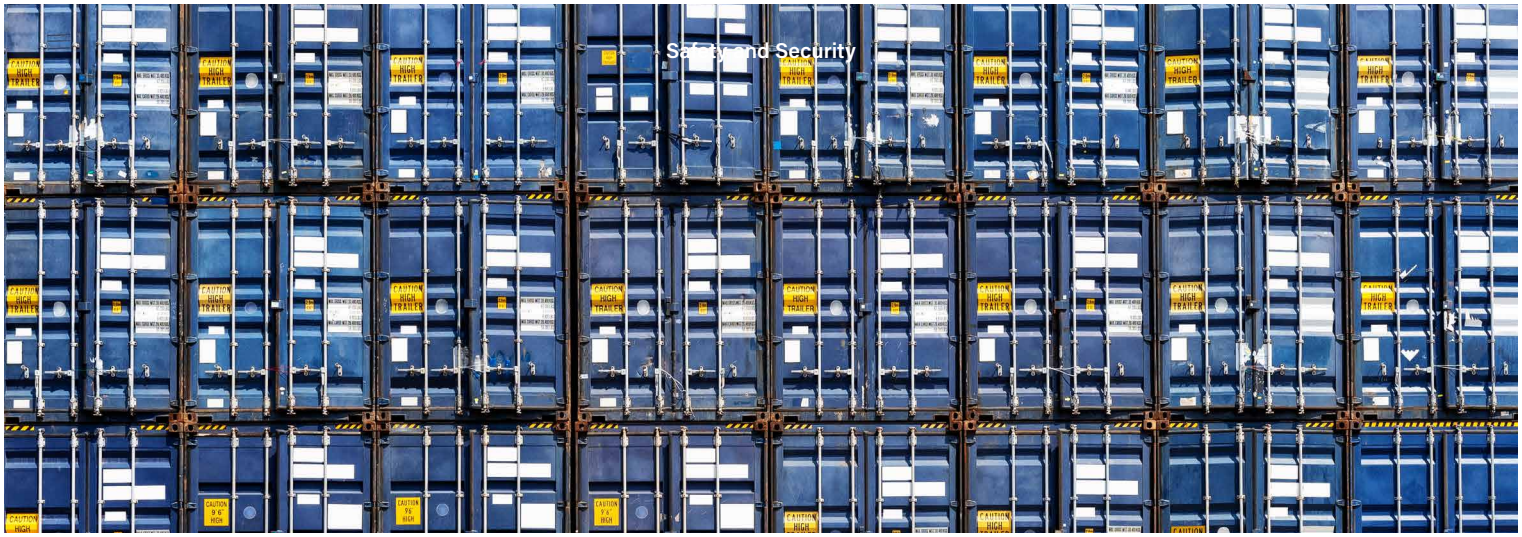
In the realm of fire safety for electric port equipment, Fogmaker International emphasizes the necessity of robust fire suppression systems amid the transition to electric-powered machinery. Our official section sponsor offers high-pressure water-based mist fire suppression systems, providing effective solutions to mitigate fire risks on a global scale.

Our journal further showcases advancements in port security, spotlighting innovations such as Porto Itapoá's inventive rescue cage and Antwerp's 'D-Hive drone-in-a-box' network, enhancing situational awareness. Additionally, EyeSeal's container breach detection device plays a pivotal role in fortifying global commerce security by delivering real-time monitoring of container parameters, ensuring unparalleled cargo visibility and security.

As we shift our attention to the maritime industry, cybersecurity and risk management experts Richard Oloruntoba and Ed McNamara emphasize the importance of protecting against cyber threats. Oloruntoba suggests a comprehensive approach to managing port security threats, while McNamara provides insights into effective port cyberattack insurance coverage. Both experts stress the need for continuous improvement of cybersecurity capabilities and vigilance against evolving threats. Cybersecurity is crucial for the maritime industry; in our last contribution, Marlink advises on preparation, compliance and awareness to counter cyber threats. With digitalisation, cybersecurity is a top priority to ensure business continuity and reputation. A coordinated approach is essential to mitigate risks and uphold the integrity of maritime operations.

We express our gratitude to all our contributors for sharing their priceless insights. Their contributions are essential in shaping a safer future for those navigating the maritime landscape.

Thank you for joining us on this journey! We hope you find this edition informative and enlightening.



CONTENTS

info@porttechnology.org
@PortTechnology
www.porttechnology.org
linkd.in/porttech

SUPPLY CHAIN TRANSPARENCY

In partnership with

Deloitte.

nexxiot

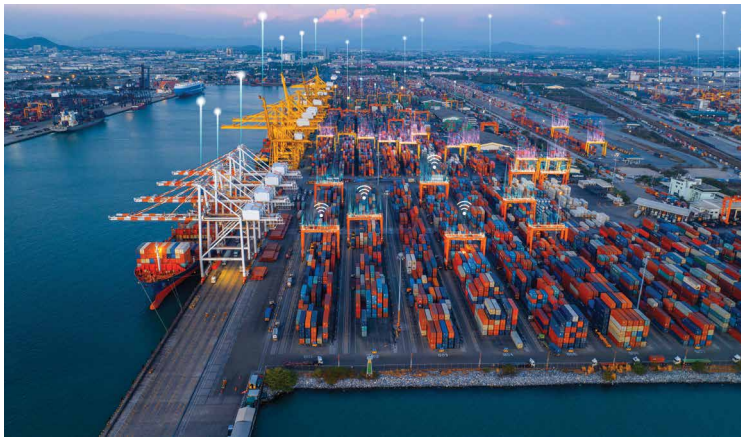
KYX: TRANSPARENCY, TRUST AND EFFICIENCY FOR THE GLOBAL SUPPLY CHAIN OF TOMORROW

"THIS NEW KYX OFFERING AIMS TO MEET SUPPLY CHAIN TRANSPARENCY, COMPLIANCE AS WELL AS SUSTAINABILITY DEMANDS."

Werner Fontanive, Fellow at the Center for the Edge, Deloitte, and **Stefan Kalmund**, CEO, Nexxiot

The global supply chain, a dynamic web connecting the farthest reaches of the world, orchestrates the movement of goods with precision and efficiency. Within this complex environment, international ports serve as gateways and nerve centres through which the ecosystem is orchestrated, thereby ensuring the seamless flow of commerce across borders. European ports are facing significant challenges that are affecting their efficiency and competitiveness, similar to ports around the world. These challenges include:

1. **Infrastructure:** Many European ports are facing infrastructure challenges, including outdated facilities, insufficient capacity, inefficiencies and hence underleveraging the actual capacity they have available, and inadequate connections to other transportation modes. This leads to congestion, delays, and increased costs for shippers.
2. **Environmental regulations:** Notably European ports are subject to strict environmental regulations, which can increase costs and limit the types of cargo that can be handled. For example, ports may need to invest in new equipment or technologies to reduce emissions or comply with waste disposal regulations.
3. **Competition:** European ports increasingly face competition from other ports around the world, particularly in Asia and the Middle East. These ports may have lower costs, more modern facilities, and better connections to other modes of transportation, making them more attractive transit hubs to shippers.
4. **Security:** European ports must comply with strict security regulations to prevent terrorism, illicit trade, contraband, trafficking, and other threats. This can increase costs and lead to delays for shippers, particularly if cargo needs to be inspected or screened and this is done in a sub-optimally organised manner.
5. **Digitalisation:** European ports are increasingly adopting digital technologies to improve efficiency and competitiveness and they still rely heavily on human-based processes. However, this requires significant investment in new technologies and infrastructure, as well as training and development for staff.



All together, these challenges require significant investment in new infrastructure, technologies, real-time data-driven insights, training, and more to ensure that European ports can continue to meet the contemporary needs of the global supply chain and remain successful in an increasingly competitive market.

Over recent years, one could witness the emergence of a broad range of initiatives and stand-alone solutions. For these to be truly successful and reach their full potential, at Deloitte we are convinced that a high level of integration into a wider and broadly adopted ecosystem is quintessential. To date, a positive trend in this direction can be recognised; with several European ports leading the way by having launched several initiatives to address these challenges.

To carry this further, optimise investments and be cost-efficient, Deloitte has devised an overarching and agnostic industry approach, allowing it to extrapolate existing and proven market capabilities into one common service model, called the "Deloitte KYX offering". Combining Deloitte's Know Your Client (known

"THE IMPLEMENTATION OF THE KYX SOLUTION, EVEN IN A PARTIAL MANNER, CAN EFFECTIVELY LOWER THE RISK OF FRAUDULENT ACTIVITIES AND ENHANCE SECURITY MEASURES IN PORTS."

as KYC) concept and expertise with its views on knowing your cargo, the KYX concept brings new and broadly adaptable data-driven services, utilities, and platforms into the market – combining with existing services where applicable.

As a starting point for exploring and further designing the KYX offering, amongst others, Deloitte is currently teaming with the companies Nexxiot and Pairpoint. By combining Deloitte's Know Your Customer (KYC) capabilities with Nexxiot's insights around Asset Intelligence Devices and Pairpoint's knowledge on EoT technology and data verification capabilities, a best practice standard is being established with the ambition to allow each party in the logistics chain to gain real-time insights; which in their turn will open the door for a myriad of relevant use-cases such as around enhanced data provenance, cargo transparency, improved operations, increasing regulatory compliance, and others. This new KYX offering aims to meet supply chain transparency, compliance as well as sustainability demands. It is designed as an open standard and open platform, to ensure broad future development and deployment as well as strong market penetration and acceptance.

KYX involves collecting, verifying and making available information about the cargo being transported, including its provenance, destination, contents, status, location, exporter, importer, Ultimate Beneficial Owner (UBO) and many more information elements. This information is then used by stakeholders in the ecosystem to ensure that the cargo complies with all relevant regulations and standards, for example.

To feed KYX, Asset Intelligence devices can be used to oversee the payment-goods transport cycle. These devices provide complete traceability of all movements, changes and handling of the asset across its entire journey. They have the capability of pinpointing delays in the supply chain to certain parties and locations, as well as confirming that transhipments were made at approved or official transhipment stations, such as free ports. Additionally, they can substantiate that the cargo did not unexpectedly and suspiciously stop somewhere along the route, where it could have been contaminated or exfiltrated.

As an additional feature, these devices can ensure that containers and the assets they contain are always sealed during the journey, except on approved occasions. As such, KYX also involves meeting inspection and screening of cargo requirements. Cargo must be inspected and screened to ensure that it complies with relevant regulations and standards. This includes checking for prohibited items, such as drugs and weapons, and ensuring that the cargo is

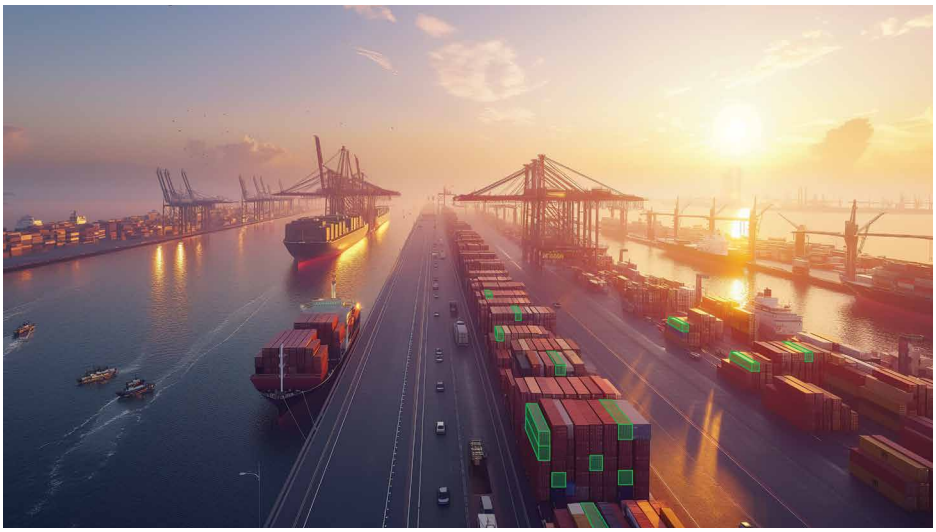
consistently, fully labelled and packaged.

Meeting the aforementioned container security and tracking requirements necessitates the use of smart technology, such as GPS tracking and RFID tags, to monitor the location and condition of the container.

One specific use case for the solution is the efficient processing of goods in ports and the clearance from customs on the on- and off-boarding, within the framework of so-called green lane objectives. The KYX solution can help ports speed up the clearance process for goods, reduce waiting times and improve the overall efficiency of the port, including cargo inspections. By using smart connected sensors, KYX provides real-time data on the location and condition of cargo, allowing port authorities to quickly identify any issues and take the appropriate action.

The implementation of the KYX solution, even in a partial manner, can effectively lower the risk of fraudulent activities and enhance security measures in ports. It also leads to more efficient interventions and operations. By verifying the provenance of data on the movement, content and status of cargo, KYX can ensure that only legitimate goods are cleared for entry into the port. This helps to prevent the entry of counterfeit goods and other illegal items, making it less dependent on the intervention of stakeholders and thereby also improving the overall safety and security of port workers and the wider hinterland community.

KYX is designed to support the needs of customs and other regulatory authorities in European ports whilst at the same time bringing benefits to global supply chain efficiency and transparency for all other stakeholders involved, including port authorities and operators themselves. These ports have specific requirements for cargo entering and leaving their facilities, and these requirements must be met to ensure that the cargo is transported safely and efficiently.



ABOUT THE AUTHORS:
Werner Fontanive is a Deloitte Fellow at the Center for the Edge identifying and exploring opportunities on the edge of business and technology. As a transformation partner, he engages company leaders, unlocks innovation potential and drives growth.

Stefan Kalmund is the CEO of Nexxiot. Passionate about technology, growth and making a positive impact on how cargo is shipped, Stefan captures global megatrends and constantly searches for ways to deliver unparalleled insights to clients.

ABOUT THE COMPANIES:
At the Deloitte Center for the Edge, we connect edges to accelerate impact. We partner with senior executives to make sense of and profit from emerging opportunities on the edge of business and technology. We help leaders understand the fundamental changes shaping the world, navigate the short-term challenges and identify long-term opportunities.

Nexxiot is digitalising freight transportation with technology that now oversees the world's most extensive network of connected shipping containers and railcars. Clients gain access to unparalleled real-time data, which streamlines fleet management and automates logistics processes. Our devices, built for resilience, withstand extreme conditions and provide long-term, detailed insights into events affecting containers and railcars, including impacts, delays, security incidents and loading activities.

"KYX IS DESIGNED TO SUPPORT THE NEEDS OF CUSTOMS AND OTHER REGULATORY AUTHORITIES IN EUROPEAN PORTS WHILST AT THE SAME TIME BRINGING BENEFITS TO GLOBAL SUPPLY CHAIN EFFICIENCY AND TRANSPARENCY FOR ALL OTHER STAKEHOLDERS INVOLVED."

