

The Journal

OF PORTS AND TERMINALS

Edition 162
2026

In partnership with

The background image is a wide-angle shot of a busy port terminal. In the foreground, a worker wearing a white hard hat and a high-visibility yellow safety vest stands with their back to the camera, looking out over the terminal. The terminal is filled with stacks of colorful shipping containers (blue, red, green, yellow). Several large gantry cranes are visible in the background, with one crane positioned over a large cargo ship. Overlaid on the image are various digital and futuristic elements: a large, semi-transparent blue rectangular interface on the left side containing icons for a container, a checklist with three green checkmarks, a red warning icon, a red container, and a document with a green checkmark; glowing blue lines and dots connecting different parts of the terminal; a red circular warning icon with an exclamation mark over a red container; a green circular checkmark icon over a green container; a blue circular padlock icon over a crane; and a blue circular camera icon over the right side of the terminal. The overall atmosphere is one of modern, high-tech port management.

Ports Under Pressure



**Port Technology
International**

PTI MEDIA KIT 2026

Connect. Influence. Lead.
Reach the port and terminal
decision-makers driving
the future.

REACH A
HIGHLY TARGETED
AUDIENCE OF
INDUSTRY
DECISION-MAKERS



50,000+
senior industry
professionals



10,000+
newsletter
subscribers



100,000+
monthly
page views

Maximise your visibility. Drive results.

The PTI Media Kit 2026 connects your brand with the professionals
shaping the future of ports and terminals worldwide.

OPPORTUNITIES AVAILABLE NOW

NEW!



**Tailored
Marketing
Packages**

Custom-built campaigns
designed around your
objectives.



**PTI Partner
Hub Premium
Subscription**

Year-round visibility with
enhanced profiling, content
promotion and lead
generation.



**Targeted
Email
Campaigns**

Reach the right audience
with highly engaged,
data-driven campaigns.



**Webinars
(60-90 mins)**

Thought leadership
with impact. Full campaign
support and GDPR-
compliant lead delivery.



Download the PTI Media Kit
to explore the opportunities and
start building your next campaign.




 Port Technology
International

Margherita Bruno,
Managing Editor

Foreword

A port is built for movement, but every movement carries a responsibility. Every container lifted, every truck routed, every vessel berthed, and every worker entering a terminal depends on a chain of decisions that must hold under pressure. A pressure that is no longer confined to the quay, but it now runs through digital systems, cargo declarations, security protocols, climate exposure, workforce capability, infrastructure planning and the wider confidence that supply chains place in ports as essential gateways for trade.

This edition of PTI's Journal, *Ports Under Pressure*, looks at what that responsibility means for ports and terminals today. The sector is being asked to do more than move cargo efficiently. It must protect people, support economic security, manage physical and cyber risk, handle new and more complex cargo types, respond to disruption, and keep operations moving while expectations from regulators, customers and communities continue to rise.

That makes safety, security and resilience difficult to treat as separate disciplines. A cyber incident can become an operational crisis. A physical security weakness can affect cargo integrity. A misdeclared shipment can create safety, environmental and commercial

consequences. A breakdown in workforce competence can undermine even the most advanced system. The modern port is a connected operating environment, and the way risk is managed must reflect that reality.

The edition opens with our partners at Stowlog, where **Pablo Aguirre** discusses the shift from compliance to care. It is a fitting starting point because so many safety discussions begin with the existence of rules, procedures and records. These remain essential, but they are not enough on their own. The real test is whether safety processes work in practice, during busy shifts, with contractors on site, permits active, equipment moving and decisions being made in real time. Stowlog's article examines how paper-based processes, spreadsheets and disconnected systems can leave gaps between policy and operational reality, and how digital workflows can improve visibility, traceability and control.

From there, **Chloe Rowland** of IAPH widens the lens. Her contribution on "resilience by design" captures one of the central arguments of the edition: ports can no longer afford to build safety, security and emergency response in silos. Cyber threats, climate disruption, physical security, emergency preparedness,

data collaboration and international cooperation are now part of the same resilience conversation. The emphasis is not simply on recovering after disruption, but on designing organisations, systems and partnerships that can anticipate, absorb and respond more effectively when pressure comes.

Lamia Kerdjoudj of FEPORT brings a European terminal operator perspective to that same question. Her article argues that competitiveness and resilience are not opposing priorities, but mutually reinforcing ones. Terminals need the ability to invest, adapt and remain attractive in a global market while also responding to geopolitical uncertainty, regulation, technological change, decarbonisation and security demands. Resilience depends not only on ambition, but on investment certainty, practical policy frameworks and the capacity to keep improving under strain.

The changing role of the Harbour Master, explored by **Captain Kevin G Allen** of IHMA, shows how these pressures are reshaping long-established responsibilities. Marine safety and traffic management remain central, but the role now extends into digitalisation, crisis response, environmental responsibility, cyber and physical risk, and collaboration



across a wider network of specialists. The Harbour Master is no longer working only with wind, tide and traffic. The role sits within a far more complex risk environment, where decisions can carry consequences across port operations, communities and supply chains.

People remain central throughout this edition. **Debbie Cavalloro** of Port Skills and Safety makes the point clearly: technology can support safer operations, but it cannot replace capable people, effective systems or a healthy company culture. Safety improvement depends on leadership, training, skills pathways, psychological safety and the willingness to learn not only from what goes wrong, but also from what goes right. Ports generate large volumes of safety data, but that data only has value when it helps organisations understand how work is actually done and how people can be better supported.

Richard Steele of ICHCA brings the discussion back to the most serious consequences of operational failure. Drawing on 25 years of cargo handling fatality data, his contribution highlights that the gravest risks are often embedded in ordinary work: cargo handling, vehicle-pedestrian interaction, enclosed spaces, work at height, quays, holds and the

ship-shore interface. These are familiar hazards, not obscure ones. The challenge is sustaining the leadership, discipline and effective controls needed to manage known risks day after day, especially where people, machinery, cargo and time pressure meet.

Collaboration is another recurring theme. The contribution from **Beatrice Björk, Neil Dalus and Pat O'Leary**, bringing expertise from sfPORTEQ, TT Club and PEMA, shows why safety learning must move across organisational boundaries. Every port has its own layout, equipment mix and operating culture, but many incidents follow recognisable patterns. Manufacturers, operators, insurers and technology providers each see different parts of the risk picture. When that knowledge is shared, the industry can learn faster than infrastructure changes and avoid repeating preventable mistakes.

Cargo risk is also changing. **Bertrand Chen** of GSBN examines hazardous cargo and lithium batteries, focusing on the risks created by misdeclaration, fragmented information and static documentation. As cargo types become more complex, ports and supply chain partners need information that can be trusted and acted on. Source-verified certification data offers

one way to improve declaration checks, traceability and operational decision-making, moving beyond documents that are simply filed towards data that supports real risk management.

Finally, **Shaleen White** of S2 Global considers inspection as a discipline of control, transparency and revenue assurance. Inspection is not only about scanning cargo. It is about creating an auditable process in which the manifest, scan, decision and release can be connected and reviewed. When inspection is integrated into port operations properly, it supports customs enforcement, protects revenue, strengthens transparency and helps compliant cargo keep moving without sacrificing control.

What we find from these contributions is an industry that is not short of knowledge, and yet still faces the harder task of turning knowledge into consistent practice. Safer and more resilient ports will not be built through compliance alone; they will be built through better data, stronger systems, skilled people, shared learning and the courage to close the gap between what policy says and what operations demand. That is the work ahead, and that is the conversation this edition sets out to advance.

Contents



Digital Safety and Operational Visibility

6.

From Compliance to Care: Why Digital Safety Workflows are Critical for Modern Ports

Pablo Aguirre, CEO and Co-Founder, Stowlog

9.

In Conversation with Stowlog: Safer Ports, Smarter Workflows

Margherita Bruno, Managing Editor, Port Technology International, in conversation with Pablo Aguirre, CEO and Co-Founder, Stowlog



The New Risk Landscape

13.

Resilience by Design: How Ports Are Reinventing Safety and Security for a Volatile Era

Chloe Rowland, Senior Manager: Data Collaboration, Risk & Resilience, International Association of Ports and Harbors

19.

Competitiveness and Resilience: Two Sides of the Same Lucky Coin for Europe's Terminal Operators

Lamia Kerdjoudj, Secretary General, FEPORT

23.

Connecting Horizons: Building Future-Resilient Ports Together

Captain Kevin G Allen, President, International Harbour Masters Association



info@porttechnology.org

www.porttechnology.org

www.linkedin.com/porttechnology



People, Skills and Safety Culture

29.

A Safer Tomorrow: Turning Insight into Action Across Port Safety, Skills and Culture

Debbie Cavaldoro, CEO, Port Skills and Safety Ltd

33.

Fatal Risk at the Port-Ship Interface: Learning from 25 Years of Cargo Handling Fatalities

Richard Steele, CEO, ICHCA

39.

Connecting Minds: How Collaboration is Strengthening Safety Across the Port Industry

Beatrice Björk, CEO, sfPORTEQ and Neil Dalus, Risk Assessment Manager, TT Club. Supported by Pat O'Leary, Head of Technology, Port Equipment Manufacturers Association



Cargo Integrity and Control

44.

Verified Data for Hazardous Cargo Risk Management: Supporting Safer Declaration Checks and Operational Decisions

Bertrand Chen, CEO, Global Shipping Business Network

48.

Port Resilience Through Integrated Inspection: What One Container Reveals About Transparency, Control and Revenue Assurance

Shaleen White, Vice President for Latin America Business Development, S2 Global



Container Terminal Automation Conference Asia

The region's leading event for **terminal automation** and **digital transformation.**

Join port authorities, terminal operators, technology providers, and industry leaders shaping the future of container terminal operations in Asia.



8-9 September 2026



Bangkok,
Thailand



Senior port and
terminal professionals



Real-world insights
from leading ports
and terminals



Practical solutions
to drive efficiency
and performance



Connect with
decision-makers
and innovators



Stay ahead
in a rapidly
evolving industry

SAVE \$300



Standard Ticket

Register now and
save **\$300**

FREE



Ports & Terminals

Complimentary
Registration

For port and terminal
authorities and operators





Digital Safety and Operational Visibility



LOCATION: Florida International Terminal (Port Everglades)

PEOPLE FROM LEFT TO RIGHT:

Pablo Aguirre, CEO (Stowlog), Eddie Cabrera, HSSE team (FIT), David Delburn, HSSE Manager (FIT), Alazne Oiarbide, Product Owner (Stowlog), Jose Gutierrez, CTO (Stowlog), Fede Gómez, Mobile Lead (Stowlog), Adrián Coll, Tech Lead (Stowlog), Jorge Juan, CDO (Stowlog)

From Compliance to Care: Why Digital Safety Workflows are Critical for Modern Ports



Pablo Aguirre,
CEO and Co-Founder, Stowlog

For decades, safety and security management in ports has been driven primarily by compliance. Regulations, audits, permits, inductions, access controls and documented procedures have formed the backbone of how terminals manage risk and demonstrate adherence to industry standards.

While compliance remains essential, the operating environment of modern

ports has changed significantly. Terminals are becoming increasingly complex ecosystems where employees, contractors, truck drivers, visitors, vessels and automated equipment interact continuously. At the same time, ports face growing pressure to improve operational efficiency, strengthen resilience, meet regulatory requirements and maintain safe working environments.

In this context, compliance alone is no longer sufficient.

The challenge facing many ports today is not the absence of procedures. In fact, most facilities already have extensive safety and security frameworks in place. The real challenge lies in execution. Many critical workflows continue to rely on paper forms, spreadsheets, emails, manual registration processes and disconnected

“Predictive safety does not begin with artificial intelligence. It begins with reliable operational data.”

systems, creating gaps between policy and operational reality.