A DEEPER LOOK INTO THE KYX SOLUTION

Margherita Bruno, Editor, Port Technology International, interviewing **Werner Fontanive**, Fellow at the Center for the Edge, Deloitte, and **Stefan Kalmund**, CEO, Nexxiot

How does the KYX offering address challenges to European ports, such as infrastructure, environmental regulations, competition, security and digitalisation?

Stefan Kalmund: European ports are undergoing a transformational phase, where they are solving various challenges to enhance their efficiency and connectivity.

They are addressing the need to modernise ageing infrastructure, improve connections with other transportation modes and expand capacity to meet growing demand. Ports are actively working to strengthen security measures, manage risks and ensure safe operations. They are also acting to accelerate the pace of digitalisation.

The KYX offering takes a holistic approach integrating the needs of all supply chain participants, including European ports. This makes it possible for them to access the services they need from a single trusted platform.

By creating pragmatic quality standards in hardware, software and analytics, the technology is accepted by ports because it is safe, secure and interoperable. By creating a solution for device management, data management and flexible access via standard interfaces (APIs), stakeholders are provided with consistent and reliable data.

Ports are enabled to be more nimble, reliable and competitive in pricing to outmanoeuvred competition. Increased asset intelligence offers ports enhanced security capabilities, and greater efficiency in port processes improves the speed and accuracy of handling to reduce errors and delays. Improved visibility also helps to overcome the problem of inadequate connections to other transport modes as assets can be located and aligned with trucks, trains and barges with greater precision.

What are the benefits of the KYX solution for different stakeholders in the supply chain, including port authorities, shippers, customs and the wider community?

Werner Fontanive: One of the most significant benefits of KYX is the financial oversight it provides on all transactions and processes across the supply chain. From the purchase of goods to the financing of the shipment, the transfer of ownership, and the insurance to safeguard the goods - everything needs to be monitored and managed.

With a trusted Banking Financial Service and Insurance Industry (BSFI) 'golden record' for all aspects of the shipment, stakeholders are fully supported. This includes 'Know Your Customer (KYC), Know Your Suppliers (KYS), Know Your Suppliers Supplies (KYSS) to KYCC (Know Your Clients Clients). The benefit to stakeholders

is that contemporary and future regulatory demands in global finance and trade can be met. Through the same KYX offering, Carbon Footprint Monitoring is also within scope.

Ocean carriers, cargo owners and other logistics stakeholders benefit from the KYX offering because it makes physical and business processes faster, more accurate, trusted and validated. Cargo routing, handling and a wide range of other processes benefit from digital monitoring and sharing of this and other data. Unplanned stops, door-opening events, audit issues, cargo declarations, pre-trip inspections and customs risks are all made more transparent and manageable. Innovative practices like setting up green lanes for customs-approved goods, which make the processes around shipments faster, are also enabled.

Services around exception management, notifications on potentially fraudulent actions, self-clearing systems, geofencing, complex event processing and dynamic ETAs all act to enable stakeholders to get a clearer view of their operations, automate processes and create more accountability and trust.

How does the partnership with Nexxiot enhance the capabilities of the KYX offering, and what role do their technologies play in improving supply chain transparency and efficiency?

WF: The partnership with Nexxiot is vital for the KYX offering as it provides a bedrock of highly reliable technology, quality data and a long hardware lifetime. The KYX offering requires a technology partner with experience in large-scale device deployment.

Nexxiot's hardware devices are robust and resilient in their physical toughness, they offer global coverage and quick installation, making them ideal for multiple journeys over several years.

The approach Nexxiot took in terms of integration is also vital for success. This is done using an open architecture to connect other sensors to the gateway and the platform with other systems like those for global trade finance, freight forwarding, road, rail and carrier operating systems.

Nexxiot's solutions offer multiple value drivers including those centred on optimising carrier processes and supply chain operations. They also offer the opportunity to rapidly create new services for other stakeholders in the value network.

Could you elaborate on specific examples or case studies where the KYX solution has been successfully implemented in European ports?

WF: The KYX offering is currently in the design and build phase. The group is working with regulatory bodies and participants across the supply chain ecosystem to ensure global acceptance.

As the KYX solution is deployed, we can see many opportunities for European ports to benefit in the ways mentioned before.

The KYX offering does not depend on replacing existing infrastructure but offers a completely integrated solution for the market. As we have seen, Hapag-Lloyd has now digitised its entire container fleet, so we will start to feel the network effects of more and more assets being equipped, and more use cases being addressed with specific products.

How does the KYX solution ensure data integrity and security while collecting and verifying information about cargo, especially considering the increasing concerns around data privacy and cybersecurity?

SK: To ensure data integrity and security Nexxiot uses end-to-end encryption on all data that is generated on each device. Furthermore, all data is signed by a third party on the device to guarantee that no modification has taken place in flight or at any later time. This means that participants and users can trust the data and concerns around privacy and security are managed.

How does the KYX offering align with existing industry standards and regulations related to cargo handling, security and customs clearance in European ports, and what steps are taken to ensure compliance with these standards?

WF: Most of the processes around cargo handling, security and customs clearance are manual, siloed or localised. The KYX offering is using a digital, financially approved framework to enable new, faster and more transparent processes to be devised. By working closely with the regulatory bodies and market participants we can revise the industry standard with real live asset data as the benchmark for approval.

We have witnessed changes to EU customs legislation which is facilitating the use of supply chain monitoring hardware for international shipping journeys to and from the EU. Devices used are intrinsically safe and can therefore be used in a wide variety of industrial environments from ports to petrochemical plants.

SAFETY AND SUSTAINABILITY

In partnership with

FOGMAKER INTERNATIONAL AB

FIRE SUPPRESSION SYSTEMS FOR ELECTRIC PORT EQUIPMENT

Gustav Stigsohn, Product Manager,
Fogmaker International

BACKGROUND

The world is in the middle of the electric revolution. The change from fossil fuel-driven machines to electric-driven has affected almost all industries in one way or another. As always with new technology, it brings new and exciting possibilities, but it also comes with the risk of misunderstandings, insecurity, and even fear, as new technology like electrified vehicles and machines replace old well-known diesel-driven alternatives.

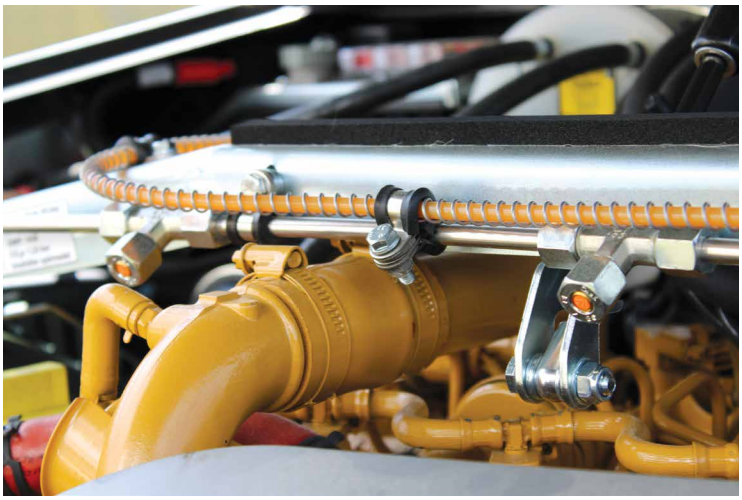
For electric machines, the risk of fire is one example of this.

Unfortunately, this lack of experience is sometimes exploited to create a market by making the customer insecure and to promote a product that might not be needed or might not do what is expected from it.

THE PROBLEM

New technology means there will be a lack of experience. It also means that there will be both a steep learning curve and a fast development of the product. What we do today might be outdated tomorrow.

Fires or thermal incidents in vehicles and machines are more common than you would expect. Heat, fuel and oxygen are all you need. Although electric vehicles



are involved in fires less often than fossil fuel-driven machines and vehicles it sometimes seems like the fear of a fire is greater with electric machines.

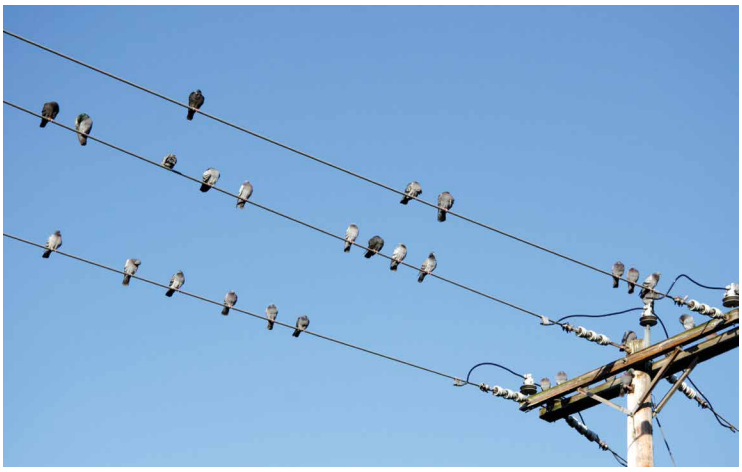
So, what is the problem? When you mention fires and electric vehicles in the same sentence, most people think about the lithium-ion battery and the devastation a fire in such a battery can result in.

The important thing to remember is that the battery is only one object of many in an electric machine that a fire can originate from. Many other components contain fuels, components that are or can be hot etc. While there aren't enough statistics available on fires in electric vehicles, the limited data suggests that it is more likely for a fire to start outside the battery and not involve the battery at all, rather than a fire where the battery is involved.

SOLUTION

So, what can you do? All machine models are unique, and they are used differently and in different environments. All this matters when it comes to risk. A well-performed fire risk analysis is the first step to a safer machine and a safer workplace. If the conclusion

"THE IMPORTANT THING TO REMEMBER IS THAT THE BATTERY IS ONLY ONE OBJECT OF MANY IN AN ELECTRIC MACHINE THAT A FIRE CAN ORIGINATE FROM."



"RESEARCH AND RECOMMENDATIONS FOR FIRE SUPPRESSION OF ELECTRIC VEHICLES HAVE CHANGED DRASTICALLY OVER THE LAST 10 YEARS."

from the risk assessment is that a fire suppression system is needed to mitigate risks, then it is important to choose a suitable fire suppression and detection system with a, for the area, suitable suppression agent.

All fires are gas fires. It is not the liquid or the solids that burn, it is the gases they release. This is of course a simple way of seeing it, but when considering this, do you really need a special fire suppression for an electric vehicle? In most cases no. Many fire suppression systems that are used for conventional vehicles today can be used with good results on electric vehicles as well. Today there are several different suppression agents in use. Each agent has its benefits and drawbacks. It is important to choose an agent that fulfils your demands and to be aware of and handle the downsides.

Research and recommendations for fire suppression of electric vehicles have changed drastically over the last 10 years. From recommending non-water-based agents to recommendation of water-based agents. The reason for this is the good cooling properties of water-based liquids. Cooling is a very effective way of suppressing a fire and water is a phenomenal chemical when it comes to absorbing heat. If you remove the heat, you will also remove or at least minimise the risk of re-ignition once the fire suppression system has been activated and emptied.

Electric machines and vehicles are subjected to water all the time; rain, road splash, washing and cleaning, high humidity, condensation etc., and they are designed for this.

It is a long-lived myth that water cannot be used to suppress fires in electric components. We all heard of the dryer or toaster in the bathtub and the myth still lives, although we know it does not work like that. In vehicles and machines, fire suppression systems are typically installed where there are no humans. To be electrocuted you need to be in contact with both the positive and negative terminal. Otherwise, you don't create a circuit and there will be no flow of current. Add to that that the high voltage parts in electric machines carry multiple safety features to avoid any dangerous situations.

There is also the possible mix-up with lithium-ion batteries and lithium batteries that could have contributed to the myth that water newer can be used near electric vehicles. Lithium batteries should not be extinguished with water since they contain lithium in their metal form, and they can react with water and create hydrogen, which reacts violently to fire. Lithium-ion batteries do not contain any metal Lithium and do not possess that risk.

It is still very difficult to extinguish a lithium-ion traction battery pack for a vehicle or machine if the battery pack is in thermal runaway. The reasons for this are:

"IT IS A LONG-LIVED MYTH THAT WATER CANNOT BE USED TO SUPPRESS FIRES IN ELECTRIC COMPONENTS."

1. You cannot reach the source of the fire if it starts inside the battery pack and the fire suppression system is installed outside the battery pack. The agent will simply not reach the source of the fire.
2. The quantity of suppression agent needed to cool down and keep a lithium-ion battery pack under control would need to be more than it is reasonable to carry on the machine. It might be possible to buy some time for evacuation with a fire suppression system but stopping a fully evolved lithium-ion battery is very difficult.

The question you should ask is, are battery fires a high risk? Risk = Severity x Probability. The severity is high for a battery fire but the probability is in most cases low, so the risk will be low or medium. There are perhaps higher risks that you should focus on.

The two major reasons for a battery fire are collision and external fire.

A fire suppression system will not protect against collision, but it can protect a battery pack from an external fire. Given what we know so far it is more important to ensure that a fire cannot start anywhere else in the machine and spread to the battery than to try and protect the battery.

To conclude:

- Look at the whole picture, what risks do we have within the machine? How do we use the machine? What environment is the machine used in? And so on.
- Do a risk assessment.
- Mitigate the high risks. If a fire suppression system is needed make sure that you choose one suitable for the task.
- Ensure that the machines and fire suppression system are serviced according to the manufacturer's instructions.
- Learn from your incidents. A risk assessment is only more or less qualified guessing. Time will tell if you made the correct assumptions. Be sure to revise your risk assessment if you get new facts and improve how you deal with the risks.

SUMMARY

Fires in electric vehicles and machines are less common than in conventional machines. However, electric vehicles and machines can still need a fire suppression system. A well-performed risk assessment is the foundation for a higher level of safety. Ensure that all aspects are included in the risk assessment. Mitigate the risks but remember to also follow up when new information is available to ensure the safety of your colleagues, employees and business.

ABOUT THE AUTHOR

Gustav Stigsohn has a Master of Science in Mechanical Engineering from Linköping University and works at Fogmaker International as a Product Owner. Gustav started working at Fogmaker in 2010 and has worked mainly with product testing, product development and product certification of the Fogmaker Fire Suppression and Detection System.

ABOUT THE COMPANY

Fogmaker International is a Swedish company that manufactures fire suppression systems with high-pressure water-based mist for engine rooms and other enclosed spaces. The company was founded in 1995 and has partners in more than 60 countries. There are more than 300,000 Fogmaker systems installed around the world.

"A WELL-PERFORMED RISK ASSESSMENT IS THE FOUNDATION FOR A HIGHER LEVEL OF SAFETY."

EXPLORING FOGMAKER'S ADVANCED FIRE SUPPRESSION SYSTEM

Margherita Bruno, Editor, Port Technology International, interviewing **Fredrik Rönnqvist**, Key Account Manager, Fogmaker International

How does the introduction of Eco 1 contribute to the overall safety and sustainability of port operations?

In terms of safety, the effect is the same. This is a very good solution for suppressing fires in vehicles and machinery, the properties are the same so there is no reduction in efficiency. In terms of sustainability, this is a great leap forward in safeguarding the well-being of our nature, its oceans and ground waters.

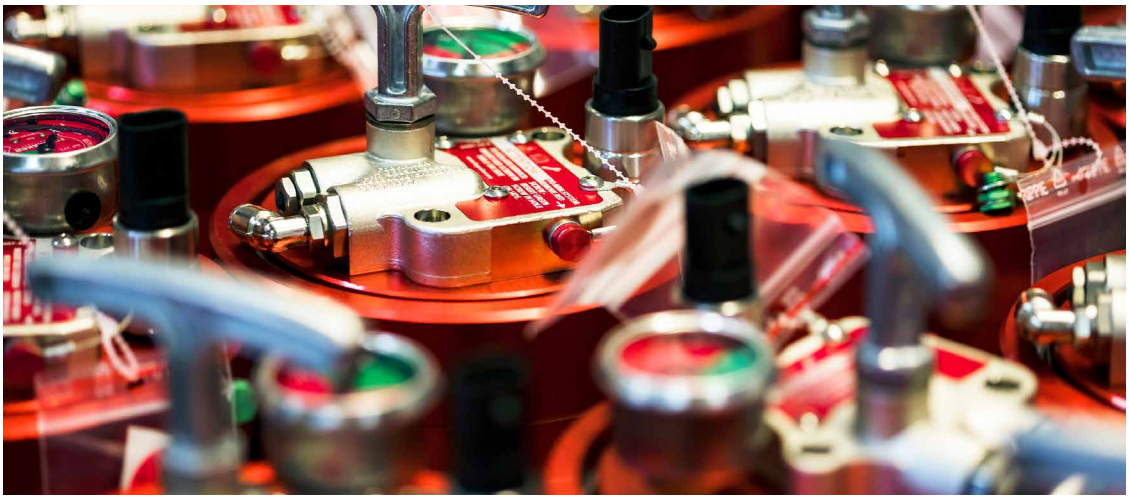
Can you elaborate on the specific benefits of Eco 1 in terms of environmental impact and its role in supporting port safety standards?

The Eco 1 solution is not just meeting the thresholds for being considered fluorine-free but Eco 1 has no fluorine in it at all, meaning that PFAS is completely removed. Fogmaker has taken the step from a low-content PFAS to a zero-content PFAS solution. Eco 1 has been validated by third party Green Screen and received its silver level certificate. By achieving this Fogmaker is making it easier for ports to uphold their safety standards while simultaneously adapting to the ever higher demands on sustainability around the world. Fogmaker Eco 1 is a product developed from the idea of not compromising between efficiency and sustainability. Still, all through the development the idea was always to achieve safety as well as sustainability.

Considering the increasing focus on sustainability in the industry, how does Fogmaker address concerns regarding traditional fire suppression systems and their environmental footprint?

Aside from the fact that Eco 1 was developed with this very notion in mind, Fogmaker is also taking all kinds of precautions to reduce the environmental footprint from start to finish in the development and production cycle. Every aspect is being questioned, how much do we travel, what kind of fuel do our company cars and service vans use and who are the most sustainable suppliers and partners. The Fogmaker Fire Suppression system is designed to last for decades and to be refurbished, refilled and re-activated upon activation, rather than having to be replaced every so often. All materials and suppliers are being scrutinised not just in terms of quality and cost but also in terms of their environmental footprint.

In what ways does the adoption of Eco 1 align with industry trends towards electrification



and reducing carbon emissions in port operations?

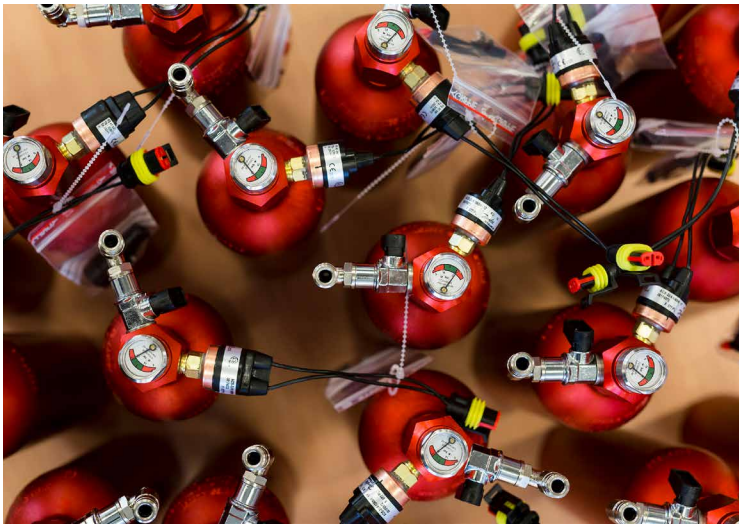
Eco 1 is developed to be suitable for all markets and all types of vehicles including EVs. As the industry moves towards electrification, Eco 1 is designed to meet the changing needs without requiring new suppliers or products. Furthermore, old systems can be updated and used with Eco 1, so even the installed base can backtrack and get a more eco-friendly fire suppression system. The system as such is very light and it prompts less fuel consumption than many other systems installed.

Could you share insights into the reception and adoption of battery-electric machines in the port industry, and how your fire suppression systems, particularly Eco 1, complement these advancements?

It is clear that the industry is progressing toward an electrified machine fleet and in that development Eco 1 perfectly complements the harder demands on environmental responsibility. Eco 1 was recently launched so it remains to be seen how it is accepted in the industry but early signs tell us that this is what the customers are asking for.

How does Fogmaker position itself as a leader in promoting both safety and sustainability in port environments, especially amidst growing concerns surrounding traditional fire suppressants and their environmental impact?

The Fogmaker product is backed by independent laboratory tests which show that it is one of the leading products on fire suppression. When combined with the eco-friendly Eco 1, it positions us as the natural choice for ports that are conscious of both safety and sustainability. Taking PFAS out of the equation removes some of the concerns regarding the environmental impact of traditional fire suppressants.



ABOUT THE AUTHOR:
Fredrik Rönnqvist works as Key Account Manager at Fogmaker International and is responsible for the Material Handling segment.

PORTO ITAPOÁ DEVELOPS IN-HOUSE EXCLUSIVE EMERGENCY CAGE FOR RESCUE

"THE EXISTING OFFER OF THIS TYPE OF EQUIPMENT IN EUROPE DID NOT MEET OUR SPECIFIC NEEDS, WHICH PROMPTED OUR TEAM TO DEVELOP THE NECESSARY SOLUTION INTERNALLY."

In conversation with **Porto Itapoá**

In a pioneering initiative in the Brazilian port scenario, Porto Itapoá has introduced a unique and innovative solution for emergency situations: its rescue cage. Faced with the absence of such equipment in the national market, the Porto Itapoá team decided to take the lead and create a cage that would meet the specific needs of port operations.

The cage will be used for rescues in critical situations, according to Porto Itapoá's Director of Operations, Technology, and Environment, Sergni Pessoa Rosa Jr. "The existing offer of this type of equipment in Europe did not meet our specific needs, which prompted our team to develop the necessary solution internally," he explained. The equipment stands out for having four doors, providing easy access for rescue teams.

This feature has been carefully planned to optimise rescue operations in emergency cases, ensuring efficiency and prompt response. Additionally, the equipment will have a system for hoisting and allocating potential accident victims, facilitating manoeuvres and making rescue even faster, including in maritime situations. "It is a significant addition to our operation, but one that we hope to never use," said the Terminal's Director.

The conception of the emergency cage involved a collaborative approach, with active participation from various sectors of Porto Itapoá. "Attentive listening and the integration of feedback were essential to ensure that the equipment met the real demands of rescue in the port environment as accurately as possible," commented Rosa Jr.

By becoming the only port in Brazil to have this safety innovation, Porto Itapoá reinforces its commitment to operational excellence and life protection. The emergency cage not only represents a significant advancement in preparing for critical situations but also highlights Porto Itapoá as a hub for innovation and safety in the national port scenario.

SECURITY AND SUSTAINABILITY

Porto Itapoá, in partnership with the surveillance company Segurpro, adopted electric vehicles to carry out motorised security patrols on the Terminal's premises. With this measure, in this type of operation alone, the company stops emitting more than four tons of carbon per year. The amount is equivalent to the 36,000 kilometres the vehicle travels annually.

For Porto Itapoá's Port Security Manager, José Aurélio Kalfeld, the initiative reflects the commitment

to excellence, sustainability, innovation and security, values shared by both companies. "In addition to the environmental benefits, with the significant reduction in carbon emissions, the 100 per cent electric vehicle will have its batteries recharged at the port's own facilities, eliminating the need to travel to gas stations", he explained.

The fact of recharging the vehicle within the port itself, highlighted Kalfeld, has an important impact on operational efficiency. "Risks related to trips to the gas station are avoided. Furthermore, we will not have the absence of a security professional at the Terminal, which would occur during the supply period".

ENERGY TRANSITION

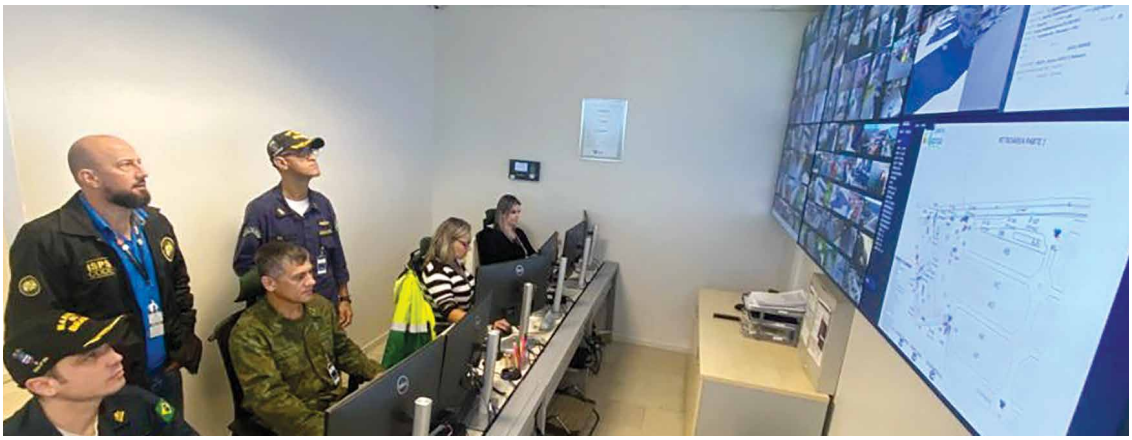
Porto Itapoá has stood out in the business scene, demonstrating its commitment to the energy transition. Through a strategic approach, the company has implemented a series of measures aimed at significantly reducing its carbon footprint and promoting sustainable practices.

The port won for the second time, in 2023, the gold seal of the GHG Protocol, a programme implemented in Brazil by the Center for Sustainability Studies of Fundação Getúlio Vargas (FGVces) in partnership with the Ministry of the Environment. Furthermore, it acquired new autonomous Rubber-Tyred Gantry cranes (RTGs) – it will be the first terminal in South America to operate them – which consume up to three times less fuel than conventional ones. In total, in 2023 more than $40 million were invested in this equipment.

NEW ENERGY POLICY

In 2023, Porto Itapoá changed its energy acquisition policy in the national system, opting to consume, in the new contracts, only energy from renewable sources. The transaction is certified by I-REC(e), a global renewable energy attribute tracking system designed to facilitate reliable accounting of renewable energy that is attributed to the consumer.

"THE CONCEPTION OF THE EMERGENCY CAGE INVOLVED A COLLABORATIVE APPROACH, WITH ACTIVE PARTICIPATION FROM VARIOUS SECTORS OF PORTO ITAPOÁ."



INVESTMENTS IN ITS MONITORING AND INCIDENT RESPONSE SYSTEM

Once again at the forefront of port security and technology, Porto Itapoá opened a Security Room with a simulated exercise carried out in conjunction with the Brazilian Navy. For the development of the space attached to the Control and Communication Center (CCCom), Porto Itapoá received guidance from a specialist in crisis management methodology from the Federal Police. The Security Room is part of investments of BRL3.75 million ($750,000), which also include a new monitoring system, in addition to new cameras, strategically installed in all areas of the terminal and a video wall for monitoring images, replacing the old monitors.

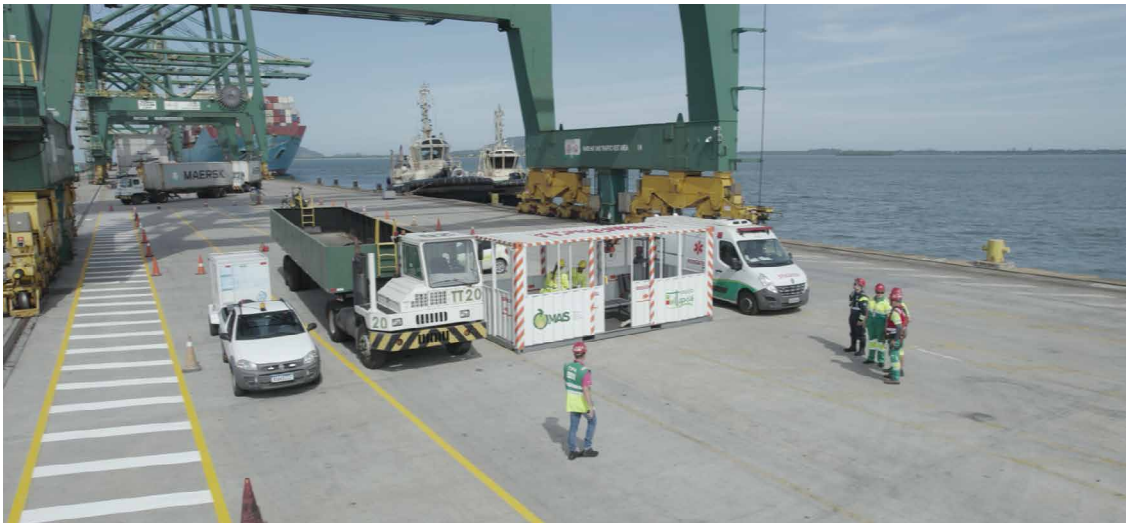
The system now features Artificial Intelligence (AI) and thermal cameras for better viewing at night and on foggy days. According to José Aurélio Kalfeld: "This embedded AI technology provides greater quality and accuracy in monitoring, minimising the risk of human error and co-option of people by organised crime".

PRIVATE CONTAINER TERMINAL WITH THE HIGHEST GROWTH IN BRAZIL IN 2023

Porto Itapoá achieved the notable 4th position in the National Waterway Transport Agency (ANTAQ) ranking, making it the private container terminal with the highest growth in Brazil for the year 2023 compared to 2022. In the past year, Porto Itapoá moved over 1 million TEU, showcasing a remarkable growth of 20.3 per cent compared to the cargo handled in 2022. This increase, the highest among private ports and the top five container movers in Brazil reflects Porto Itapoá's commitment and operational efficiency in making significant contributions to the Brazilian port sector.