As a result, ports often struggle with limited visibility of people, activities and risks across their facilities. This lack of real-time awareness makes proactive risk management difficult and can force many organisations into a reactive approach to safety.

The Cost of Reactive Safety Management

Port operations remain among the most complex and high-risk industrial environments in the world.

Workers routinely operate around heavy machinery, moving vehicles, cranes, vessels, hazardous cargo and restricted areas. Every day, thousands of individuals may enter and leave a terminal, each requiring different levels of access, training and supervision.

When safety processes are fragmented, organisations face several challenges:

- Delays in validating contractor competence and authorisations.
- Limited visibility of personnel locations.
- Difficulty coordinating permit-to-work activities.
- Manual collection of safety and compliance records.
- Slow incident response.
- Reduced ability to identify emerging risks.

These challenges create more than administrative inefficiencies. They can directly impact workforce safety, operational continuity and organisational resilience.

Historically, incident investigations have focused on understanding what happened after an event occurred. However, the industry is increasingly recognising the value of identifying risk indicators before incidents happen.

The transition from reactive to proactive safety management depends on visibility.

The Visibility Gap

Many ports have invested heavily in physical infrastructure, operational technology and security systems. Yet critical safety information often remains scattered across multiple platforms.

A typical contractor entering a terminal may need to complete:

- A safety induction.
- Access authorisation checks.
- Permit-to-work procedures.
- Site-specific risk assessments.
- Training validation.
- Security clearance requirements.

In many facilities, these processes are managed independently.

This fragmentation creates a visibility gap, with HSSE teams spending considerable time collecting information instead of managing risk.

The issue is not necessarily a lack of data. Ports generate enormous amounts of operational information every day. The problem is that this information is often disconnected, making it difficult to establish a complete operational picture.

Without visibility, proactive intervention becomes challenging.

Without proactive intervention, organisations remain dependent on reactive responses.

Digital Safety Workflows: Connecting Operations

The next stage in safety management involves connecting previously isolated processes into integrated digital workflows.

Digital safety workflows bring together safety, security and compliance activities into a single operational environment. Rather than treating inductions, permits, visitor management, incident reporting and contractor control as separate administrative tasks, they become part of a connected ecosystem.

This approach creates several advantages.

Improved Situational Awareness

Real-time visibility enables operational teams to understand:

- Who is on site.
- Where individuals are located.
- What activities are taking place.
- Which permits are active.
- Whether authorisations remain valid.
- Where risks may be developing.

This information supports faster and more informed decision-making.

Stronger Risk Management

Connected workflows improve the consistency and traceability of safety processes.

By digitising operational activities, ports can reduce reliance on manual records and improve their ability to identify deviations from established procedures.

The result is improved compliance and stronger operational control.

Enhanced Incident Response

When incidents occur, response time is critical.

Access to real-time operational information can significantly improve coordination between safety, security and operational teams.

Knowing who is affected, where they are located and what activities were taking place provides valuable context during emergency situations.

Better Data for Continuous Improvement

Digital workflows generate structured operational data.

Over time, this data becomes an important asset for identifying trends, recurring hazards and opportunities for improvement.

Near-miss events, permit violations, unauthorised access attempts and recurring risk patterns can all contribute to a more informed safety strategy.

From Digitalisation to Predictive Safety

Perhaps the most significant opportunity created by digital workflows is the foundation they provide for predictive safety.

Predictive safety does not begin with artificial intelligence. It begins with reliable operational data.

Historically, many safety records have existed in formats that are difficult to analyse at scale. Digital workflows transform previously fragmented activities into structured datasets that can support deeper analysis.

As ports continue to digitalise critical processes, opportunities emerge to:

- Identify recurring risk patterns.
- Detect abnormal operational behaviour.
- Analyse near-miss events.
- Prioritise preventive interventions.
- Support data-driven decision-making.

The goal is not to replace human judgement.



LOCATION: APM TERMINALS PIER 400 (Port of Los Angeles), DESCRIPTION: the Stowlog team with the APM Terminals Pier 400 team studying how to digitalise the vendor gate of the terminal in the safest way.

Instead, technology should empower HSSE professionals with better information and earlier visibility of potential risks.

The most effective safety teams of the future will likely combine operational expertise with digital intelligence.

Building a Culture of Care

Technology alone does not create safer ports.

Successful digital transformation depends on people, processes and culture.

One of the most important shifts occurring across the industry is the movement from a compliance mindset towards a culture of care.

Compliance asks:

"Have we followed the procedure?"

Care asks:

"Have we reduced the risk?"

While both questions remain important, the second reflects a more proactive approach to safety management.

Digital workflows support this transition by helping organisations focus less on administrative activities and more on prevention, visibility and continuous improvement.

Ultimately, safety is not about software, forms or regulations.

It is about people.

Every permit issued, every induction completed, every risk assessment conducted and every access control verified serves a common objective: protecting the individuals who keep global supply chains moving.

Conclusion

The future of port safety will not be defined solely by new regulations or emerging technologies. It will be defined by the industry's ability to connect information, improve visibility and act proactively before incidents occur.

As ports continue their digital transformation journey, digital safety workflows are emerging as a critical layer of operational infrastructure.

By connecting safety, security and compliance processes, organisations can move beyond reactive incident management and towards a model built on awareness, prevention and resilience.

The transition from compliance to care is ultimately about creating safer ports, stronger operations and more resilient supply chains.

Most importantly, it is about ensuring that everyone who enters a port goes home safely.

About the author

Pablo Aguirre is CEO and co-founder of Stowlog, a modular SaaS platform digitalising safety, security, and compliance processes in port and logistics facilities worldwide. A certified Port Facility Security Officer (PFSO), he leads Stowlog's international expansion and works closely with HSSE teams to modernise operations through real-time visibility and digitalisation.

About the company

Stowlog is a modular SaaS platform that digitalises safety, security, and compliance processes in port and logistics facilities. By replacing fragmented manual workflows with a centralised, real-time system, it improves visibility, traceability, and operational control, supporting safer and more efficient port ecosystems worldwide.

[Find out more](#)



In Conversation With Stowlog: Safer Ports, Smarter Workflows



Margherita Bruno, Managing Editor,
Port Technology International, in
conversation with **Pablo Aguirre**,
CEO and Co-Founder, Stowlog

In this Q&A, we catch up with Stowlog on the everyday realities of port safety, from visibility across busy terminals to the role of digital workflows in helping teams act earlier and with greater confidence.

Ports and terminals are busy environments, with staff, truck drivers, contractors and visitors moving through the same space. What are the main safety and security challenges you see in these operations today?

One of the biggest challenges is maintaining visibility across increasingly complex operational environments. Modern ports involve thousands of daily interactions between employees, contractors, truck drivers, visitors, vessels

and equipment. While safety and security procedures exist, information is often fragmented across different systems, departments and manual processes.

This can create blind spots around who is on site, where they are located, what activities they are authorised to perform and whether the appropriate controls are in place. As ports continue to grow and become more connected, maintaining real-time situational awareness is becoming one of the most important challenges for both safety and security teams.

Many companies have safety rules and procedures in place, but problems can still happen in daily operations. Where do you think the gap usually appears between policy and practice?

The gap typically appears during execution.

Most ports have robust procedures, policies and compliance frameworks. The challenge is ensuring that those procedures are consistently applied in real operational conditions. Manual processes, disconnected systems and limited visibility can make it difficult to verify that training has been completed, permits are valid, risks have been assessed, or access permissions remain appropriate.

In many cases, incidents do not occur because procedures are missing. They occur because organisations lack the visibility needed to ensure those procedures are being followed effectively in real time.

How does Stowlog help port and logistics facilities manage safety,

security and compliance in a more connected way?

Stowlog provides a digital platform that connects safety, security and compliance workflows into a single operational environment.

Processes such as safety inductions, contractor management, visitor control, permit-to-work procedures, risk assessments, incident reporting and personnel geolocation are integrated into one system. This allows organisations to move away from fragmented manual processes and towards real-time operational visibility.

By centralising information and connecting workflows, Stowlog helps HSSE and security teams make faster, more informed decisions while improving traceability, accountability and operational control.

Why is it important for terminals to know who is on site, what they are authorised to do and whether their training or access permissions are up to date?

Effective risk management starts with knowing who is operating within your facility.

Ports are high-risk environments where individuals may require different levels of training, authorisation and supervision depending on the tasks they perform and the areas they access. Without accurate and up-to-date information, organisations increase their exposure to both safety and security risks.

Having real-time visibility of personnel, qualifications and permissions helps ensure that the right people are carrying out the right activities in the right locations, reducing risk while supporting operational efficiency.

Safety and security controls can sometimes be seen as slowing operations down. How can digital tools help terminals improve control without creating delays at the gate or inside the facility?

The perception that safety and security slow operations often comes from manual processes rather than the controls themselves.

Digital tools can automate validations, streamline approvals and provide immediate access to critical information. Instead of relying on paperwork, phone calls or multiple systems, terminals can verify training records, authorisations and access permissions instantly.

When implemented correctly, digitalisation removes administrative friction while strengthening operational control. The result is a safer and more efficient process for both the terminal and its users.

What role can real-time information play when a terminal needs to respond quickly to an incident, unsafe behaviour or an unauthorised access issue?

Real-time information is critical during any operational event.

Whether responding to an incident, investigating unsafe behaviour or managing an unauthorised access situation, decision-makers need immediate visibility of who is involved, where they are located and what activities were taking place.

The faster organisations can access reliable information, the faster they can coordinate resources, assess risks and take appropriate action. Real-time visibility improves response times, enhances coordination and ultimately helps reduce the potential impact of incidents.

For ports that still rely on paper forms, spreadsheets or disconnected systems, what is usually the first step towards a more digital safety and security process?

The first step is not technology, but identifying the processes that create the greatest operational friction.

Most ports do not need to digitise everything at once. A more effective approach is to start with a high-impact workflow, such as safety inductions, contractor management, permit-to-work processes or visitor control.

By digitising one critical process and demonstrating measurable benefits, organisations can build confidence, improve adoption and create a foundation for broader digital transformation initiatives.

Looking ahead, how do you think safety and security management in ports will change over the next few years?

I believe the industry will move increasingly from reactive management towards predictive and data-driven decision-making.

As more safety and security processes become digital, ports will gain access to richer operational data and better situational awareness. This will enable organisations to identify patterns, detect risks earlier and make more proactive interventions before incidents occur.

The future of port safety will not be defined by more procedures. It will be defined by better visibility, connected workflows and the ability to transform operational information into actionable intelligence. Ultimately, the goal is not only compliance but also creating safer ports and ensuring that everyone who enters a facility goes home safely.



The New Risk Landscape



Container Terminal
Conference
Americas

THE FUTURE OF TERMINALS IS BEING BUILT NOW

Intelligence.
Sustainability.
Growth.

SUPER EARLY BIRD

SAVE
UP TO **\$600**



PORTS & TERMINALS
ATTEND FREE

Complimentary delegate
passes available*



THE AMERICAS' LEADING TERMINAL TECHNOLOGY EVENT



16–17 FEBRUARY 2027



PANAMA



REGISTER TODAY

events.porttechnology.org/ctac-americas



Resilience by Design: How Ports Are Reinventing Safety and Security for a Volatile Era



Chloe Rowland,
Senior Manager: Data Collaboration,
Risk & Resilience, International
Association of Ports and Harbors

For much of modern maritime history, port safety and security were viewed through distinct lenses. Safety focused on protecting people, infrastructure and cargo from operational hazards. Security concentrated on preventing criminal activity, terrorism, smuggling and unauthorised access. Resilience, meanwhile, was often treated as a downstream outcome: the ability to recover after disruption.