ABOUT THE PORT:

Porto Itapoá began operations in June 2011; it is considered one of the most agile, efficient, safe and sustainable terminals in Latin America and one of the largest and most important in the country in the movement of containerised cargo, according to ANTAQ. Located in Babitonga Bay, on the north coast of Santa Catarina State (South Brazil), among the most productive regions in the country, covering importers and exporters from different business segments.



Panasonic CONNECT

TOUGHBOOK

The Role of 5G Private Networks in Building Smarter Ports.

With global freight trade demand expected to triple by 2050, ports and harbours are looking to new technologies to help them optimise yard and terminal operations.

IoT has the power to seamlessly connect humans, data, cargo, and machinery across the full spectrum of port operations to offer:

- Live asset tracking and container monitoring
- Improved safety, security, and environmental impact
- Higher operational uptime through predictive maintenance
- Faster cargo and terminal traffic processing

But what does this mean for connectivity requirements and mobile devices?

5G private networks for ports and harbours

Learn more about the global trends shaping ports and harbours, and how 5G private networks and rugged devices can play a crucial role in propelling maritime operations into the future.

Download guide

PORT SECURITY AND INNOVATION

SMART CONTAINERS: THE EYESEAL DEVICE

Enrique Acosta, CEO and co-founder, EyeSeal Information Systems, and **Thibo Clicteur**, Senior Consultant, Deloitte

FROM ENHANCING THE SECURITY OF CONTAINERS TO THE ESTABLISHMENT OF FAST LANES

In the intricate tapestry of global commerce, where the seamless transit of goods in containers forms the new standard, the role of container breach detection devices emerges as both pivotal and prescient. These devices, far from being mere technical fixtures, serve as a crucial line of defense against illicit activities such as the theft of goods, the smuggling of contraband and the infestation of narcotics. As trade grows in volume and complexity, mirroring the labyrinthine nature of global supply chains, the reliance on such technologies transcends mere preference to become a necessity.

Enter EyeSeal's innovative container breach detection device. Apart from its primary security function, it also harbours the potential to establish a highly efficient and reliable fast-lane system. By doing so, EyeSeal's technology could be a game-changer with the potential to redefine efficiency in the current logistics landscape, promising swifter customs clearances and streamlined container processing. In an era where time is tantamount to currency, such advancements are not just beneficial but essential. The deployment of these devices, therefore, is not just a step but a leap towards fortifying the arteries of international trade, ensuring they pulse with security and efficiency.

ENHANCEMENT OF CONTAINER SECURITY

EyeSeal, a trailblazer in container security, has unveiled a device that marks a significant leap forward in addressing the multifaceted challenges of global trade and logistics. This innovative gadget is not merely a tracker, but rather a sophisticated amalgamation of Internet of Things (IoT) sensors, location tracking, and

"THROUGHOUT OUR COLLABORATION DURING THE GATEWAY BRITAIN PROJECT, WE HAVE EXPERIENCED EYESEAL AS A KNOWLEDGEABLE, TRUSTWORTHY AND PUNCTUAL PARTY IN THE PREPARATION AND EXECUTION OF A NUMBER OF CLOSELY MONITORED PILOT SHIPMENTS FROM THE EU TO THE UK, DURING ITS TECHNOLOGY WAS SUCCESSFULLY TESTED."

Daan De Vlieger, Partner Global Trade Advisory

FIG 1.
Internal mounting of the EyeSeal device

communication technology, designed to meticulously monitor the status of shipping containers.

At the heart of EyeSeal's offering is the ability to detect and report real-time changes in critical parameters like temperature, humidity, location, and security status, notably the opening of container doors. This feature provides stakeholders in the supply chain with an unprecedented level of visibility into both the condition and location of their cargo throughout its journey. Such comprehensive monitoring is invaluable, not only in preventing theft and epitomising access but also in preserving the integrity of sensitive or perishable goods.

A distinctive aspect of the EyeSeal device is its installation methodology. Unlike conventional systems that attach to the container's exterior, EyeSeal's innovation is strategically mounted inside, offering an added layer of security and discretion. The mounting of the EyeSeal device within a container is illustrated in Figure 1.

The data collected by the EyeSeal device is streamed in real time to the EyeTrack platform, a digital nerve centre capable of integrating seamlessly with existing logistics infrastructures. This includes Transport Management Systems (TMS), Port Community Systems (PCS), and even national customs authorities' networks, as shown in Figure 2. In the event of deviations from pre-set conditions or potential security breaches, EyeTrack acts swiftly, sending alerts to relevant stakeholders. Moreover, it generates comprehensive trip reports for containers equipped with the EyeSeal device, providing a detailed account of the journey. An example of a trip report is depicted in Figure 3, the user interface is displayed in Figure 4.

This capability for external integration is not just a boost to operational efficiency; it represents a paradigm shift in the way supply chains are managed. By fostering a more secure, reliable, and transparent global trade network, EyeSeal and its EyeTrack platform are setting new standards in the domain of logistics and international commerce.

Establishment of a fast lane

In the lexicon of global logistics, the term "fast lane" has taken on a revolutionary significance, epitomising a dramatic shift in the movement of goods across borders. This concept is not merely about speed; it represents a fundamental overhaul in how shipments navigate the often-maze-like process of customs clearance.

At the crux of this transformation lies the innovative EyeSeal device, a harbinger of the "smart container" era. As previously described the device actively gathers and reports on the container's internal conditions and, crucially, its breach status. The implications for customs

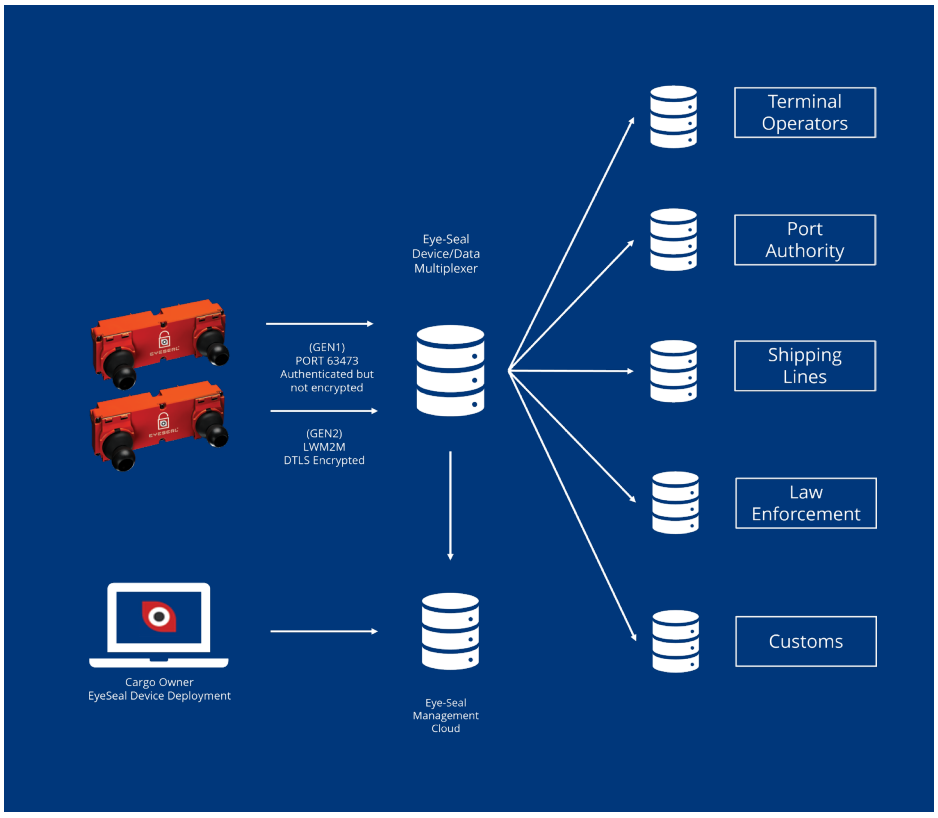


FIG 2.
Integration with external systems

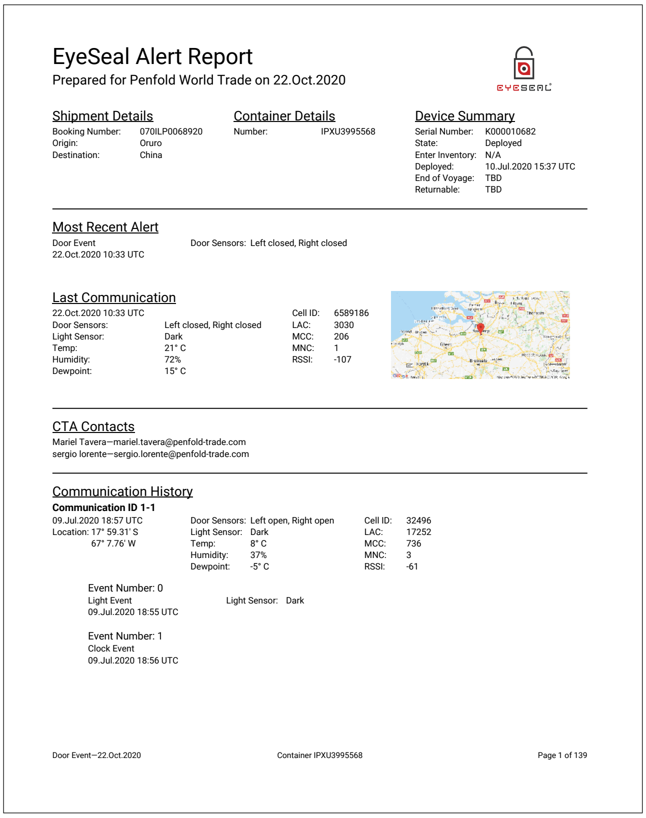
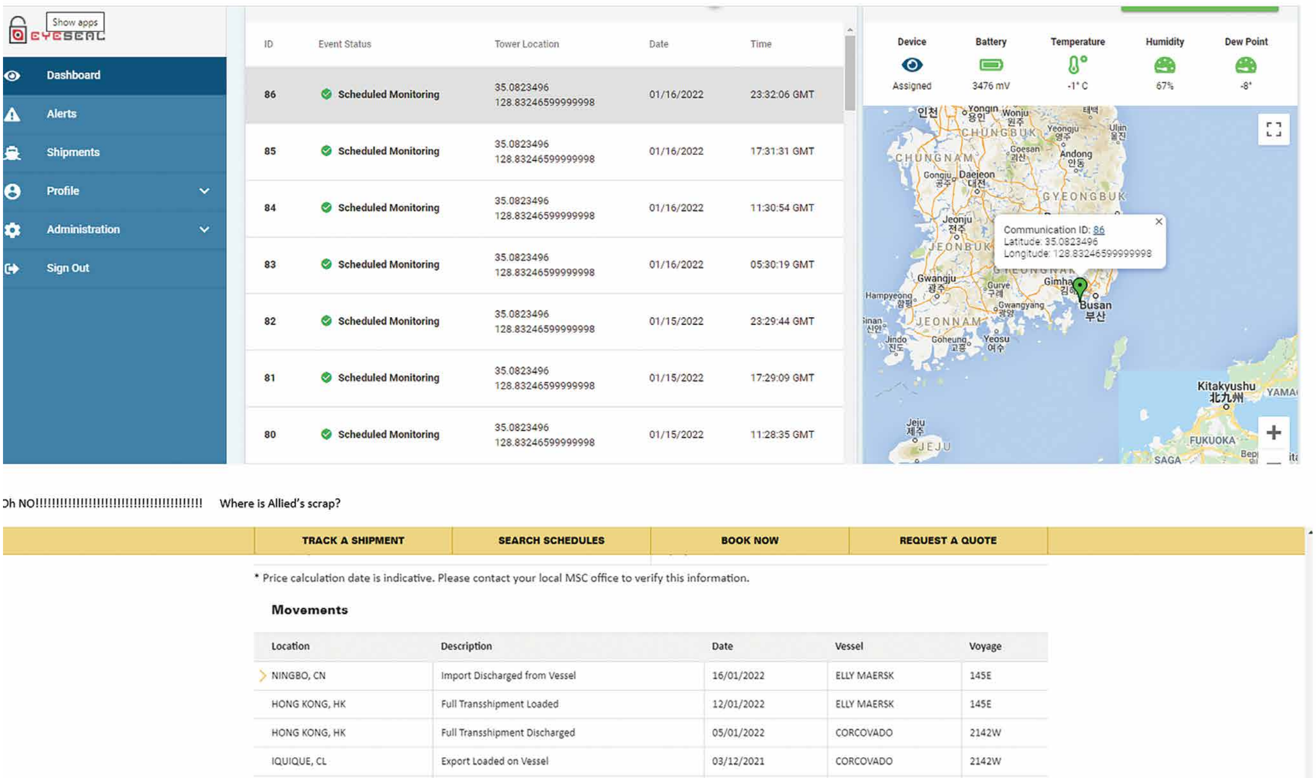


FIG 3.
Trip report of a container

procedures are profound: traditionally, a bottleneck in the supply chain, customs clearance can now be expedited, thanks to the data relayed by EyeSeal. If the device indicates an unbreached status, customs authorities in the destination country have the option to green-light the clearance of goods almost instantaneously. This is the essence of the "fast lane" – a streamlined, efficient and faster passage of the goods at borders. The unsecured, normal container flow is presented in Figure 5, where the red areas show potential areas of vulnerability for theft, contraband insertion, or narco-infestation. The secure, fast-lane container flow is depicted in Figure 6.The benefits of this innovation are manifold. The acceleration of transit times leads to tangible gains in supply chain efficiency and agility. But the ripple effects extend further, manifesting in cost savings and heightened customer