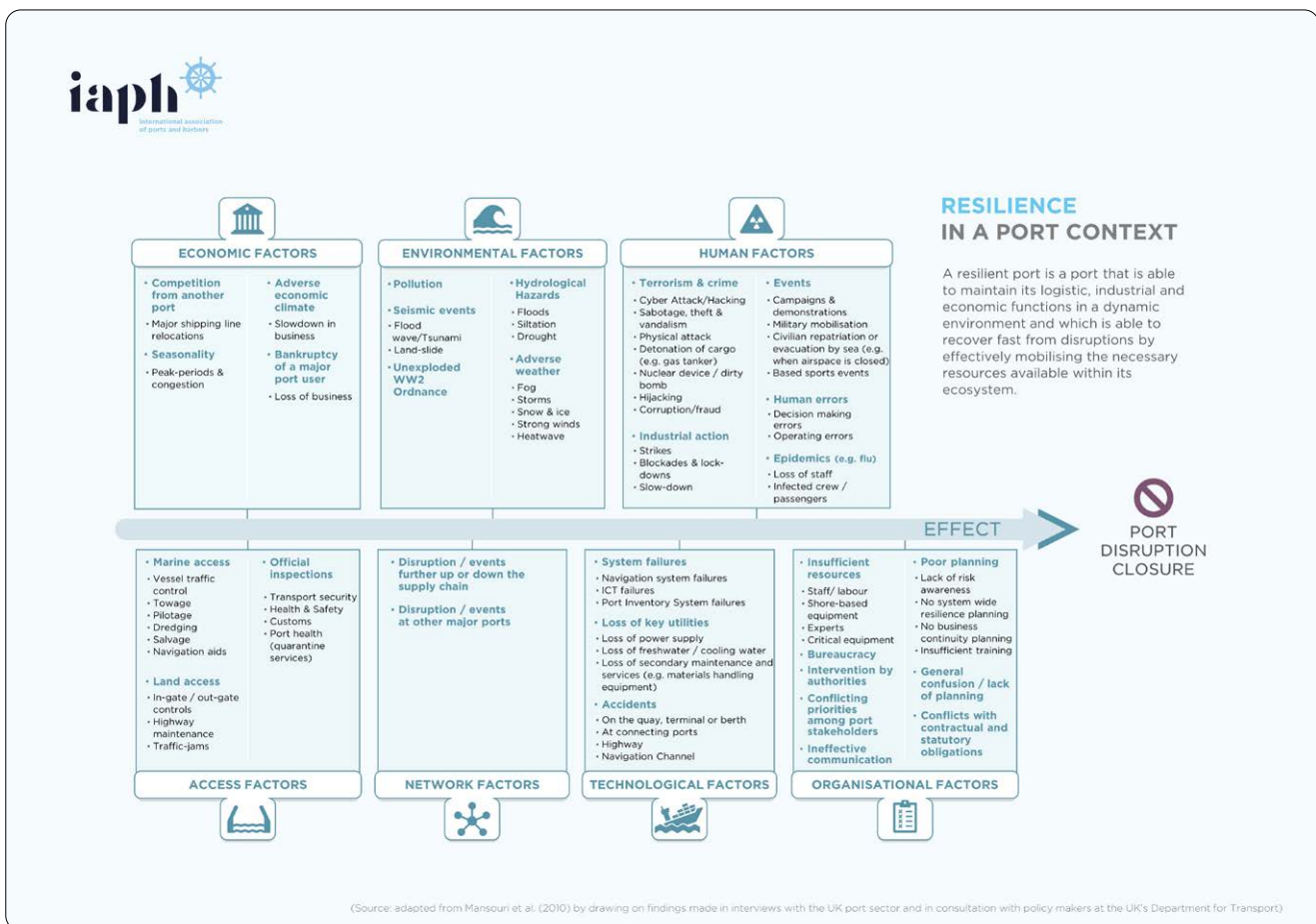
Today, those boundaries have collapsed. Ports now operate in an environment shaped by geopolitical volatility, cyber threats, climate disruption, supply chain fragility, automation, energy transition pressures and increasingly sophisticated criminal networks. No longer simply physical gateways for cargo, they have become deeply interconnected digital and physical ecosystems, functioning as critical

national infrastructure and essential nodes in global supply chains.

This reality is forcing a profound shift in how ports approach risk.

Around the world, port authorities and terminal operators are moving away from siloed approaches to safety, security and emergency response. In their place, a more integrated philosophy is emerging, built around resilience by design. The

“The question is no longer whether disruptions will occur, but how quickly and effectively ports can anticipate, absorb, respond to and recover from them.”



question is no longer whether disruptions will occur, but how quickly and effectively ports can anticipate, absorb, respond to and recover from them.

This transformation is taking place across multiple fronts: cyber resilience, physical security, emergency preparedness, risk governance, data collaboration and international cooperation. It is also reshaping the priorities of the global port community, including the work of the International Association of Ports and Harbors (IAPH), whose technical committees and collaborative initiatives increasingly focus on helping ports navigate a more complex operating environment.

The Expanding Threat Landscape

Ports have always had to manage operational risk. What has changed is the scale, speed and interconnectedness of modern threats.

A cyber incident in one logistics platform can ripple across multiple terminals and hinterland networks. Extreme weather

events can simultaneously disrupt port operations, energy supply and inland transport connectivity. Criminal organisations exploit digital vulnerabilities alongside physical weaknesses. At the same time, geopolitical tensions are introducing new uncertainties around trade routes, sanctions compliance and infrastructure protection.

The digitalisation of maritime supply chains has amplified both efficiency and exposure. Automated equipment, cloud-based logistics systems, Internet of Things (IoT) devices, drones, AI-enabled systems and remote operations all create new operational capabilities, but they also create new attack surfaces.

The maritime sector has already experienced the consequences of cyber disruption. High-profile attacks on shipping and logistics operators over the past decade have shown how cyber incidents can rapidly evolve into operational crises, with impacts measured in hundreds of millions of dollars and severe, long-term supply chain disruption.

For ports, the challenge is especially acute because operational technology (OT) and information technology (IT) environments are converging. Cranes, gates, vessel traffic systems, terminal operating systems and energy infrastructure are now digitally connected in ways that were unimaginable a generation ago.

This convergence has transformed cybersecurity from an IT issue into a core operational resilience issue.

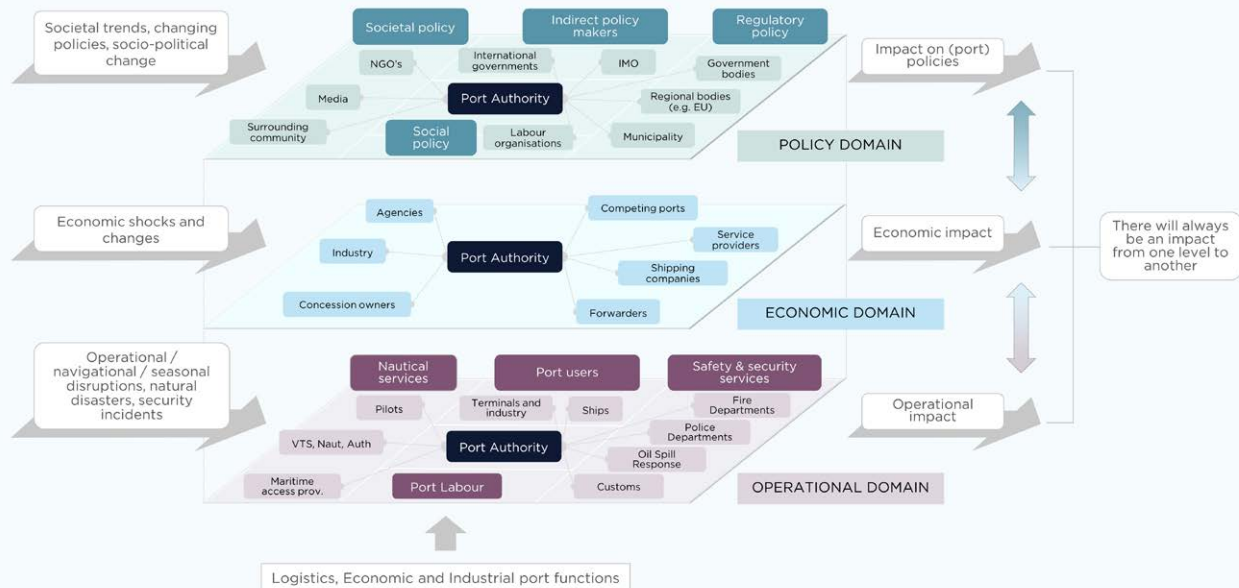
Cyber Resilience Becomes a Strategic Priority

Across the global port sector, cyber resilience has moved into the boardroom.

Ports are investing not only in cybersecurity tools, but also in governance frameworks, staff training, incident response planning and supply chain-wide collaboration. Increasingly, port leaders recognise that resilience depends as much on organisational preparedness and cross-sector coordination as it does on technical controls.



DEVELOPMENT OF AN ORGANISATIONAL RESILIENCE MODEL FOR PORTS



(Source: N. Vanlaere et al 2021 adapted from Padgett & Powell, 2012)

The work being undertaken within IAPH reflects this evolution. Through its Data Collaboration Committee and associated working groups, the Association has developed practical cybersecurity guidance aimed specifically at ports and port facilities.

In June 2025, IAPH launched updated cyber resilience guidelines addressing the risks associated with emerging technologies such as artificial intelligence, quantum computing, drones, IoT systems, 5G connectivity, automation and smart green energy infrastructure. These guidelines were developed through collaboration between ports, technology specialists, and IAPH partners, the World Bank and the World Economic Forum and can be found here: [IAPH Cyber Resilience Guidelines for Emerging Technologies in the Maritime Supply Chain by Ports & Harbors](#).

What is significant about this work is not simply the technical guidance, but the recognition that cyber resilience is inseparable from broader operational resilience. In 2023, IAPH published a

set of risk and resilience guidelines for ports, offering a structured process for defining and inventorying risk, managing stakeholders and building resilient operations. These guidelines can be found here: [IAPH Risk and Resilience Guidelines for Ports](#).

Ports increasingly understand that it is impossible to eliminate all cyber risk. Instead, the focus is shifting towards continuity: maintaining safe operations during disruption, rapidly isolating compromised systems, restoring services and minimising cascading impacts across the supply chain.

This aligns with a broader global trend towards resilience-oriented security frameworks. Traditional perimeter-based approaches are proving insufficient in highly connected operational environments. As critical infrastructure sectors adopt 'zero trust' models and more adaptive security architectures, ports are beginning to follow suit.