FIG 4.
User interface of the EyeTrack platform



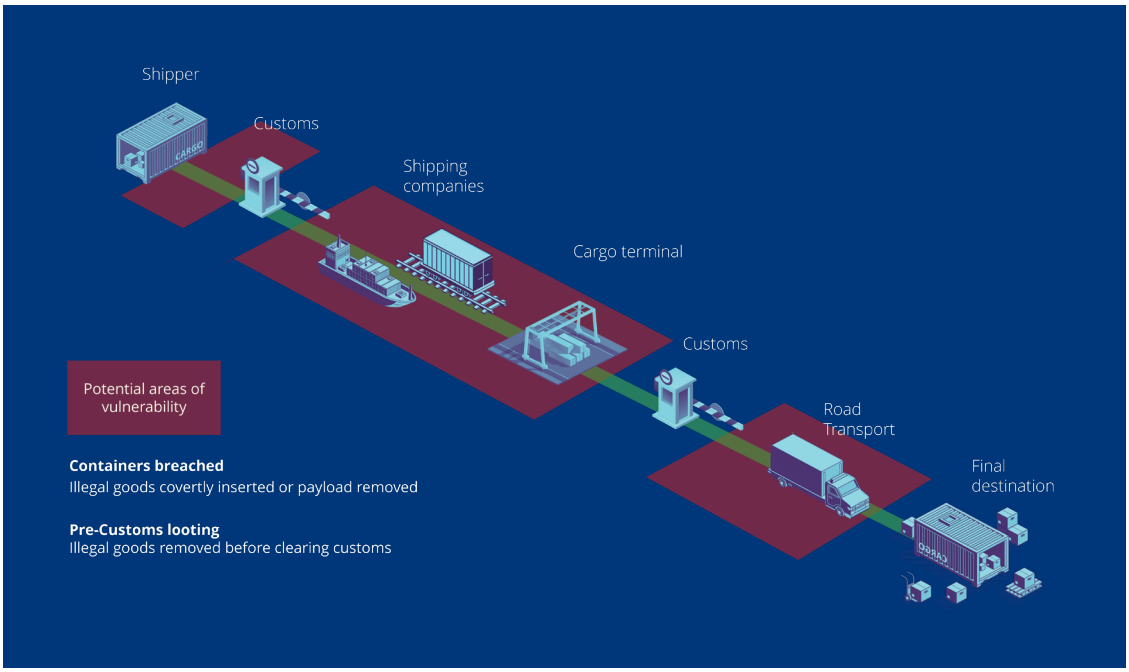


FIG 5.
Unsecured, normal container flow

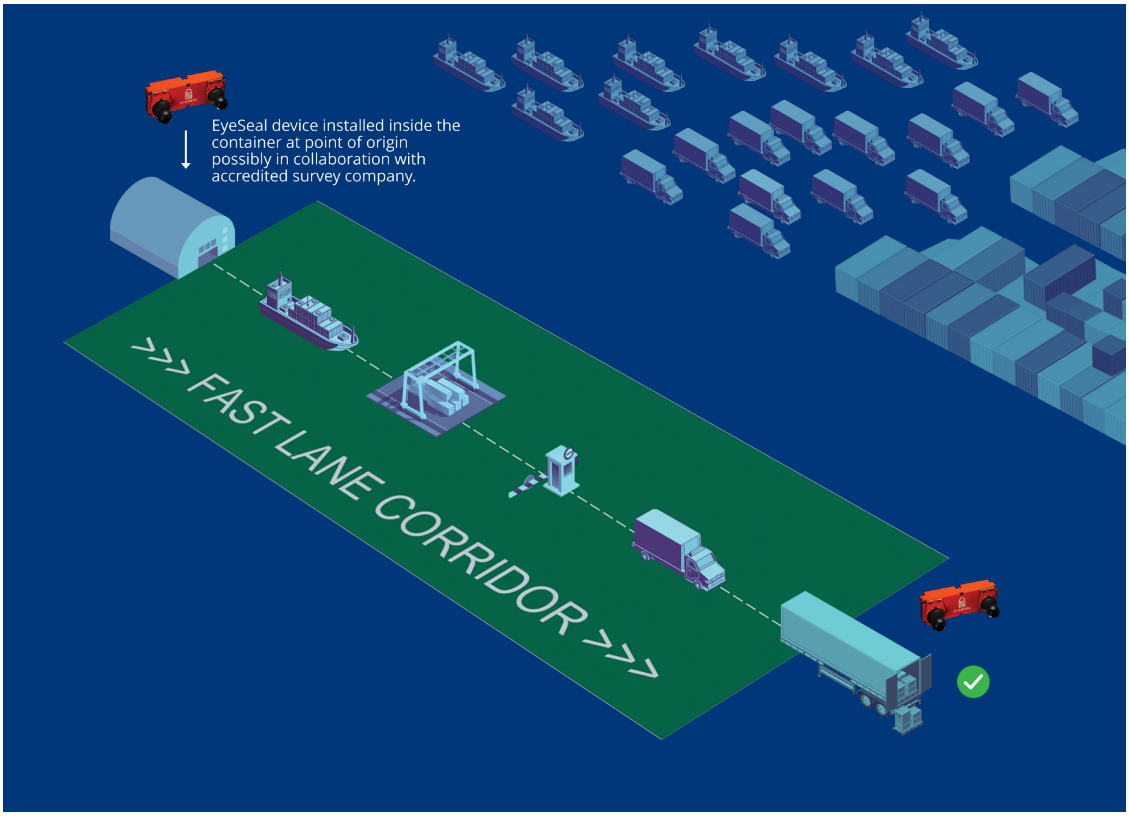


FIG 6.
Secured, fast-lane container flow

satisfaction. In an era where speed is synonymous with competitive advantage, the EyeSeal-enabled "fast lane" in logistics is not just an advancement, but rather a reinvention of the rules of international trade.

ECOSYSTEM BENEFITS

The advent of the EyeSeal device in global trade has heralded a new era, showering a plethora of benefits across both private and public sectors, in realms spanning cargo security to operational efficiency.

For exporters, EyeSeal is nothing short of a game-changer. It allows exporters not only to monitor their cargo in transit but also to intervene promptly in case of

potential breaches, thus mitigating risks effectively. Additionally, the integration of the "fast lane" concept significantly trims down transit times, which is especially important for time-sensitive shipments.

Third-party logistics providers (3PLs), encompassing freight forwarders and customs brokers, now find themselves armed with a potent tool. EyeSeal bestows upon them the capability to offer clients real-time visibility of their cargo, which is not just about tracking but also about the enhancement of efficiency and the diminishment of liability risks.

Transportation companies, including road carriers, shipping lines and airlines, also reap substantial benefits. With EyeSeal, they are empowered to make more strategic transport decisions, as the data harvested by the device can swiftly identify breaches.

Insurance companies join the cadre of private beneficiaries, as EyeSeal's precise tracking and reporting enhance the quality of their risk assessments and decision-making processes.

On the public stakeholder front, customs authorities find in EyeSeal a tool for smarter enforcement. The device's alerts allow them to target inspections more effectively, facilitating legitimate trade while clamping down on malfeasance. This targeted approach not only streamlines operations but also potentially boosts tax revenue (import duties, excises, VAT) by unearthing non-reported or illegal imports.

Law enforcement agencies also gain a formidable ally in EyeSeal, receiving timely intelligence about suspicious activities, thereby enabling quicker, more effective responses to security threats.

Lastly, port authorities find in EyeSeal a solution to perennial congestion issues. By reducing bottlenecks, EyeSeal contributes to optimised capacity management at port terminals, a critical factor in maintaining the smooth flow of global trade. This optimal capacity management equally benefits the terminal operators that are active within the port.

In essence, EyeSeal stands as a beacon of innovation, illuminating the path to a more efficient, secure, and transparent global trading ecosystem, benefitting a broad spectrum of stakeholders from private exporters to public law enforcement.

ABOUT THE AUTHORS:
Thibo Clicteur is a Senior Consultant in Deloitte's Global Trade Advisory team in Belgium. Given his background as an engineer, he focuses on operational port projects around modeling and improving logistics processes. He has a strong focus on digitalisation and technologies that facilitate international trade. Thibo is currently involved in the Gateway Britain project, which aims to build a data sharing platform to facilitate trade between Flanders and the United Kingdom.

Enrique Acosta is a notable figure in the world of logistics and container security. He is recognised as the CEO and co-founder of EyeSeal Information Systems, a collaborative venture with Coremet Trading. Enrique, along with the dedicated EyeSeal team, has achieved significant milestones, including the development of the EyeSeal internal container breach solution, which has been granted two US patents. Moreover, he is leading EyeSeal deployment projects across all corners of the globe.

ABOUT THE COMPANY:
Deloitte
The Deloitte Global Trade Advisory team is a true end-to-end, integrated trade service provider and a trusted partner for their broad base of dedicated clients. Focusing on strategy, advisory, automation and compliance, the team has developed a comprehensive knowledge of trade regulations, operations and technologies.

EyeSeal
Founded in 2013 and located in Florida, EyeSeal has developed a ground-breaking innovative container breach detection technology in maritime logistics. It addresses the transportation industry's pervasive lack of visibility by exposing where and when unplanned container breaches occur, and insertion of drugs and contraband risk exists. EyeSeal has won the "IoT Evolution Supply Chain and Cargo Monitoring Product of the Year" Award in 2023.

"EYESEAL HIGHLIGHTS HOW THE BLENDING OF DEVICES AND CONNECTIVITY ENABLES EXCELLENCE AND INNOVATION, AND SOLVES THE CRITICAL ISSUES WE FACE IN THE WORLD."

Carl Ford, CEO Crossfire Media

SKYWARD VIGILANCE: DRONE SECURITY AT THE PORT OF ANTWERP-BRUGES PORT

"WHEN CONSIDERING SAFETY AND SECURITY USE CASES, THERE IS AN ADDITIONAL BENEFIT: FROM A SINGLE POINT, OTHER SYSTEMS AND SUPPLEMENTARY DATA SOURCES CAN BE EASILY ACCESSED VIA STANDARD WORKSTATIONS."

Margherita Bruno, Editor, Port Technology, interviewing **Bob Spanoghe**, Platform Manager Port of the Future, Port of Antwerp-Bruges

How does the implementation of the 'D-Hive drone-in-a-box' network specifically contribute to enhancing security measures within the Port of Antwerp-Bruges?

The D-Hive drone network provides our port authority with the opportunity to enhance general situational awareness in the port from a unique perspective, aiding in the coordination of safety and security aspects. These drones can be considered as flexible cameras that offer a bird-eye view, allowing us to observe various operational situations from behind our workplace.

Can you elaborate on the role of autonomous drones in addressing security concerns within the expansive 120-square-kilometre port area?

We can deploy the drone network for various use cases that contribute to the overall coordination of operational activities in the port. Specifically, we utilise drones to monitor ship traffic and manage berth assignments. These drones play a crucial role in detecting floating debris and oil spills and inspecting infrastructure such as quay walls, bridges and locks. Additionally, they assist during emergencies and support firefighting efforts in case of major incidents. Furthermore, we employ drones to enhance the safety of all port users in compliance with the International Ship and Port Facility's security code (ISPS) regulations

What's the build-up of the D-Hive network and how does it work?

The D-Hive drone-in-a-box network is structured as follows:

- The network comprises six drone-in-a-box units strategically positioned across the entire port area.
- These drones are controlled centrally from a command and control centre.
- Within this centre, port planners from the port authority determine when and where the drones should be deployed for specific use cases.
- Before each flight, a safety analysis is conducted, and flight authorisation is granted. The drone then takes off to execute its specific mission.
- Live streaming of imagery from the drone occurs during the flight, directly to the command and control centre.
- Port planners can intervene during the flight, adjusting the flight path and independently manipulating the camera. This flexibility allows for efficient drone deployment.
- Meanwhile, the pilot in command remains vigilant about safety aspects throughout the flight.
- After landing, the captured images are uploaded in high quality to the CCTV system, ensuring that they remain accessible for later reference

"THESE DRONES PLAY A CRUCIAL ROLE IN DETECTING FLOATING DEBRIS AND OIL SPILLS AND INSPECTING INFRASTRUCTURE SUCH AS QUAY WALLS, BRIDGES AND LOCKS."

What advantages does the Beyond Visual Line of Sight (BVLOS) capability provide in terms of security surveillance compared to Visual Line Of Sight (VLOS) flights?

The benefits of **Beyond Visual Line of Sight (BVLOS)** operations are substantial, and the ability to conduct BVLOS flights was a key requirement for the Port Authority to initiate this project. Given the vast expanse of the port area – spanning **120 square kilometres** – BVLOS represents the only feasible approach to rapidly and flexibly deploy drones. Sending drone pilots to specific locations for every situation would be impractical due to the considerable time lost in transit. Additionally, BVLOS technology enables the execution of all use cases efficiently and effectively

Could you explain how the command-and-control centre facilitates rapid response and coordination in security incidents leveraging the data gathered by the drone network?

The fact that the command and control centre is centralised within the port and that the drones can be operated from behind a workstation by port planners from the port authority provides significant advantages across various use cases. However, when considering safety and security use cases, there is an additional benefit: **from a single point**, other systems and supplementary data sources can be easily accessed via standard workstations. The dissemination of this consolidated information to all relevant safety partners can occur swiftly and efficiently. The command and control centre truly sits at the heart of coordinating such use cases.

How does the collaboration between the Port of Antwerp-Bruges and its partners in developing the drone network reflect a concerted effort to prioritise security in port operations?

When constructing the **D-Hive drone-in-a-box network**, we deliberately adopted a **drone-as-a-service model** in our search for partners. Our approach was twofold: first, as a port authority, we aimed to remain **flexible** and keep pace with rapidly evolving technological developments in the field of autonomous drones. Second, we wanted to remain **agnostic** regarding the legal framework required for BVLOS (Beyond Visual Line of Sight) flights. This legal expertise is best left to the drone operators.

Regarding sharing our capabilities and data with safety partners such as the fire department, police, and customs, we strongly believe in a **collaborative model** where information exchange is crucial. This way, each partner can leverage the available data and information within their specific mandate, addressing various safety and security aspects in a large seaport

ABOUT THE AUTHOR:

Bob Spanoghe is a member of the innovation enablement team at the Port of Antwerp-Bruges Authority. As an innovation Platform Manager, he focuses on the facilitation of the ideal ecosystems to accelerate technological development in the domains of drones and smart shipping. Currently, he's the Project Lead for the 'Port of Antwerp-Bruges Drone Roadmap'. The main goal is to introduce autonomous drones as a strategic asset to support the optimisation of the operational efficiency of the Port.

Bob is passionate about using innovative technology to support the transformation of the Port of Antwerp-Bruges into a port of the future. He was active as an IT professional in both the city of Antwerp and the Port of Antwerp.

ABOUT THE PORT:

With a throughput of 271 million tonnes, the Port of Antwerp-Bruges is a critical hub in worldwide trade and industry. It is home to 1,400 companies and accommodates the largest chemical cluster in Europe. The port provides a total of 164,000 jobs and generates an added value of €21 billion ($23 billion).