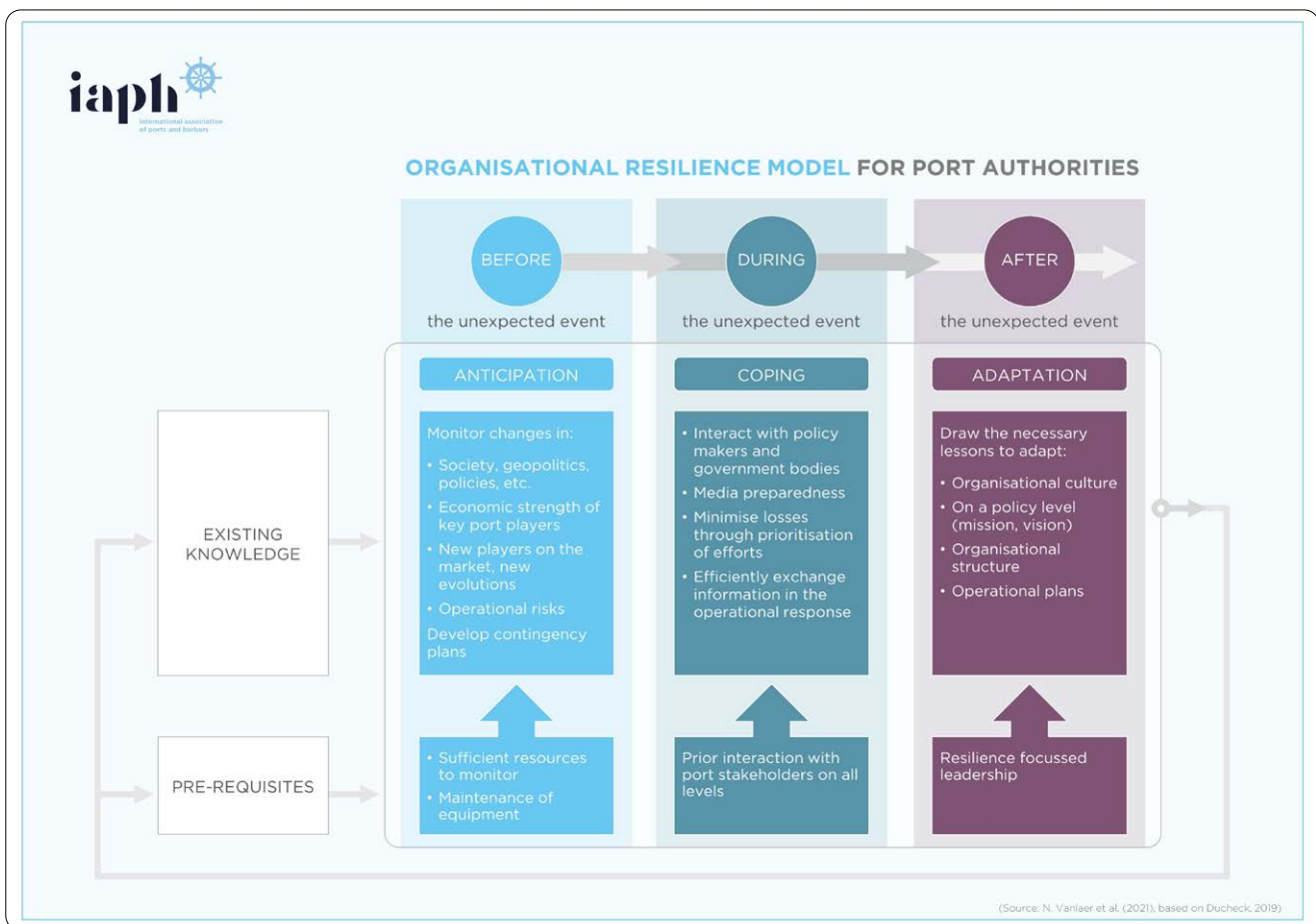
Importantly, human factors remain central.

Many successful cyberattacks exploit organisational weaknesses rather than purely technical vulnerabilities. Training, awareness, governance and incident simulation exercises are therefore becoming essential components of port resilience strategies. Cybersecurity is no longer confined to specialist teams; it increasingly involves everyone from harbour masters and operations personnel to boardroom executives and external stakeholders.

Physical Security in a More Complex World

While cyber resilience commands growing attention, physical security threats have not diminished. In many respects, they have become more complicated.

Ports face persistent risks associated with cargo theft, smuggling, organised crime, unauthorised access and potential terrorism-related activity. Geopolitical instability has also sharpened concerns about critical infrastructure protection and supply chain security.



At the same time, the energy transition is creating entirely new safety and security considerations. The growth of alternative fuels, battery storage systems, hydrogen infrastructure and electrified operations introduces unfamiliar operational hazards.

Recognising these evolving risks, IAPH's Risk and Resilience Committee has identified issues such as climate resilience, lithium-ion battery hazards and potential revisions to the International Ship and Port Facility Security (ISPS) Code as key priorities for 2026.

This reflects a broader industry realisation: resilience planning can no longer rely solely on historical assumptions about risk.

Ports are now reassessing everything from access control and surveillance systems to emergency evacuation procedures and mutual aid agreements. Many are also adopting more integrated command-and-control models that combine physical security monitoring with cyber situational awareness and operational continuity management.

In practice, this means that security operations centres increasingly monitor digital and physical environments simultaneously. A cyber intrusion affecting gate systems, for example, may now be treated as both a cybersecurity incident and a physical security event.

Emergency Preparedness as an Operational Discipline

One of the most important changes in the sector is the evolution of emergency preparedness from a compliance-driven exercise into a continuous operational discipline.

In the past, contingency planning was often document-based and heavily procedural. Today, leading ports are emphasising dynamic preparedness through regular training exercises, multi-agency simulations, cross-border coordination and real-time decision-making capabilities.

This shift is being driven by the recognition that crises rarely occur in

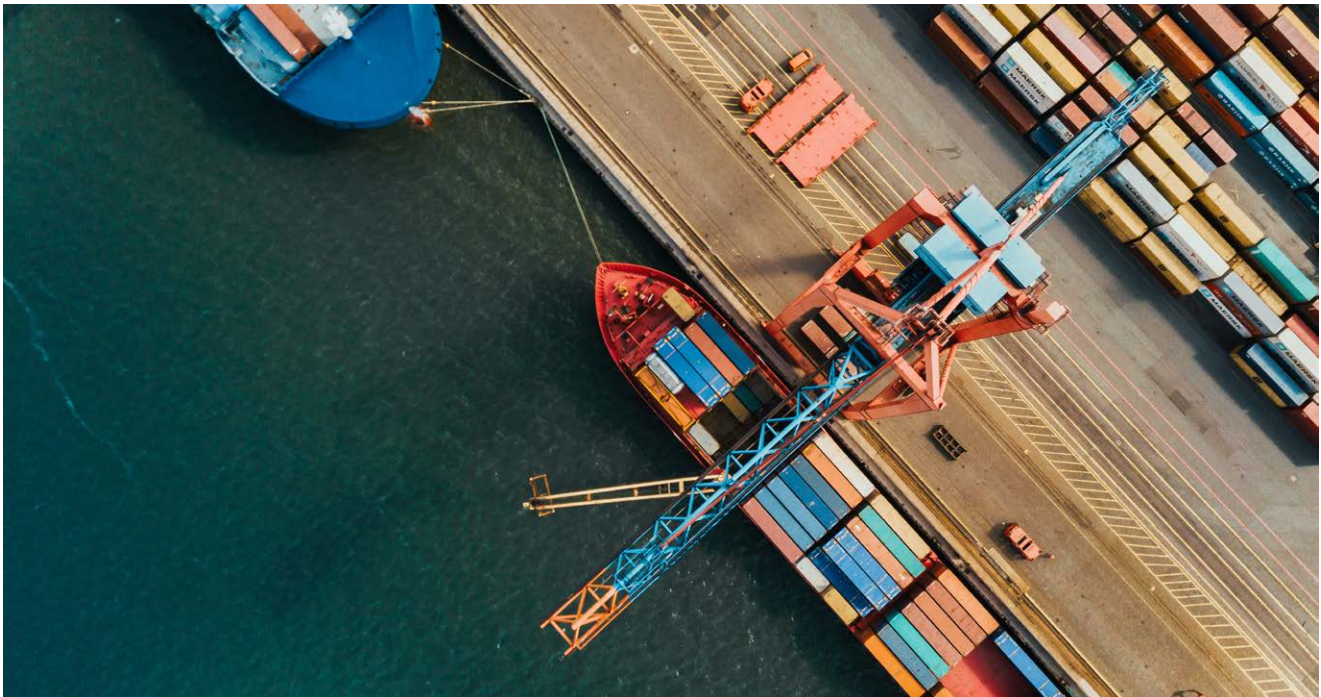
isolation. A cyber incident may exploit a severe weather event. Supply chain disruption may create congestion that increases physical safety risks. Energy outages may affect digital infrastructure. Effective response, therefore, depends on integrated planning and organisational adaptability.

Ports are increasingly investing in resilience centres, digital twins, predictive analytics and advanced monitoring systems to improve situational awareness during emergencies. Some are also using AI-driven tools to model disruption scenarios and optimise response planning.

However, technology alone is not sufficient.

The most resilient ports are often those with strong governance structures, clearly defined decision-making processes and well-established relationships with emergency services, coast guards, customs authorities, logistics operators and government agencies.

Collaboration remains critical because port resilience is fundamentally



interdependent. A port cannot be resilient if the surrounding transport network, energy infrastructure or digital ecosystem is vulnerable.

Data Collaboration and Shared Awareness

As ports become more digitally connected, data collaboration is emerging as a key enabler of resilience.

Historically, supply chain stakeholders often operated within fragmented information environments. Shipping lines, terminals, customs authorities, logistics providers and hinterland operators maintained separate systems with limited interoperability. That fragmentation reduced visibility and slowed crisis response.

Today, ports increasingly recognise that shared situational awareness improves both efficiency and resilience.

The IAPH Data Collaboration Committee is active in promoting a Port Call Optimisation framework and associated guidance for trusted data exchange across the maritime supply chain. The Association has highlighted the importance of public-private collaboration and interoperable digital ecosystems in strengthening operational resilience.

This focus is especially relevant during disruptions, when timely access to reliable information becomes critical. Shared

data platforms can support congestion management, incident response, cargo prioritisation and recovery planning.

Yet greater connectivity also introduces governance challenges around cybersecurity, privacy, data ownership and regulatory compliance. As ports accelerate digitalisation, resilience considerations must be embedded into system design from the outset. Security can no longer be treated as an afterthought added after deployment.

Climate Resilience and the Security Agenda

Another important shift is the growing integration of climate resilience into broader port security and risk-management strategies.

Extreme weather events, rising sea levels, flooding and heat-related operational disruptions are no longer distant concerns. They are increasingly immediate operational realities affecting ports across all regions.

Climate-related risks have significant security implications. Infrastructure damage, prolonged operational shutdowns, energy disruptions and supply chain interruptions can quickly evolve into broader economic and societal challenges.

For ports, climate resilience therefore intersects directly with business continuity, infrastructure protection and emergency

preparedness. This is one reason why climate resilience has become a central focus within IAPH's Risk and Resilience Committee agenda.

Many ports are now conducting integrated risk assessments that examine physical climate vulnerabilities alongside cyber, operational and geopolitical threats. Others are investing in adaptive and environmentally sustainable infrastructure, flood defences, resilient energy systems and diversified operational capabilities.

The lesson is increasingly clear: resilience cannot be compartmentalised. Physical, digital, environmental and geopolitical risks are interconnected and must be managed holistically.

International Cooperation as a Strategic Imperative

Perhaps the most important development of all is the growing recognition that resilience is a shared global responsibility.

Ports do not operate in isolation. They are part of international networks where disruptions in one region can have cascading global effects. As the events of recent years have demonstrated, vulnerabilities in maritime supply chains rapidly transcend national boundaries.

This reality makes international cooperation indispensable.

Organisations such as the International Maritime Organization, the World Economic Forum and IAPH therefore play a critical role in creating shared standards, guidance frameworks and collaborative platforms for knowledge exchange.

This collaborative approach matters because many resilience challenges cannot be solved individually. Cyber threats evolve globally. Supply chain disruptions cross borders. Climate risks affect entire trade corridors. Emerging technologies introduce shared vulnerabilities across multiple jurisdictions.

International alignment on standards, best practices, and incident response coordination will therefore become ever more important in the years ahead.

From Protection to Adaptation

The port sector is entering a new era of resilience thinking.

The traditional goal of preventing disruption entirely is giving way to a more realistic and adaptive model: anticipating disruption, minimising impact and recovering quickly while maintaining operational continuity.

This does not mean abandoning safety or security fundamentals. On the contrary, it means integrating them more effectively into broader resilience strategies that reflect the complexity of today's operating environment.

For ports, resilience is no longer just about infrastructure hardening or regulatory compliance. It is about

organisational agility, digital trust, collaborative governance and the ability to function under conditions of uncertainty, be they physical, political or both.

That evolution will continue to shape investment priorities, operational models and international cooperation across the maritime sector.

The ports that succeed in this environment will not necessarily be those with the largest infrastructure footprints or the most advanced technologies. They will be the ones capable of adapting continuously to changing risks while maintaining the confidence of customers, governments and communities alike.