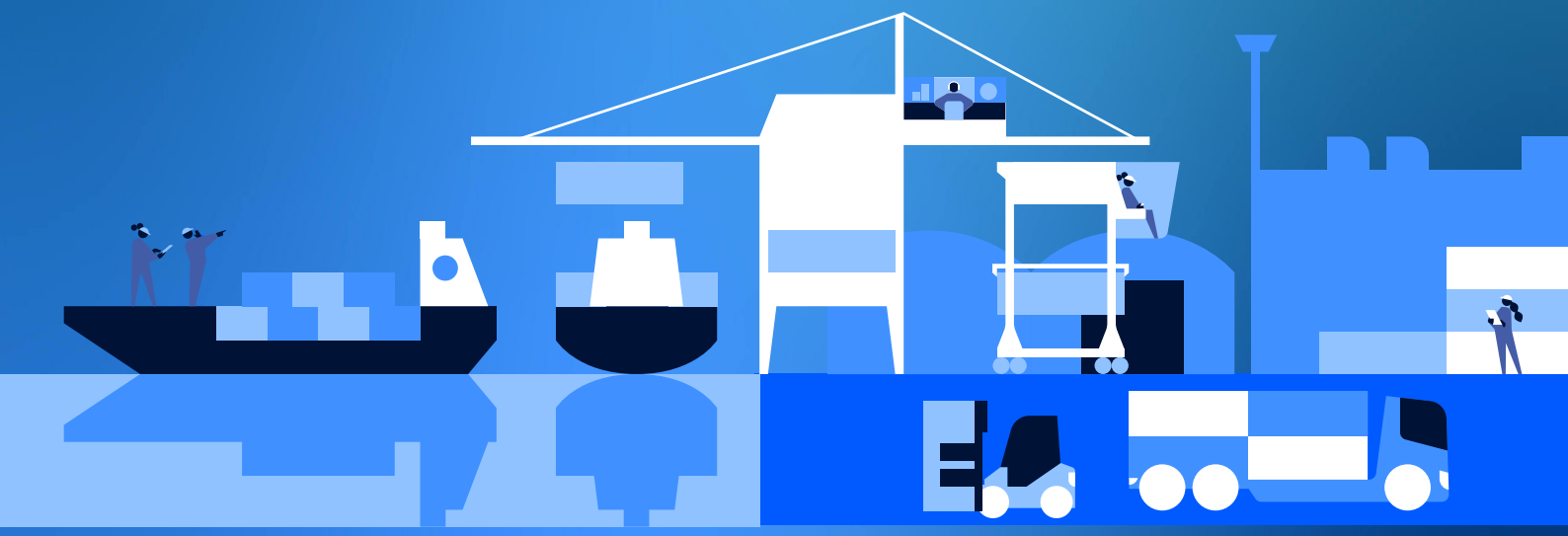
"PORT PLANNERS CAN INTERVENE DURING THE FLIGHT, ADJUSTING THE FLIGHT PATH AND INDEPENDENTLY MANIPULATING THE CAMERA. THIS FLEXIBILITY ALLOWS FOR EFFICIENT DRONE DEPLOYMENT."

NOKIA

Simplifying the digitalization of port terminals

Volatile market demands, shifting transport routes and growing vessel sizes pushed port terminal operators to become more flexible and resilient. Learn how Nokia digitalization platform helps enable the demanding use cases at ports.

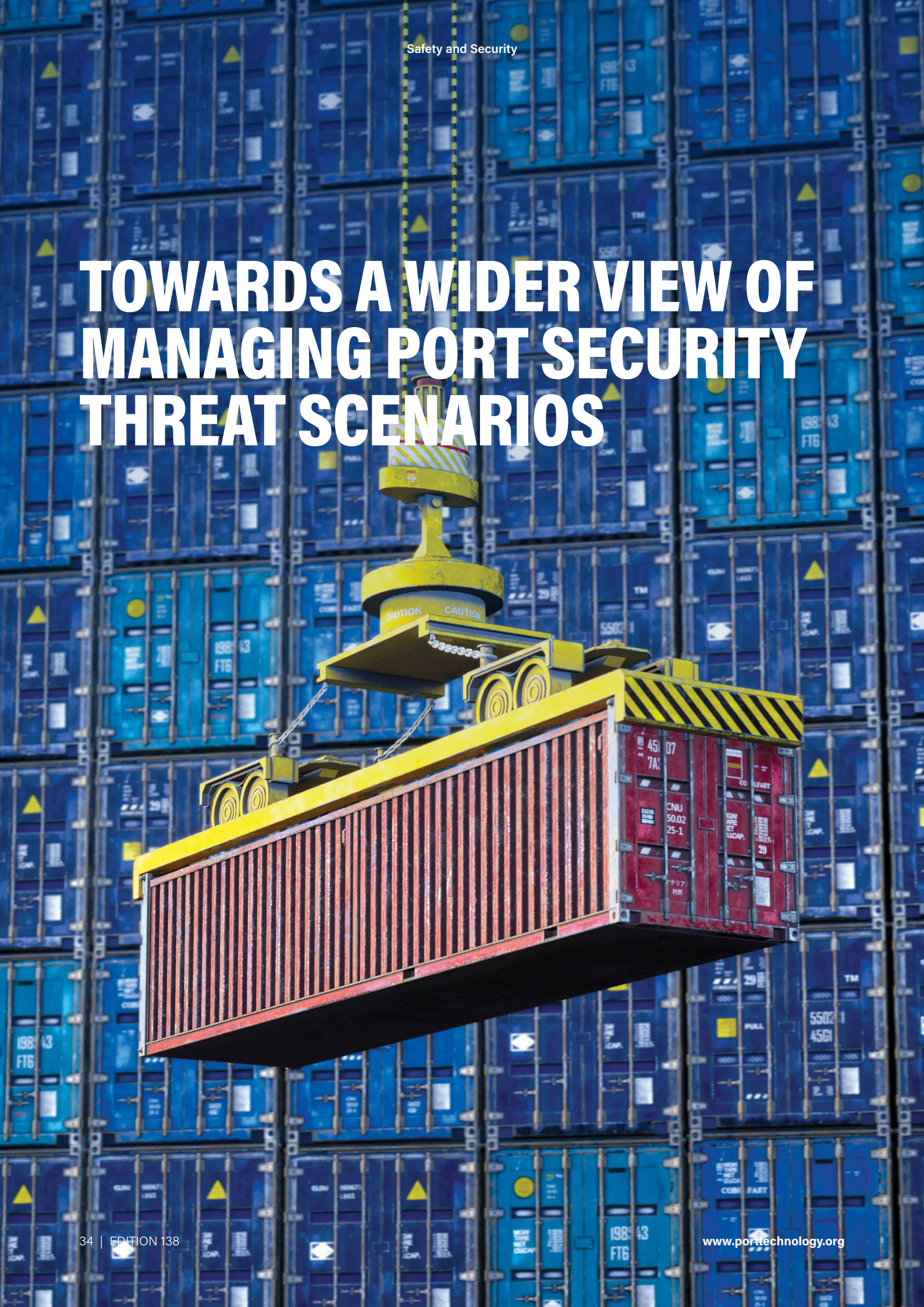
4G/5G private wireless & Wi-Fi | edge | apps | devices



Visit us to learn more

MARITIME CYBERSECURITY AND RISK MANAGEMENT

TOWARDS A WIDER VIEW OF MANAGING PORT SECURITY THREAT SCENARIOS



Richard Oloruntoba, Associate Professor in Logistics and Supply Chain Management, Curtin Business School, Curtin University, Perth, Western Australia

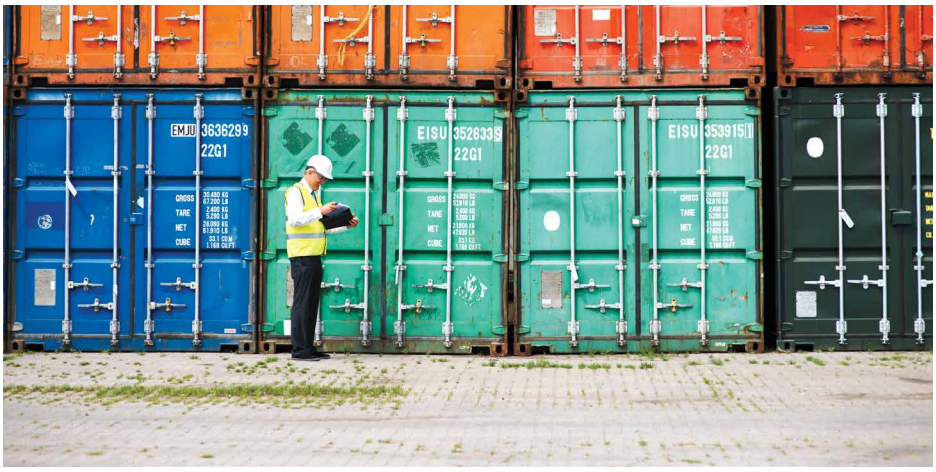
INTRODUCTION

Since the terrorist events of 11 September 2001, the attention of port managers and others has shifted to matters of port security, whether sea or air. Indeed, security and safety assurance across maritime trading systems has become a critical and ongoing factor for international business managers and international trade. Port security is a small part of broader maritime security. Port security has to do with treaties, defence and law enforcement, as well as counter-terrorism activities within the port and extending to the maritime domain. Since 9/11, port security measures have focused on the protection of (a) seaports (b) cargoes moving through the ports, and (c) personnel moving through or working in ports. Port security risk management focuses on the physical security of the port and its perimeters, its cargoes, the ships departing or arriving within port waters and the harbour, and any risks to the continuity of port operations as well as the safety of port data. Additionally, the port is connected to a much larger supply chain with various risks along the chain that can and do affect port security.

The International Maritime Organization (IMO) has a security framework of rules that govern port security globally. For instance, the 2002 International Ship and Port Facility Security Code (ISPF Code), and the Safety of Life at Sea (SOLAS) Convention address ship security and requirements for compliance with the ISPS Code, including ship identification, security planning, and alert systems that have been mandated, Similarly, the World Customs Organization (WCO) and the International Maritime Bureau (IMB) have supported processes that enhance broader regulatory coverage of safety and security within the world trading system.

In addition to IMO port security rules, the United States unilaterally introduced its own Container Security Initiative (CSI) and the Customs Trade Partnership Against Terrorism (CTPAT). The main aim of all these initiatives is to reduce the likelihood of maritime-vectored terrorism in port premises and other human-induced port security breaches. Although some analysts have argued against the implementation of port security governance measures based on

"SECURITY AND SAFETY ASSURANCE ACROSS MARITIME TRADING SYSTEMS HAS BECOME A CRITICAL AND ONGOING FACTOR FOR INTERNATIONAL BUSINESS MANAGERS AND INTERNATIONAL TRADE."



"HALF OF ALL MARITIME INCIDENTS IN 2022 OCCURRED IN PORTS AND TERMINALS."

its prohibitive costs, threats to competitiveness, and ineffectiveness, it appears there has been growing consensus internationally, in recent times, that security governance measures are a necessity because of new and evolving threats and risks. Examples of such new threats and risks include malicious port operations breakdown, illegal entry of contraband material including humans, fraud, geopolitical tensions, military conflict, cyber and ransomware attacks, and technological failures amongst others. Most recently, the handling and storage of lithium batteries in and out of electric vehicles is of increasing safety concern to ports. Half of all maritime incidents in 2022 occurred in ports and terminals according to Seatrade Global Port Report 2023, and when safety and security incidents disrupt operations, they can set off a cascade effect across the supply chain. In essence, economic and trading boundaries have become 'security' and 'safety' boundaries. Hence, this article argues that the expected reliability and assurance of port security and maritime trade will not arise from mere adoption, compliance, and implementation of port security governance frameworks alone. The article suggests that effective security outcomes will only result from properly integrating underlying risks, and safety and security concepts into existing managerial practice, and making sure they are systemic and sustainable.

The rest of the article is structured as follows: first, the article discusses several well-recognised risk factors within the international maritime trading system; second, it highlights the value of ports undertaking scenario and vulnerability analysis for on and offshore aspects of maritime commerce for preparedness. The article concludes by identifying a couple of urgent issues relevant to port security policy and management within the port and maritime supply chains.

COMMON RISKS: OLD AND NEW

Increasing trade volumes and sub-standard vessels

The United Nations Conference on Trade and Development (UNCTAD) in their 2022 report highlighted that in 2022 globally, 4.6 million port calls were recorded, and growing. The increased flows of trade, port calls, and increasing size of ships are sources of risk to safety and security in ports. The enormous trade volumes passing through ports have prompted them to pursue efficiency through automation and advanced information and communication technologies, which could also be a solution to personnel safety. Also, there are unknown risks arising from sub-standard vessels arriving in port, which could result in safety-related incidents that could disrupt port operations. A recent Seatrade article reported that vessel-related safety incidents in ports in 2022 alone resulted in 175 fatalities, 114 missing persons and 76 serious injuries, globally. Furthermore, 1,955 vessels were detained by Port State Control for 10,445 days for serious non-compliance with international safety regulations. Safety-related incidents could occur anywhere within the remit of the port authority such as while transiting channels, at berth, while using facilities, or while at anchorage. Hence, ports and harbourmasters need to pay close attention to managing this concern.

The complexity of modern port operations

A different perspective on risk factors for ports is the recognition of the complexity of modern port operations and the challenges of effectively implementing safety and security coverage over them. The Ammonium Nitrate explosion at the Port of Beirut on 4 August 2020 caused 204 deaths, more than 7,000 injuries, and a loss exceeding $ 15 billion, with 300,000 people left homeless. Tonnes of Ammonium Nitrate (AN) confiscated by Lebanese authorities from the abandoned vessel 'Rhosus' were stored in a warehouse within the port for almost six years without good safety management. The explosion was preceded by a fire resulting from welding work to repair the warehouse door.

With enormous volumes of international maritime cargo movements, and up to 90 per cent of world cargo movements by tonnage occurring in shipping containers, the size and complexity of ensuring safety and security staggers the imagination. Of this

trade, less than 10 per cent is subjected to physical inspection after arrival at a destination. The issue of complexity parallels a suite of practices that further add layers of risks and grounds for concern about safety and security matters generally. Security and safety risks often emerge from the interaction of factors such as:

- **The cargo and nature of cargo** – i.e. hazardous cargoes of a conventional, explosive, flammable, nuclear, chemical, or biological nature, and using cargo containers to smuggle people and/or weapons;
- **The vessel** – using the vessel as a tool or weapon or a means to launch an attack such as sinking a vessel in the channel or at berth to disrupt infrastructure;
- **The people** – using fraudulent identity in support of criminal and/or terrorist activities;
- **The lack of transparency in ship registration and ownership** – i.e., the absence of clear registration details, and anonymity of vessel ownership is a standard shipping industry practice that can enable a cloak of anonymity.

Cybersecurity risks

Seaports often deploy and are reliant on advanced information and communication systems that are in turn reliant on automated satellite-based internet systems. These information systems are vulnerable to being hacked for ransom, or hacked to disrupt port operations and in turn, global supply chains. Hacking of vessel-based systems may also be used to illegally track, mislead or divert vessels for hijack.

US seaports alone handle more than $5.4 trillion in goods every year, making US ports a unique target for cybercriminals. The same is true for major hub ports like Singapore, Shanghai, Hong Kong, Rotterdam, Busan, Ningbo-Zhoushan and others. Moreover, more than 500 cyberattacks were reported to have occurred in the global maritime industry in 2020, according to the U.S. Coast Guard. These cyberattacks were targeted at conventional information technology systems such as networks, data and proprietary information. The attacks include malware, ransomware, spear phishing and credential harvesting. Other attacks may target operational technology (OT) systems such as gantries, cranes, lifts and conveyance systems that lift on and lift-off cargoes on and off vessels, to paralyse port operations. Attacks may also aim at paralysis of port gates and truck loading and offloading operations.