In an increasingly unpredictable world, resilience itself is becoming the defining infrastructure of global trade.

About the author

Chloe Rowland is the Senior Manager for Data Collaboration, Risk & Resilience at the International Association of Ports and Harbors (IAPH). She has extensive experience in strategic leadership, stakeholder engagement and network and relationship development, as well as close working partnerships with governments, NGOs, the UN agencies, international policy makers, regulatory bodies, defence forces and key maritime industry stakeholders worldwide. Her role is primarily focused on IAPH activities in the fields of maritime supply chain security and resilience, general port operational risk management, climate resilience, digitalisation, and cyber-secure maritime operations. She is also active in representing member ports' interests at the regulatory level at the International Maritime Organization, the World Customs Organization, the International Organization for Standardization (ISO) and other global alliances such as the Global Maritime Forum and the World Economic Forum. Chloe is also a Harbour Commissioner for Plymouth Cattewater in the Southwest of the UK.

About the association

IAPH is a non-governmental organisation headquartered in Tokyo, Japan. Formed in November 1955, IAPH has developed into a global alliance of ports, today representing more than 400 ports and port-related businesses in over 90 countries. The member ports together handle well over 60 per cent of the world's seaborne trade and world container traffic. IAPH aims to be the global trade association of choice for port authorities and operators, representing their interests at the regulatory level at the International Maritime Organization, the World Customs Organization, the ISO and other global alliances such as the Global Maritime Forum and the World Economic Forum. IAPH has consultative status and works on behalf of ports with additional United Nations bodies such as the UN Conference on Trade and Development (UNCTAD), United Nations Environment Programme (UNEP) and the UN Global Compact.



Competitiveness and Resilience: Two Sides of the Same Lucky Coin for Europe's Terminal Operators



Lamia Kerdjoudj,
Secretary General, FEPORT

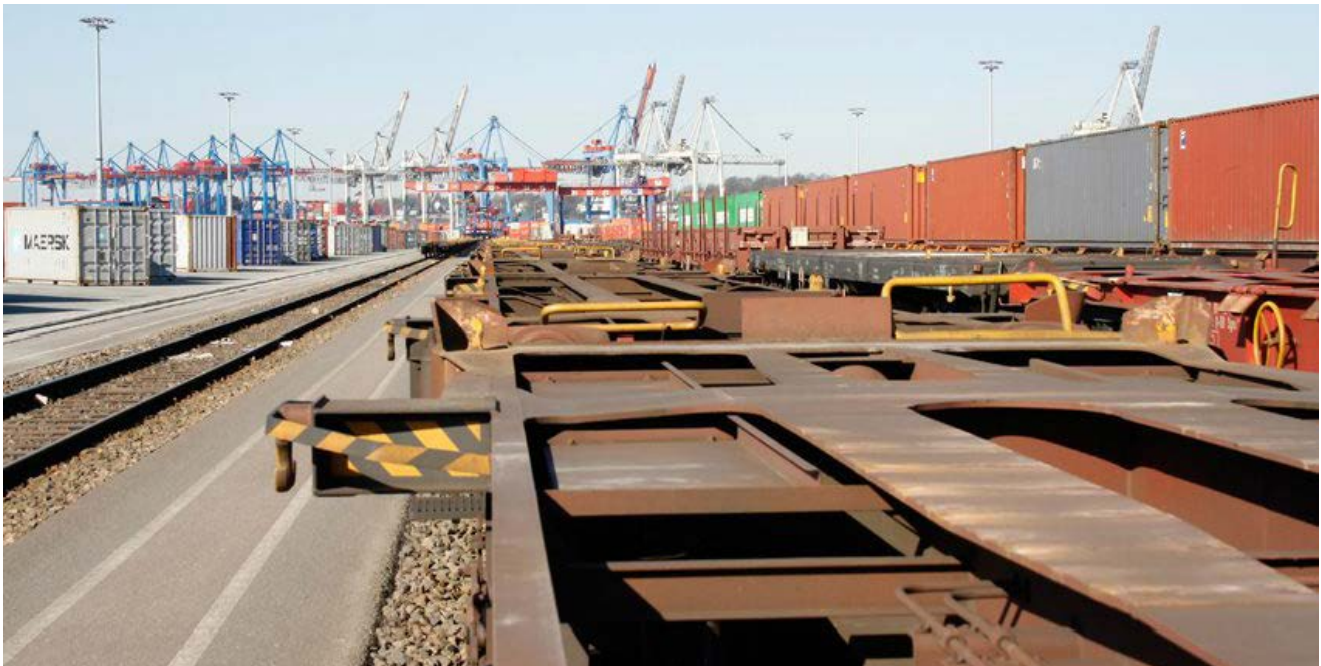
Over the last five years, European terminal operators have demonstrated remarkable resilience. They kept supply chains moving during the COVID-19 pandemic, adapted to the consequences of Russia's war against Ukraine, responded to disruptions affecting

global shipping routes and continued investing in the green and digital transitions despite growing economic uncertainty.

Today, however, the expectations placed on ports and terminals extend far beyond their traditional role as gateways for trade.

European ports are increasingly recognised as strategic assets. They are expected to facilitate international trade, contribute to the energy transition, support military mobility, strengthen Europe's economic security, combat organised

**"Competitiveness and resilience are not competing objectives.
For Europe's ports and terminals, they are two sides of the same coin."**



crime, enhance cybersecurity and improve the resilience of supply chains. At the same time, they must remain competitive in a global environment characterised by intense international competition and significant investment needs.

The publication of the EU Ports Strategy in March 2026 reflects this new reality. The Strategy acknowledges the growing role of ports as critical infrastructure underpinning Europe's competitiveness, security and strategic autonomy. It also highlights the need to ensure that European ports remain attractive destinations for investment while adapting to evolving geopolitical, technological and environmental challenges.

For terminal operators, resilience is no longer limited to emergency preparedness or business continuity planning. It has become the ability to adapt, invest and continue delivering reliable services in an environment marked by geopolitical uncertainty, technological transformation, evolving security risks and growing regulatory expectations.

In this context, competitiveness and resilience should not be viewed as competing objectives. On the contrary, they are mutually reinforcing. Without competitive ports and terminals capable of attracting investment, resilience ambitions will remain difficult to achieve. Likewise, without resilient infrastructure, Europe's ports will struggle to remain attractive and competitive in the long term.

Resilience in a More Complex Operating Environment

The operating environment facing terminal operators has changed considerably over the past decade.

Ports have always dealt with operational safety concerns, physical security risks and the challenges associated with managing complex logistics operations. Today, these traditional responsibilities coexist with a new generation of risks that are increasingly interconnected.

Geopolitical developments have demonstrated how quickly disruptions can affect global trade. The consequences of the war in Ukraine, disruptions in the Red Sea and growing uncertainty surrounding international supply chains have forced operators to adapt rapidly to changing cargo flows, fluctuating demand and operational constraints.

At the same time, organised criminal networks continue to exploit ports as critical nodes in international logistics chains. Drug trafficking, cargo manipulation and the infiltration of supply chains require constant vigilance and close cooperation between terminal operators, port authorities, customs authorities and law enforcement agencies.

Climate-related challenges are adding another layer of complexity. Extreme weather events, flooding and storms can disrupt operations and damage

infrastructure, while the energy transition requires ports to accommodate new technologies, fuels and operational models.

"The reality for terminal operators is that these risks rarely occur in isolation. Physical security, operational continuity, cybersecurity, workforce preparedness and infrastructure reliability are increasingly interconnected. Resilience therefore requires a holistic approach capable of addressing multiple challenges simultaneously," says Lamia Kerdjoudj, Secretary General of FEPORT.

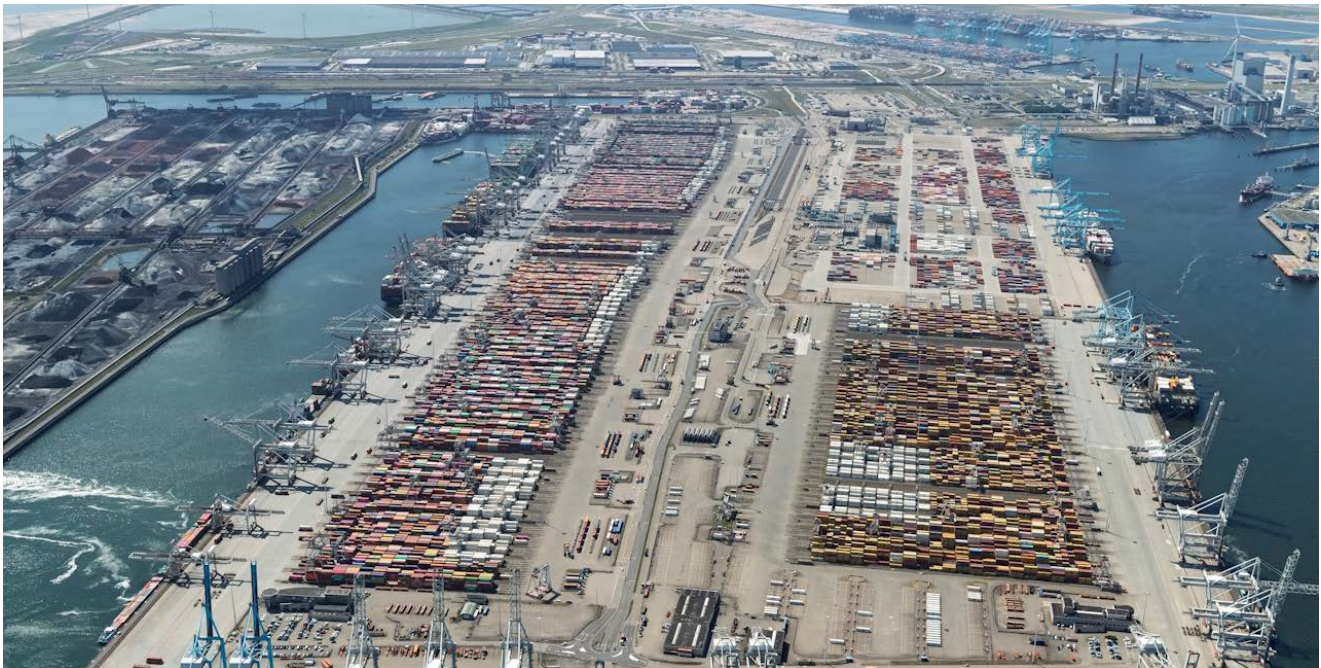
Investment: Turning Ambition into Reality

Resilience cannot be achieved without investment.

Whether the objective is strengthening cybersecurity, upgrading security systems, deploying clean technologies, enhancing energy infrastructure or improving operational capabilities, investment remains the common denominator.

This reality should remain central to ongoing European policy discussions.

The EU Ports Strategy rightly recognises that ports are expected to contribute simultaneously to competitiveness, security, decarbonisation and resilience. Achieving these objectives will require substantial investment from both public and private actors.



This is particularly relevant in a context where terminal operators are investing in electrification, onshore power supply, alternative fuels infrastructure, cybersecurity measures, organised crime prevention initiatives and infrastructure supporting military mobility. Facilitating such investments should be viewed as a contribution to Europe's economic security and strategic autonomy.

"Ongoing discussions regarding State Aid rules and the revised General Block Exemption Regulation (GBER) should consider how investments contributing to resilience, security and decarbonisation can be accelerated and supported. Regulatory frameworks should be adjusted and adapted in a timely manner to enable the implementation of EU policies; otherwise, we will miss the competitiveness race with other regions of the world," adds Lamia Kerdjoudj.

Similarly, ongoing discussions regarding the use of revenues generated through the EU Emissions Trading System offer an opportunity to support investments that contribute to both the green transition and operational resilience. As FEPORT has repeatedly highlighted, European ports are expected to deliver multiple policy objectives simultaneously. Ensuring that part of the revenues generated by the maritime ETS is reinvested into port-related projects would support the deployment of clean technologies,

infrastructure upgrades and resilience-enhancing measures that benefit the entire logistics chain.

Cybersecurity: From Technical Issue to Strategic Priority

Digitalisation has transformed terminal operations. Automated gates, smart logistics systems, digital documentation, remote monitoring solutions and data-driven operational management have significantly improved efficiency and transparency across the supply chain.

However, increased connectivity also creates new vulnerabilities.

The distinction between physical and cyber threats is becoming increasingly blurred. Criminal organisations seeking to exploit weaknesses in logistics chains may target both physical infrastructure and digital systems. Access management, cargo information, operational technology and communication networks have all become critical components of port security.

Cybersecurity can therefore no longer be viewed solely as an IT issue. It is a strategic business concern that directly affects operational continuity, customer confidence and supply chain reliability.

The implementation of the NIS2 Directive and the growing focus on protecting critical infrastructure demonstrate that policymakers increasingly recognise the strategic

importance of cybersecurity. Yet compliance alone will not be sufficient. Effective cyber resilience requires continuous investment in technology, governance, risk management, incident response capabilities and staff awareness.

The maritime and port sector has already recognised the value of collective action in strengthening cyber resilience. In this context, FEPORT is involved in SAFEDIGIMAR, a European project supported under the Digital Europe Programme and implemented together with France Cyber Maritime and Federazione del Mare. The project aims to support the implementation of the NIS2 Directive across the maritime ecosystem by strengthening the protection of network and information systems, improving incident detection and reporting mechanisms, and enhancing cooperation between industry, national authorities and law enforcement bodies. Beyond regulatory compliance, SAFEDIGIMAR seeks to provide practical tools, training activities and monitoring mechanisms that help ports and terminal operators improve their cybersecurity posture and preparedness in an increasingly digitalised environment.

As ports become more interconnected and data-driven, cyber resilience is not only a technical challenge but also a matter of operational readiness, cooperation and trust across the entire logistics chain.

Ports at the Heart of Europe's Strategic Objectives

The growing emphasis on military mobility provides a useful illustration of how the role of ports is evolving.

While discussions often focus on roads, railways and defence infrastructure, ports are equally essential to the movement of equipment, supplies and strategic goods. Many terminals effectively serve dual-use functions, supporting both commercial activities and broader European security objectives.

Similarly, ports are expected to contribute to Europe's ambitions regarding economic security, strategic autonomy and supply chain resilience. They play a critical role in facilitating trade, supporting industrial value chains and ensuring access to energy resources, raw materials and strategic goods.

These expectations place additional responsibilities on terminal operators. Infrastructure must be reliable, secure and capable of adapting to changing operational requirements. Operational continuity, cybersecurity and crisis preparedness are becoming increasingly important not only from a commercial perspective but also from a strategic one.

As Europe seeks to strengthen its resilience in an increasingly uncertain world, ports will continue to play a central role. However, delivering on these expectations requires a supportive policy framework that recognises the realities of terminal operations and enables long-term investment.

Skills: The Often Overlooked Pillar of Resilience

While discussions on safety and security frequently focus on infrastructure and technology, one of the most important dimensions of resilience remains people.

The port sector is undergoing profound transformation driven by digitalisation, automation and decarbonisation. These developments are creating new skills requirements across terminals and logistics operations.

Advanced technologies can improve safety and efficiency, but they also require a workforce capable of operating, maintaining and securing increasingly sophisticated systems. The deployment of automated equipment, digital platforms and cybersecurity tools creates new training needs and highlights the importance of continuous upskilling and reskilling.

Across Europe, ports are already facing recruitment challenges in several technical and operational professions. These shortages have direct implications for resilience. A terminal may invest heavily in new technologies, but resilience ultimately depends on the availability of skilled workers capable of responding effectively during periods of disruption.

This challenge is receiving increasing attention within the European port sector. Beyond infrastructure and technology, workforce development is becoming a strategic priority. Initiatives focusing on training, inclusion, skills anticipation and social dialogue will play an important role in ensuring that ports remain capable of adapting to changing operational and technological requirements.

"Investment in people should therefore be considered as important as investment in infrastructure. In a rapidly changing operating environment, resilience will depend not only on the infrastructure ports build, but also on the capabilities of the people who operate it," says Kerdjoudj.

Looking Ahead

European ports and terminals are entering a period in which resilience will increasingly define competitiveness.

The challenges facing the sector are diverse: organised crime, cyber threats, geopolitical uncertainty, climate-related disruptions, skills shortages and growing strategic expectations. Addressing these challenges will require cooperation between public authorities, port authorities, terminal operators and other stakeholders.

The central lesson, however, remains simple.

Safe and secure ports are not created solely through regulation. They are built through investment, innovation, skilled people and long-term planning.

Competitiveness and resilience are not competing objectives. For Europe's ports and terminals, they are two sides of the same coin.

"As Europe seeks to strengthen its economic security, support military mobility, accelerate the energy transition and improve supply chain resilience, ports will continue to play a critical role. Ensuring that terminal operators have the legal certainty to invest in this transformation is therefore not only a sectoral priority; it is a European strategic imperative," concludes Ms Lamia Kerdjoudj.

About the author

Ms Lamia Kerdjoudj has been Secretary General of FEPORT, the Federation of European Private Port Companies and Terminals, since March 2014. She has more than 27 years of professional experience, during which she has held different positions within the maritime and logistics sector. Among others, she was, for more than seven years, the Public Affairs Manager of the French Shipowners' Organisation.

Between 2009 and 2012, she was also appointed as a senior expert and adviser in the framework of several European projects financed by different directorates of the European Commission. She has also worked for private companies and corporations and has been in charge of consulting and business development assignments for large multinational companies.

About the association

FEPORT represents the interests of 2,290 private seaport companies and operators that perform cargo-handling and logistics-related activities in the seaports of the European Union, Norway and Turkey. FEPORT members employ around 400,000 port workers and have invested more than €70 billion over the last 10 years to enhance the attractiveness and competitiveness of European seaports.



Connecting Horizons: Building Future-Resilient Ports Together



Captain Kevin G Allen,
President, International Harbour Masters Association

I am writing this editorial having just returned home from another fascinating and successful 15th International Harbour Master Congress in Rotterdam, held with the support of State Harbour Master René de Vries and his superb team at the Port of Rotterdam.

The Congress brought together 174 delegates from across the globe: Harbour Masters, marine managers, technical port professionals and industry professionals

for three days of animated discussions and workshops through the lens of what faces us in the future.

Our theme of "Building Future-Resilient Ports Together" gave everyone the opportunity to discuss the ever-present and changing challenges facing Harbour Masters worldwide.

Evident from the beginning of the Congress was the passion and

commitment of my colleagues and the marine industries, working together to provide solutions and support to ensure safe, efficient and sustainable trade can continue in an environment where the rules-based order, as understood for a generation, is now changing.

This was echoed loud and clear by the State Harbour Master for the Port of Rotterdam, René de Vries, who told

"The challenges we face are no longer just about managing wind and tide."



delegates: "This year's theme, Connecting Horizons -Building Future Resilient Ports Together, is not just a slogan; it is a call to action. It is a reminder that in a world of rapid change, our strength lies in our unity, our innovation and our shared commitment to resilience."

The global maritime and port sector stands at a critical crossroads where technological acceleration, environmental responsibility and human capability must converge. Relying on legacy operational models is no longer a choice as global supply chains face mounting climate pressures, rapid digital innovation and cyber or physical risks of disruption.

Building a truly resilient maritime ecosystem requires an integrated strategy that addresses the needs of our industry: digital innovation, sustainable operations and human capital.

The modern commercial port, irrespective of scale, is also an arena of compounding risk. As the global shipping industry pushes the boundaries, the traditional role of the Harbour Master, particularly in smaller regional ports, is undergoing a radical transformation.

Once viewed primarily as the chief enforcement officer of local maritime bylaws, today's Harbour Master must perform as a strategist, IT integration expert, environmental expert and crisis manager all at once. This position was highlighted by Isabelle Ryckbost, the Secretary General

of ESPO. In her address to the assembled delegates, she discussed climate resilience, decarbonisation, alternative fuels, sanctions and the changing geopolitical landscape.

The challenges we face are no longer just about managing wind and tide. They are about navigating a perfect storm of unprecedented vessel scale, rapid digitalisation, a volatile risk landscape and increasingly severe consequences when it all goes wrong.

Digital Innovation

Digitalisation is transforming the maritime and port sector, and the pace of innovation is accelerating. During the first day, the speakers and expert panels explored the technologies that are redefining how ports operate, connect and evolve.

We heard submissions on a broad array of cutting-edge tools and methodologies, such as AI-driven decision support systems, drone technologies and innovative data standards such as S-100. Whether we were piloting a new solution, scaling up a proven tool or rethinking how technology supports collaboration, we shared practical experiences, learned from each other and discovered what is next on the digital horizon.

This left me with the reinforced understanding that digitalisation is necessary to allow improved efficiencies, but it introduces vulnerabilities which must be protected.

Sustainable Operations

Sustainability is a shared challenge across the maritime sector and other economic sectors. On day two, we focused on how the industry is working towards greener operations together. There were contributions and case studies from port authorities and industry experts on decarbonisation strategies, the use of alternative fuels and other innovations related to sustainability.

The enduring memory, however, was the keynote morning address by the Port of Rotterdam CEO, Boudewijn Siemons, who highlighted for the audience the concerns of European ports on cyber and physical security and geopolitical instability from either internal or external actors.

On the environment, he shared how the port and environmental NGOs generally share the same goals but vary in method or expectations around the time of delivery. He confirmed that the environment and resilience are among the highest priorities in his port's strategy.

Within the port industry, he knows better than most the pressures of competition. He said: "We should compete where we have to and co-operate when we can".

Clearly recognising the need for the broadest collaboration on all aspects of the challenges facing us in the future, he



also suggested: “We should meet each other before we need each other”, sage advice indeed.

Human Capital

On our final day, we focused on what is, for me, our biggest challenge: the human and organisational dimensions of resilience in the port sector. We were treated to expert insight into the building or transforming of port infrastructure to be resilient.

The President of PIANC, Señor Francisco Esteban Lefler, emphasised the need to invest time to understand the problem before implementing the solution. This requires the right skills and resources to be engaged in defining both the problem and the solution.

We further welcomed contributions on safety and security, workforce development, training, and strategies to attract and retain talent. These human capital topics made us think about diversity, inclusion, leadership and international cooperation.

On the point of security, Arthur van Lohuijzen again reaffirmed this need for cooperation. He told delegates that when international regulations, such as ISPS, no longer meet the threats facing Europe's largest ports, action initiated by the Port of Antwerp brought them together with

Hamburg and Rotterdam to develop an agreed way forward on security management.

As with any collection of passionate professionals, consensus or agreement on solutions was not always the case, with autonomous operations being one example. Who regulates first: port, region, state, or do we wait on the machinations of international regulation through the IMO?

It is too simplistic to think that the Harbour Master will blindly regulate or adopt new operations without fully understanding the risks to marine and wider port safety. This is a position not shared, or perhaps not understood, by some in industry, or even the ports we work in. My own experience as the Appointed Person for drone operations in Belfast Harbour is a lived example of trying to do the right thing in the wrong way.

Change management, therefore, must be resourced by properly trained, skilled and experienced personnel in adequate numbers to achieve the objectives. This is not easy in a world of dynamic challenges, where failure can be catastrophic on a local scale, such as the MV Dali, or an international scale, such as the MV Ever Given, against a backdrop of diminishing budgets and reluctance to invest in people.

But perhaps our biggest problem is finding the right people and training them in the right way.