"SCENARIO DEVELOPMENT AND ANALYSIS PROVIDE A MEANS FOR DECISION-MAKERS TO ANTICIPATE POSSIBLE INCIDENTS AND SCENARIOS AND STRATEGIES TO MITIGATE LIKELY ADVERSE IMPACTS."

Liquefied natural gas risks

The increasing import and export trade in liquefied natural gas is an emerging safety risk in an increasing number of offshore and onshore ports, globally. Port gas infrastructure networks are often extensive with storage, liquefaction, regasification and distribution networks in terminals. Liquefied natural gas (LNG) comprises explosive methane, butane, propane and ethane. Hence, many port terminals with LNG facilities are concerned about highly flammable LNG cargoes which is a safety and security risk to staff members, and adjoining communities and populations. The whole chain of supplies of LNG and storage must be securely and safely managed with sustained risk management processes put in place beyond the port itself.

SCENARIO AND VULNERABILITY ANALYSIS MAY BE A WAY FORWARD

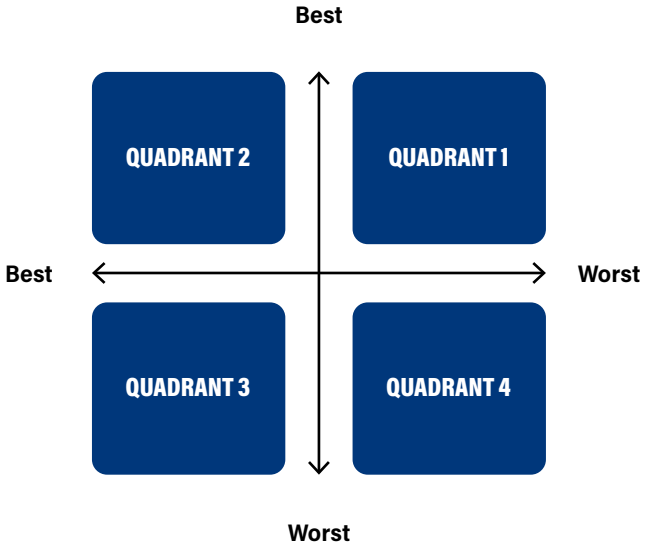
Scenario development and analysis provide a means for decision-makers to anticipate possible incidents and scenarios and strategies to mitigate likely adverse impacts. In the scenario methodology, each scenario considers how the future might eventuate by analysing past, current and possible situations or scenarios, and creating informed assumptions.

The scenario development process entails identifying past and current environmental pointers and constructing expressive images based on possible, and plausible, future happenings in the port. Plausible scenarios could be developed based on a desk review of relevant literature such as published case studies and exemplars, publicly known historical incidents and accidents, security analysts' reports, relevant media analysis and commentaries and similar other sources relevant to security and safety issues in the context of ports and their connected hinterlands and maritime supply chains. Such analysis of literature can be supplemented with a scenario thinking workshop informed by reconstructed historical accounts of past security and safety incidents, geopolitical debates, and accounts of knowledgeable individuals. The scenarios with the most significant uncertainties would then be selected for consideration, identification of possible outcomes, and development of managerial and policy recommendations. The process involves constructing expressive images based on possible, and plausible, future happenings and assessing their impact on operations, finances and supply chains. The next stage in scenario thinking is the generation of an impact and certainty matrix. This matrix reveals the impact and certainty/likelihood of each possible outcome of the studied event. Participants in a scenario thinking workshop would be asked to consider the current and future impacts of various dimensions of the scenarios, their level of certainty, and plausible scenario outcomes.

A consideration of the positive and negative aspects of the key issues is the focus of the scoping and building of scenarios. The threat dimensions of the scenarios may be dissected into four quadrants to provide the basis for scenario building on a best-worst continuum on each of the X and Y axes. The quadrants represent a set of conditions to define four possible combinations e.g., best-best, best-worst, worst-best and worst-worst conditions in which the impacts of a particular type of port safety and security risk might unfold. The worst-worst scenario is quadrant 4 with maximum adverse impacts and the best-best scenario is quadrant 2 with minimal adverse impact from the identified port security and safety risk.

Prioritisation of the worst-worst risks for management based on severity and certainty of impact is key to managing the most important port safety and security risks, and this would be different from one port to another. Some risks would be relatively manageable, whilst others would be more challenging to manage. Cyberattacks for example would likely exert an enormous adverse

"PORT SECURITY IS CRITICAL TO ECONOMIC SECURITY AS SEEN FROM VESSEL VOYAGES THAT HAVE THEIR DEPARTURE, ARRIVAL OR DESTINATION POINTS IN A PORT."



impact on port IT systems, as such disruptions and safety concerns are far more likely to occur, given the rapid pace of port automation and self-directed navigation of vessels. Maersk IT and communications systems were paralysed by the NotPetya worm for two weeks in 2017, affecting 800 vessels and 76 ports across the world, and costing the company almost $300 million.

Wider vulnerability analysis

Vulnerability analysis considers how vulnerable a port and its hinterland and overseas shipping connections are to the previously identified safety and security risks and the worst-worst scenario. Vulnerability analysis is conducted in four main steps. In the first step, AIS transponder data of vessels may be used to explore port-to-port seaborne trade of groups of commodities with other countries in the region and globally, e.g. iron ore, crude oil, or containers. The AIS data helps to identify ports involved in particular commodity seaborne trades within the shipping network. In the second step, we can gain insights into the role of the port being analysed for vulnerability within the network as regards the specific commodity group under analysis by varying a range of measures at the network and node levels.

In the third step, import chains of specified commodities are mapped to gain further insights into the vulnerability of a particular port. This mapping supports the fourth step, which includes a scenario analysis of port safety and security risks and broader maritime security threats such as those emanating from international shipping, and allied vulnerabilities. For example, current military challenges from Houthis in South Yemen in the Red Sea have had a significant adverse impact on port arrivals in ports in Sudan, Eritrea, Djibouti and Somaliland region, and on vessel traffic in the Suez Canal as many vessels re-route via the Cape of Good Hope in South Africa.

Hence, the concept of port security and operational disruption risks is broader than the physical security of port premises, infrastructure, approaches and channels. Port security is critical to economic security as seen from vessel voyages that have their departure, arrival or destination points in a port. This is because the port is a node in the network of vessel sailings for a specific commodity. For example, interruptions to vessels transporting crude oil from the Middle East/Persian Gulf to Japan are expected to affect the operations of receiving ports and refineries in Japan.

SUMMARY AND ISSUES OF PORT SECURITY POLICY AND MANAGEMENT

The article has discussed the concept of port safety and security and highlighted that port security extends to the broader supply chain with various safety and security risks along the chain, which affects port security, and thus requires management. The article discusses many well-known safety and security risk factors for ports within the international maritime trading system and suggests scenario and vulnerability analysis methods for managing risk and enhancing preparedness through mapping vulnerability within ports and across supply networks. Scenario development and vulnerability analysis provide a means for decision-makers to anticipate broader port-centric risks and mitigate likely impacts.

The article also suggests that the complexity of interactions between ports as nodes in a complex network of shipping, maritime operations, and supply chains create extensive vulnerabilities that simple compliance with CSI, CTPAT, SOLAS, ISPS codes and other WCO and IMB governance protocols would alone not mitigate. Hence, the need for systems-based supply chain-wide scenario and vulnerability management capabilities within ports.

ABOUT THE AUTHOR:
Richard Oloruntoba is an Associate Professor of Supply Chain Management at Curtin Business School, Curtin University, Australia. Richard has 22 years' experience as a logistics and SCM academic in UK and Australian universities. Before academic life, Richard worked in freight forwarding. His research is focused on human and community sustainability in the context of supply chains. He is the Sustainable Development Goal Advisor, Responsible Management, Emerald Publishers UK, and editorial board member of the Asian Journal of Shipping and Logistics.

CTAC

CONTAINER TERMINAL AUTOMATION CONFERENCE EUROPE

POWERED BY PORT TECHNOLOGY INTERNATIONAL

EUROPE'S TERMINAL TECHNOLOGY HUB

17 - 18 MAY 2024

VALENCIA, SPAIN

Ports & Terminals can attend for FREE!

TICKETS NOW AVAILABLE!

The Container Terminal Automation Conference is a flagship Port Technology International event. Register your interest for the 8th instalment and look forward to a range of networking opportunities and expert-led discussions on Automation, Digitalisation, Sustainability, Intermodality and more.

REGISTER FOR JUST €1,498 **CTAC.PTIEVENTS.COM**

Official AI Partner
INFORM

Gold Sponsors
RBS
WESTWELL

Silver Sponsors
AVLINO
BOXBOT
CONROO
ROCSYS
TMEIC

Bronze Sponsors
allread
atai
CAMCO TECHNOLOGIES
DSP
FERNRIDE
KALMAR
igo Solutions
navis
moffatt & nichol

Welcome Drinks Sponsor
TMEIC

Evening Dinner Sponsor
prodevelop

Lunch Sponsor
Three Group Solutions

Breakfast Sponsor
PORTCHAIN

Networking Break Sponsor
GullsEye KEY TO PRODUCTIVITY

Exhibitors
AUCOS-Systems
TCK.W rope monitor

ctac.ptievents.com | #CTACEU2024

FIVE TOP TIPS FOR SOURCING PORT CYBERATTACK INSURANCE COVER

Ed McNamara, CEO, Armada Risk Partners

Port cyberattacks are now one of the biggest and most sophisticated threats facing port operators.

In late 2023, multiple ports in Australia came under attack with operations at DP World Australia container terminals in Melbourne, Sydney, Brisbane and Perth taken offline and disrupted across four days. The port operator manages around 40 per cent of the goods entering and leaving Australia. This attack had echoes of an earlier breach in 2023 when a cyberattack simultaneously hit three Canadian ports.

Other prominent breaches have included a ransomware attack on Nagoya port in Japan in July 2023, a major incident that deleted swathes of data and forced the suspension of operations at the container terminal.

The Port of Lisbon has also suffered an attack with confidential information compromised and, in some instances, published online. Port operations were not compromised but the impact, not to mention embarrassment, of a breach leading to confidential partner information being disclosed is all too obvious.

With criminal gangs and nation states now pumping resources into cyber warfare how can ports get the best possible cyberattack insurance in place and how does insurance fit into an overall defence strategy?

1. UNDERTAKE A THOROUGH CYBER REVIEW BEFORE SOURCING INSURANCE

As ports are now painfully aware the nature of their setup makes them vulnerable to attack. Hosting large numbers of vessels operated by a wide variety of companies employing a range of different IT systems provides a perfect environment for network intrusions, hacks and ever more sophisticated ransomware attacks.

When looking at cyber insurance, evaluating your organisation's overall cybersecurity capabilities across all areas and the risk exposure is a good starting point for port and terminal operators.

It is important to undertake this review as part of a strategic approach to sourcing port cyber insurance. It is now more vital than ever to get your systems and processes as secure and up-to-date as possible before engaging with insurance companies.

At Armada, we advise ports to present the strongest picture to would-be insurers to secure the best coverage and reduce premiums.

Insurers are looking for hard evidence of robust risk management policies and protocols, including well-prepared cybersecurity policies, along with regular assessments and continuous employee training.

This should include identifying potential threats, assessing the value and sensitivity of the data that you handle, and evaluating your current security measures.

2. COMMIT TO CONTINUOUS CYBERSECURITY IMPROVEMENT

Cyber insurance is a vital consideration in any cyber risk mitigation strategy. Insurance can play a key role in helping pay for recovery costs if you suffer a ransomware attack, data breach and any business interruption. It can also cover third-party liabilities.

Moreover, there are policies that provide incident response support, giving access to expert teams to provide guidance and support in the event of an attack, again helping mitigate the damage caused.

"WHEN LOOKING AT CYBER INSURANCE, EVALUATING YOUR ORGANISATION'S OVERALL CYBERSECURITY CAPABILITIES ACROSS ALL AREAS AND THE RISK EXPOSURE IS A GOOD STARTING POINT FOR PORT AND TERMINAL OPERATORS."

"IT IS GOOD PRACTISE TO WORK WITH A BROKER WHO IS WELL-VERSED IN UNDERSTANDING THE NUANCES OF CYBERSECURITY AND IS KEEPING ABREAST OF THE CHANGING PORT INSURANCE LANDSCAPE."

However, it is important to stress that cyber insurance coverage doesn't release any organisation from the responsibility of managing its cyber risks. It requires ports and terminal operators to sustain a cybersecurity programme with continuous improvement at its heart.

Those running ports must have awareness of the level of threat posed by cyberattacks. The threat from hackers is so great, that the United States FBI now has a separate top 10 most-wanted list purely for cybercriminals. At the top of this list is a Russian hacker and a $10 million reward is available for information leading to his arrest.

Typically, the threat does not come from individuals, lone wolf style attacks, those instigating cyberattacks work as collectives, operating like businesses. These are sophisticated organisations.

Being at the forefront of global trade, ports are an obvious target. The cybercriminals see a target that is of prime logistical importance, where the fear of continued disruption will make prompt ransom payment more likely.

It is against this backdrop that those running ports operate.

3. BE AWARE CYBER INSURANCE MARKET IS CHANGING

The insurance marketplace is responding sharply to the increased threat of cyberattacks on ports.

The result is a fluid and constantly changing market. Cyber premiums may be rising, driven by the increasing activity and claims, while coverage is, in many cases, diminishing.

We advise searching for policies that cover a wide range of cyber risks. Consider the policy limits and deductibles that best suit your port's risk profile. Ensure that the policy's limits adequately cover potential financial losses, including costs associated with breach response, recovery, and legal expenses.

Insurers will also look more favourably at ports that follow guidelines relating to cybersecurity. Currently, guidelines including those from the International Maritime Organization (IMO) are voluntary but they provide a framework that could well become part of the legislature in the future.

Ship owners mitigating their own risks could also be disinclined to use ports that are failing to adhere to voluntary guidelines. It is worth noting that in 2024 the European Union will rubber-stamp new cybersecurity regulations obligating critical infrastructure companies to become more secure.

4. STAY ALERT TO NEW THREATS

Be aware cyber risks are evolving rapidly and it is vital that port operators keep up to speed. That means being thoroughly informed and acting when it comes to emerging threats, regulatory changes and industry best practices.

Even after your insurance is in place you should regularly review that insurance coverage to ensure it is still adequate. Be aware your current policy may not be addressing the latest threats.

Staying alert applies on many levels.

On a day-to-day basis, this means being wary of links in emails and unsolicited communication.

Senior employees at a port have a degree of public visibility, their job titles and contact details may be easily found. They become a target for cybercriminals and could fall victim to a ransomware attack that ultimately infects all IT systems.