Captain and Professor Syamantak Bhattacharya of Sharjah Maritime Academy gave the audience reason to think in presenting the questions:

- Is STCW still fit for purpose?
- Do we train new recruits to our industry in the right way, given generational changes in expectations?
- Are we attracting the right candidates?
- So, what do we need to do to build future-resilient ports together?

As a marine professional with 44 years of experience and in the twilight of my career, I suggest some things to consider.

The evolution of port activity requires the acceleration of change from reactive traffic management to proactive maritime governance.

Harbour Masters within their ports will always be the referees watching from the shore as activities outside their control, namely ships, enter into their sphere of risk management. However, as the International Harbour Masters Association and as an NGO within the IMO, we must double our efforts in advocating for reform

and updating international standards. This includes matters such as vessel design, manning and STCW crew training, education for marine pilots, and the introduction of international standards for ports and Harbour Masters on managing marine safety and emergencies. ISM was first introduced on ships on 1 July 1998, but the ports they visit may or may not have a similar formalised safety management system.

We must recognise and accept that, depending on the scale, profit and resource capacity of the port we work in, being a jack of all trades and a master of only one, while once suited to traditional port risk such as traffic management, weather and the many vagaries of shipping, may not be right for the future.

The modern port risk profile has not lost any of the old risk, but it has added cyber and dynamic physical threats to infrastructure. This has not diminished the risk management role of the Harbour Master. This means they need to be better equipped, either through more training or specialist resourcing support, to keep ports functioning in times of crisis. Therefore, while our traditional command structure is still required, modern port emergencies cannot be resolved without adding dedicated specialisms such as IT and security personnel to the response team. Harbour Masters are available 24/7/365 to manage safe and efficient operations.

Do all ports receive the same level of support from their IT teams?

The President of PIANC, Señor Francisco Esteban Lefler, told us we need to understand the problem before setting out the solution. Increasing challenges mean the need for more solutions. Existing ports need to prioritise where digitalisation starts, accepting that this must begin with proper security, then consider where decarbonisation, electrification, navigational safety and traffic management efficiencies sit. For me, it is always marine safety and the protection of people and the marine environment. In a business of competing priorities and limited resourcing, my experience has shown me that priorities may be diverted towards areas that are more show than substance rather than essential business needs.

The economic pressure to operate ageing infrastructure, accept larger ships and achieve faster turnarounds will always be present. However, the ultimate responsibility of the Harbour Master remains unchanged, so in an era of compounding complexity, maintaining their authority to manage shipping is essential.

We at the International Harbour Masters Association recognise these challenges and the importance of working collaboratively. Our greatest asset will always be our shared commitment to evolution without compromising on safety.

About the author

Captain Kevin Allen has worked in the marine industry since the age of 16 and is approaching his 45th year. He has served on a range of ship types, including almost 10 years in command on passenger ferries across the Irish Sea and English Channel. He has spent 20 years in Belfast Harbour's Port Operations department, 18 as Harbour Master. He is President of IHMA and a long-serving RNLI volunteer.

About the association

The International Harbour Masters Association (IHMA) is a professional membership association for those responsible for the safe, secure, efficient and environmentally sound conduct of marine operations in port waters. Its members include Harbour Masters, port operations managers, VTS managers and others involved in the control of marine operations. IHMA has observer status at IMO and supports members through information, resources and participation in relevant industry work.



People, Skills and Safety Culture



**Maritime
Information
Services**

MIS MEDIA PACK 2026

Connect with the global
maritime audience that
moves the world forward.



50,000+

senior maritime
executives and
decision-makers



25,000+

international
website visitors



40,000+

page views



900,000+

LinkedIn
impressions

OPPORTUNITIES TO GROW YOUR BRAND



TAILORED MARKETING PACKAGES

Built around your
business objectives
and commercial goals.



TARGETED EMAIL CAMPAIGNS

Reach a highly engaged
audience with the
right message.



WEBINARS

Position your organisation
as a thought leader and
generate qualified leads.



SPONSORED CONTENT & DIGITAL ADVERTISING

Increase visibility, drive
engagement, and build
brand awareness.



VIEW THE MIS MEDIA PACK

Explore opportunities to
connect, engage and grow
with the maritime industry.



MIS is growing rapidly.
Partner with us now and
be seen by an expanding
audience of senior maritime
decision-makers.



A Safer Tomorrow: Turning Insight into Action Across Port Safety, Skills and Culture


 PORT SKILLS
& SAFETY
IMPROVING STANDARDS THROUGH COLLABORATION

Debbie Cavaldoro,
CEO, Port Skills and Safety Ltd

Achieving continuous improvement in safety is an ongoing challenge for any sector, and for ports in the UK, the last few years have felt like all the 'easy wins' have been achieved. Walking through most UK ports, PPE is being consistently worn, the health and safety office has risk assessments, policies and safe operating procedures for operations, and even the Health and Safety Executive views the sector as mature, with a good health and safety record.

Despite these improvements, the sector is not standing still on safety. Through the sector safety body Port Skills and Safety (PSS), it is working to ensure a safer tomorrow, where lessons are learned, best practice is shared, and everyone goes home safely at the end of the day.

To deliver a "safer tomorrow", it is tempting to focus solely on new technologies: automation, artificial intelligence and remote operations. While

those developments are undoubtedly part of the story, they are not the starting point and will not protect people from harm if adopted in isolation. A safer tomorrow for ports will be shaped by how we lead, how we learn and how we invest in people.

Across the port sector, there is no shortage of awareness about what needs to improve. Conversations about safety culture, workforce capability, and operational risk are well established.

"Skills are not a supporting factor in safety; they are its foundation."



Yet there remains a gap between knowing and doing. The challenge now is not identifying the right direction but embedding it consistently and at scale.

At the heart of that challenge are three interconnected themes: culture, competence, and the intelligent use of data and technology. Progress in one depends on progress in all.

From Safety Culture to Company Culture

For many years, the sector has focused on “safety culture” as a distinct concept, something to be managed by the safety team, developed and measured. That framing has been useful, but the sector now needs to build on this.

Safety culture is not a standalone system that can be installed or managed in isolation, and it is not just for the safety team. It is the outcome of broader company culture: the everyday behaviours, decisions and priorities that define how work is actually done. When organisations talk about improving safety culture without addressing the underlying company culture, they risk focusing on symptoms rather than causes.

This is increasingly recognised across ports. The way leaders behave, the questions they ask, how often they “walk the quay”, and the trade-offs they accept all send powerful signals. Where leadership consistently prioritises “how safe” alongside

“how fast” or “how much”, the tone is set for the entire organisation. Where that alignment is missing, even well-intentioned safety initiatives struggle to gain traction.

Frontline teams and middle managers often feel this tension most acutely. They are asked to deliver operational performance while also driving cultural change, frequently without the time, resources, or support required. When senior messages are not matched by visible action and meaningful support, it becomes harder to sustain momentum.

Closing this gap requires leadership that goes beyond endorsement. It demands visible commitment, role modelling, and accountability. It also requires recognising what has already been achieved. Ports have made significant progress in safety over recent years, and acknowledging that progress is essential to building confidence and engagement for the next stage.

Ultimately, the goal is not to create a separate safety culture, but to embed safety as an integral part of “the way we do things here.” That means moving from compliance to shared responsibility, from delegation to ownership, and from aspiration to action.

Learning Differently: From Failure and From Success

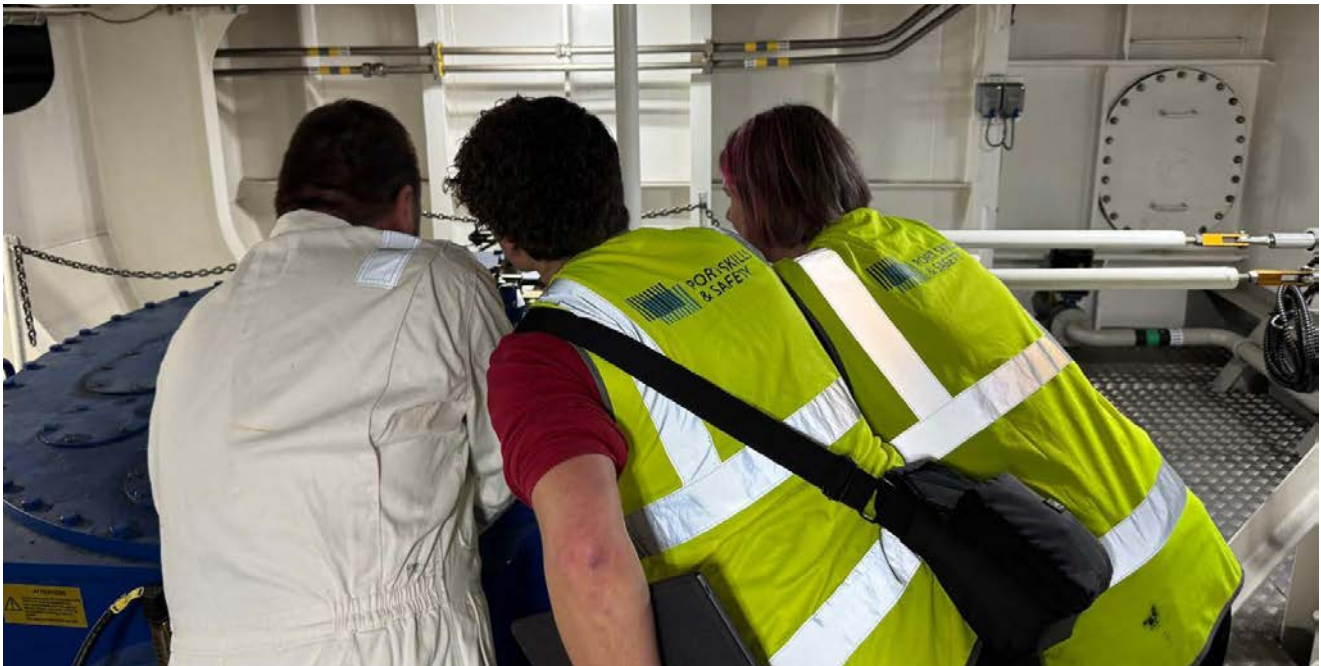
Ports generate a significant volume of safety data, particularly through incident

and near-miss reporting. This has traditionally formed the backbone of safety improvement efforts, with investigations focused on understanding what went wrong and how to prevent recurrence. While incident investigation remains essential, it is also only part of the picture.

If we are serious about moving from reactive to proactive safety, we need to expand our focus to include what goes right. Every day, across the sector, complex operations are carried out safely and efficiently. These successes often go unexamined, yet they contain valuable insights into the conditions that enable good performance.

Understanding “why things go right” requires a different mindset. It involves looking at normal work, not just exceptional events. It means engaging with frontline teams to understand how they adapt, make decisions and manage risk in real time. It also requires capturing richer, more qualitative data through conversations, observations and structured reflection.

By analysing both success and failure, ports can begin to identify patterns, strengthen positive behaviours, and detect early warning signs before incidents occur. This approach supports a more balanced and realistic understanding of risk, grounded in how work is actually done rather than how it is assumed to be done.



Importantly, this shift also reinforces psychological safety. When reporting and learning are not solely associated with things going wrong, but also with recognising what works well, engagement improves. People are more likely to contribute openly when they see that learning is about improvement, not blame.

The Role of Data and Technology

The growing availability of data presents a significant opportunity for the sector when used effectively. Ports already collect large amounts of information, yet much of it remains underutilised. Incident reports, for example, often contain rich qualitative detail that is difficult to analyse at scale using traditional methods. Advances in data analytics and artificial intelligence offer new ways to unlock these insights, identify trends, patterns and systemic issues that might otherwise go unnoticed.

However, technology is not a shortcut. Implementing new tools requires investment, not just in systems, but in time, capability and understanding. It also requires clarity about purpose. Technology should enhance human decision-making, not replace it.