However, staying alert also means having sophisticated systems in place to fight against cyberattacks, a call for all employees to remain vigilant alone will not be sufficient. Attacks are too sophisticated and too frequent, for instance, the Port of Los Angeles has revealed it has suffered attacks twice as frequently in 2023 compared to previous years.

An option is to build a cybersecurity defence system, but an alternative is to outsource to experts and specialists in defending against cyberattack in the maritime industry.

With these standards applied, the port might wish to ensure those operating IT systems encountering their own have similarly robust defences.

The links between systems and need to share information mean that often any defence is

only as strong as its weakest link. Ports therefore must consider what minimum standards of cybersecurity apply to those they deal with in any capacity.

5. WORK WITH A PORT SPECIALIST

It is good practise to work with a broker who is well-versed in understanding the nuances of cybersecurity and is keeping abreast of the changing port insurance landscape.

It is wise for CEOs themselves to examine the fine print of any insurance renewal and work with the broker who should go the extra mile and source a wide variety of quotes.

Do not automatically renew with your existing provider, check the coverage itself as this could have changed significantly. Do not base the renewal on cost alone, as this could result in you being dangerously exposed and underinsured.

Your broker needs to fully understand your business and research the policies that are best suited to your port's setup, risk profile and type of operations. They can also provide advice on specific compliance standards that your port may have to follow.

A port specialist will also help ensure there is a clear plan should any attack prove successful.

If a ransom is demanded, which authorities should be contacted and in what manner? What response should there be to any ransom demand? Panic can lead to an escalation of the impact, for instance, the paying of any ransom could be illegal with those monies heading to a criminal, or even terrorist organisation.

A specialist can help source insurance where there is an immediate response to any query.

There are policies available that provide access to digital experts who can help get the port back and operational as soon as possible in the event of a digital attack.

Expert providers can also help a port with contingency planning and work through potential risks, cross-referencing these against both the existing policy and potential alternatives.

Port operators will benefit from working with a skilled broker to help find a cover that caters to all eventualities and emerging threats.

In conclusion, cybersecurity is a rapidly changing landscape and ports are uniquely vulnerable. Insurers are therefore very cautious and ports need to put themselves in a position of strength. Working with specialists, having a clearly tested cyber strategy and showing a commitment to continuous improvement are all key elements to securing the best insurance protection for your people, assets and reputation.

ABOUT THE AUTHOR:
Ed McNamara has worked in the insurance industry for more than 15 years. A Cleveland native Ed is the son of a Cleveland Police Captain. Ed's charitable work includes working as a founding board member of the Prayers from Maria Foundation, and a board member at the Lorain County Board of Health and Irish American Charitable Foundation

ABOUT THE COMPANY:
Armada Risk Partners is a Cleveland-based commercial insurance broker that shields companies and their employees from catastrophes by providing insurance solutions. The company is a global ports insurance specialist and further offers property and casualty, health and benefits, private risk, and life insurance expertise.

"BE AWARE CYBER RISKS ARE EVOLVING RAPIDLY AND IT IS VITAL THAT PORT OPERATORS KEEP UP TO SPEED."

PREPARATION, COMPLIANCE AND AWARENESS: THE THREE PILLARS OF MARITIME CYBERSECURITY

"THE SPEED AND TRAJECTORY OF DIGITALISATION MAKE THE NEED FOR EFFECTIVE CYBERSECURITY IN THE MARITIME INDUSTRY EVER MORE URGENT."

MARLINK

Nicolas Furgé, President, Digital, Marlink

Organisations are increasingly aware of the threats from hackers but need to work proactively to build defences.

The era of maritime digitalisation onboard ships and ashore is accompanied by the growing threat from cyberattacks and the resulting risk of economic and reputational damage to companies across the supply chain. The speed and trajectory of digitalisation make the need for effective cybersecurity in the maritime industry ever more urgent.

An effective cybersecurity strategy is critical to protect IT and OT systems, networks and data within the organisation. The infrastructure at risk encompasses vessels, office sites and data centres all of which host sensitive data. Protecting these assets calls for a combination of cyber awareness, security procedures and regulatory compliance – rules are emerging on national and local levels designed both to protect organisations and hold them accountable in the case of lapses.

Much of the success in combating cybersecurity can be delivered by ensuring that best practices for cybersecurity are followed within an organisation drawing on a cybersecurity framework that is aligned to corporate business objectives.

A central element of effective cybersecurity is risk management. Organisations must take into consideration everything inside a corporate network from how it is functioning, its hardware and software components, assets, people and processes, to determine where

risk exists and threats may emerge that could hurt corporate operations.

Marlink's experience working in the maritime industry over many years is that risk management is not always performed to the level required as this approach is still considered new for maritime, whereas in other business sectors, it is seen as a standard tool to improve cybersecurity.

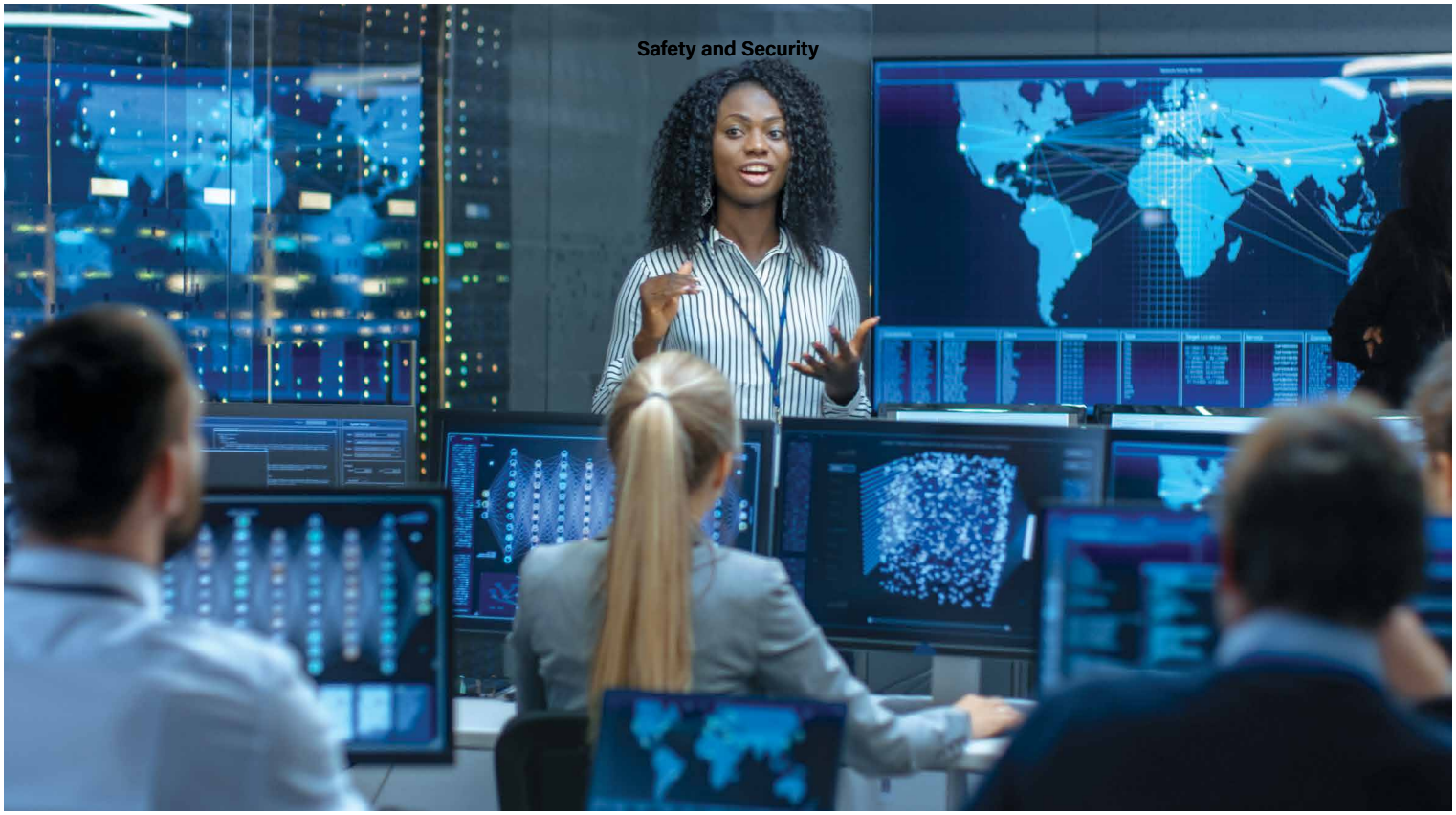
One of the realities that maritime organisations and their stakeholders must face is that the high prevalence of cybercrime means an attack at some point is a certainty. However, there are three key elements that organisations can put in place that enable them to prepare, respond and prevent cyberattacks.

PLANS FOR DEFENCE AND RESPONSE

The first element is to ensure the organisation is prepared to respond to an incident. This is as simple as accepting that, if hacking is a fact of life, the organisation needs a plan for how to respond in the case of an incident. If the attack is successful, how does the organisation minimise the impact and how does the business maintain operations until it is resolved?

Increasingly important is compliance with the burgeoning regulatory regime, which is becoming more and more important across the maritime industry. Current instruments include the IMO 2021 regulation, which has been in force for a couple of years and requires organisations to demonstrate that they have taken steps to harden their assets and have plans in place to respond to an attack.

The next piece of regulation on the radar for maritime is the upcoming NIS2 Directive, an EU-wide legislation which is set to come into force from October 2024. Designed to enhance cybersecurity measures in the European Union, it will have implications for maritime companies larger than



"THE COSTS OF CYBERSECURITY ARE CONSIDERABLE BUT THE BENEFITS OF INVESTING IN THE PEOPLE AND SYSTEMS THAT CAN MANAGE THE ASSOCIATED RISKS ARE FAR GREATER."

50 employees or those generating an annual revenue exceeding €10 million ($10.8 million), broadening its scope to include both medium and large-size companies within the sector.

The critical element of NIS2 is that it has consequences for non-compliance; it is no longer acceptable to suffer a cyberattack and not act. Preparation and response are essential. Companies are not only required to ensure they are cybersecure for the health of the business but they can also be hit with a fine for non-compliance.

With a growing number of threats comes larger consequences and bigger business impacts, making regulation and compliance something that should keep cybersecurity at the forefront of the maritime industry mindset.

The final element is the need to build cyber awareness inside the company, something which is often the weakest link in cybersecurity. It is the responsibility of the whole ecosystem of people onboard and ashore from the most senior people to the most junior, to be aware of the threats to IT and OT assets and how to manage that risk. Because organisations are traditionally constructed with hierarchies and segregation between departments and sections of the workforce, they can lack the ability to bring cybersecurity together in a consolidated strategy.

Improved security awareness means making sure people are informed and aware of how to recognise threats and how to handle IT and OT systems regardless of their role. This means ensuring that all employees are aware of where a company is vulnerable and implementing a policy that ensures these processes are correctly followed so that they remain effective.

THE COST OF DOING NOTHING

The challenges posed by cyberattacks are escalating, both in increased frequency and sophistication and attacks are not performed exclusively by state actors but also by independent groups and individuals who successfully exploit poor cyber hygiene.

In any safety-related industry, experts will contrast the cost of prevention compared to the cost of an accident and this remains true in cybersecurity. The cost outlays for a programme of awareness, compliance and response pale into insignificance compared to the costs - both operational and reputational - that can flow from a successful cyberattack.

The costs of cybersecurity are considerable but the benefits of investing in the people and systems that can manage the associated risks are far greater.

"THE INEVITABILITY OF CYBER INCIDENTS MAKES THE IMPORTANCE OF PLANNING AND RAPID RESPONSE STRATEGIES CRITICAL IN MINIMISING DAMAGE AND KEEPING THE BUSINESS RUNNING."

Cybersecurity budgets across the maritime industry have been rising and are expected to keep climbing in the future.

More organisations in the maritime industry have realised that there is a cost-saving benefit to applying high-quality cybersecurity principles because when they start using the right tools and services, they will save the company money.

The inevitability of cyber incidents makes the importance of planning and rapid response strategies critical in minimising damage and keeping the business running. Surveys and research have previously concluded that many of the companies that have been hacked choose not to make it public but not all have that luxury.

Examples of collateral damage in cyberattacks such as on subsidiaries, suppliers, clients or supply chain partners, mean that being able to keep a hack private is a luxury most companies do not have. Implementing sound cybersecurity principles and placing the right importance on prioritising spending on cybersecurity measures can at least help to manage the reputational impact of an attack, especially where multiple stakeholders are affected.

NEW THREAT VECTORS EMERGING

The increased focus on cybersecurity threats is a welcome development and it comes at a time when the number of 'threat vectors' is increasing with the availability of new Low Earth Orbit (LEO) network solutions.

The increased availability of new network providers and communications options means the cybersecurity landscape is changing and it will change further as new constellations such as Kuiper are added to the new players, Starlink and Eutelsat OneWeb. These services provide very high throughput and low latency connectivity and are especially attractive for crew and passenger applications. They also bring new security challenges.

From a cybersecurity perspective, more connectivity onboard can also introduce some new challenges; with more users applications and devices connected to the internet, there are more potential vectors for cyber criminals to exploit.

The increase in internet access and traffic from LEO satellite services comes at a time when warnings are increasing of the potential for politically and economically driven hackers to target the maritime sector. Always-on internet connectivity of the type enabled by LEO transforms a ship from an asset with regular but limited internet access to a world of interactive, constantly updated internet and social content.

Owners also need to understand that in the case of LEO satellites, the cybersecurity tools employed across a blended network require protection to be in place both via traditional satcom gateways and onboard ships.

Because cyber threats such as hacking, malware, and data breaches are increasing year by year, Marlink is constantly refining cybersecurity protection for our clients. Marlink provides advanced tools to manage and monitor network assets, secure individual devices and search for threats to prevent exploitation of the ship's network and devices.

As businesses adopt new and emerging technologies to support their digitalisation strategies, the need for cybersecurity increases - as does the demand for experts who can prepare prevention and response strategies. There has been a realisation within the maritime industry around the severity of the threat cybersecurity poses to business continuity and reputation.

What is needed next is a more concerted move towards the three-part approach that combines awareness with response planning and regulatory compliance to demonstrate a co-ordinated strategy that extends from ship to shore.

ABOUT THE AUTHOR:
Nicolas has 30 years of experience in technology-powered businesses, holding successive functions in project management, business unit management and general management in Orange, Alstom and Keolis Groups. He scaled up cybersecurity at Orange Business Services to a €150 million ($163 million) business. He has been serving as President Digital of Marlink Group since 2021.

ABOUT THE COMPANY:
Marlink, a global leader with $800+ million annual revenues and 1,500 employees across 30+ countries, offers end-to-end managed solutions for challenging environments like shipping, offshore, and yachting. We design hybrid network solutions integrating satellite, terrestrial, and digital services, empowering customers to innovate and operate efficiently with advanced technologies and 24/7 support.

For further information please visit **www.marlink.com**.