There is a risk in viewing digitalisation and automation as solutions in themselves. In reality, they introduce new

types of risk alongside new opportunities. Ensuring that these technologies contribute positively to safety depends on how they are designed, implemented, and integrated into existing operations.

This reinforces a critical point: the effectiveness of technology is directly linked to the capability of the workforce using it.

Skills as the Foundation of Safety

While culture shapes behaviour, and data informs decisions, it is people who ultimately deliver safe and efficient operations. Skills are not a supporting factor in safety; they are its foundation.

As ports adapt to decarbonisation, digitalisation, and changing operational pressures, the demands on the workforce are evolving rapidly. New technologies require new competencies, while traditional skills remain essential. At the same time, the sector faces ongoing challenges around recruitment, retention, and succession planning.

Meeting these challenges requires a more strategic and coordinated approach to workforce development.

Early career pathways are a critical starting point. Apprenticeships, graduate schemes, and outreach programmes all play a role in attracting new talent into an industry that remains relatively unknown to many. Without sustained effort in this

area, there is a risk that future workforce needs will not be met.

At the other end of the spectrum, experienced workers need opportunities to upskill and reskill. Short courses and specialist training are valuable, but their impact is limited when provision is fragmented. When individual ports engage in isolation, it becomes difficult to sustain high-quality, cost-effective training, and opportunities for benchmarking and standardisation are lost.

This fragmentation also affects career progression. Without clear, recognised pathways, it is harder for individuals to understand how to develop within the sector, and for employers to assess competence consistently.

Standardisation offers a way forward, and PSS, as the sector body for skills standards, is working to establish clearer sector-wide expectations around qualifications, training and competence, providing a shared framework that supports safety, mobility and credibility.

Middle managers represent a particularly important focus. Often promoted based on technical expertise, they are expected to lead teams, shape culture, and manage risk, sometimes without formal development in these areas. Targeted support for this group can have a strong impact across the organisation, strengthening both safety outcomes and workforce engagement.

The Importance of Data Sharing and Collaboration

A recurring challenge across both safety and skills is the availability of sector-wide data. Ports hold valuable information on workforce composition, training, and capability, yet this is rarely aggregated in a way that provides a comprehensive picture. As a result, it is difficult to identify trends, forecast skills gaps, or make the case for targeted interventions.

Improving this position requires collective action. Individual organisations may have understandable concerns about sharing data, but anonymised, aggregated information can deliver significant benefits for the sector as a whole. It enables better decision-making, supports engagement with government and regulators, and strengthens the case for investment.

By working together, ports can share learning, align approaches, and accelerate progress. This is particularly important in areas such as training, where scale and consistency are critical to effectiveness.

From Intention to Implementation

Across all of these themes, a common thread emerges: the need to move from isolation to collaboration. By working together, through organisations such as PSS, insight at the individual organisational level can be translated into sustained improvement across the sector.

This requires clarity of purpose and consistency of effort. Change does not happen overnight, and it is rarely linear. Setting realistic goals, measuring progress, and maintaining focus over time are all essential.

It also requires honesty. Creating a safer tomorrow means asking difficult questions about why incidents occur, why certain behaviours persist and where gaps remain. It means being willing to challenge internal assumptions and confront uncomfortable truths.

Crucially, it requires engagement at every level. Leadership sets direction and provides resources, but culture is lived day-to-day by the entire workforce. Empowering individuals to take responsibility for their own safety and for others is fundamental.

Psychological safety plays a key role here. When people feel able to speak up, share concerns, and contribute ideas without fear, organisations are better equipped to learn and adapt. This is particularly important in complex, high-risk environments like ports, where conditions can change rapidly and unpredictably.

A Collective Journey

While safety has improved over time, no port claims to have "solved" safety. Each organisation is on its own journey, shaped by its context, challenges, and opportunities. What matters is not the starting point, but the direction of travel and the commitment to continuous improvement.

A safer tomorrow will not be delivered by any single initiative or intervention. It will emerge from the combined effect of many actions: strengthening culture, investing in people, using data intelligently, and embracing collaboration.

Technology will continue to evolve, and operational pressures will continue to change. But the fundamentals remain constant. Safe operations depend on capable people, supported by effective systems, working within a culture that prioritises doing the right thing.

For the port sector, the opportunity is clear. By bringing together expertise in safety, skills and collaboration, it is possible to build a more proactive, resilient and forward-looking approach, one that not only prevents harm but actively creates the conditions for success.

The vision of a safer tomorrow is within reach. The challenge now is to make it real through the choices we make today and the actions we sustain over time.

About the author

Debbie Cavaldoro is the Chief Executive Officer at Port Skills and Safety Ltd (PSS). Coming from a membership communications background, she moved into the maritime sector in 2008.

Debbie joined PSS in 2021 and has seen the organisation go from strength to strength. She has a Master's in Economics, Governance and Public Policy, is a champion for diversity in maritime and is a charity trustee for three other charities.

About the company

Port Skills and Safety Ltd is the professional safety and skills membership organisation for ports. We work in collaboration with our members to promote best practice and innovation, develop guidance and deliver services that drive continuous improvement in safety and ensure a highly skilled workforce.



Fatal Risk at the Port-Ship Interface:

Learning from 25 Years of Cargo Handling Fatalities

**ICHCA**
INTERNATIONAL

Richard Steele,
CEO, ICHCA

For all the technological progress seen across ports and terminals over recent decades, one challenge continues to resist easy resolution: the persistent risk of fatal accidents in cargo handling.

Automation, digital planning tools and increasingly sophisticated operating systems have transformed the way terminals operate, yet the fundamental hazards remain remarkably familiar. Heavy

loads still need to be moved. Vehicles continue to share space with pedestrians. Workers may enter enclosed spaces, work at height and operate at the water's edge.

Evidence gathered by ICHCA International suggests that, despite decades of learning and an enduring commitment to safety, the industry continues to confront patterns of fatal incidents that are both recognisable and preventable.

Perhaps the most striking lesson is that the greatest risks are not hidden within exceptional circumstances. They are embedded within normal work. They arise while loading cargo, maintaining equipment, conducting inspections and moving vehicles. In other words, the work that ports and terminals exist to perform also creates the conditions in which their most serious risks emerge.

“Safety should never depend solely upon people remembering not to make mistakes.”

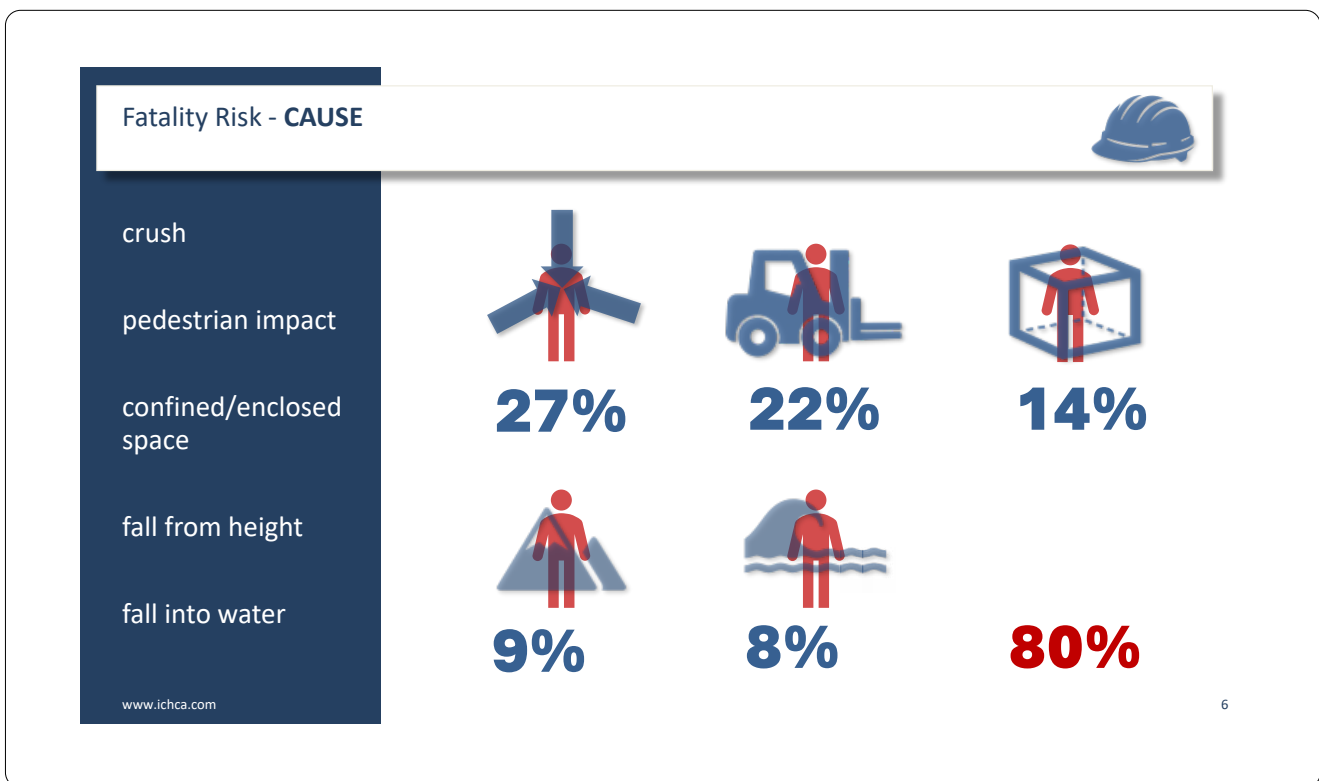


Figure 1: The five dominant fatal risk categories

That reality places an important responsibility on leaders. Safety cannot be something separate from operations. It must be integral to the way operations are planned, managed and executed. Ultimately, the objective is simple: that no one is harmed in the course of cargo handling operations.

Why ICHCA Analysed 25 Years of Fatality Data

As an independent, not-for-profit association dedicated to improving the safety, productivity and efficiency of global cargo handling and movement, ICHCA has long sought to understand the causes of the most serious accidents affecting port workers and seafarers.

To support this objective, ICHCA has developed and maintained a database of fatal accidents occurring in ports and terminals around the world. Covering the period from 2000 to 2025, the dataset now includes more than 1,100 incidents involving almost 1,700 casualties.

No single global source exists for fatal accident data in ports and terminals. Information is dispersed across accident investigation reports, regulatory

publications and other publicly available sources. The purpose of the analysis is not to calculate precise industry fatality rates, but to identify recurring patterns and understand where efforts to prevent future tragedies should be concentrated.

The value of the dataset lies not in perfect completeness, but in the consistency of the messages emerging from a quarter of a century of experience.

Familiar Hazards Continue to Dominate

One of the clearest findings is that fatal accidents involving port workers are highly concentrated around a relatively small number of hazards.

Five risks account for approximately 80 per cent of all port worker fatalities recorded within the database. Crush by cargo remains the largest category, accounting for 27 per cent of fatalities. Vehicle-pedestrian interaction represents 22 per cent, while confined and enclosed spaces account for 14 per cent. Falls from height and falls into water contribute a further nine per cent and eight per cent respectively.

These are not obscure hazards. They sit at the centre of everyday port operations.

They have been recognised for decades and are supported by extensive guidance, procedures and training.

The challenge, therefore, is not discovering new risks. It is ensuring that the controls designed to manage them remain effective under the realities of day-to-day operations.

Too often, discussions following serious incidents have focused on what workers should have done differently. Yet 25 years of evidence suggests that the answer to fatality prevention does not lie in asking people to be more careful. It lies in creating the conditions in which safe work becomes the natural outcome. Workers should not be expected to compensate for weaknesses in systems or controls through vigilance alone.

The question leaders should ask is not simply whether controls exist on paper, but whether they remain effective in practice. In short, leaders need to understand the gap between work as imagined and work as done.

Normal Work Creates Normal Risk

The data also reveal that fatal accidents are overwhelmingly associated with routine activities.

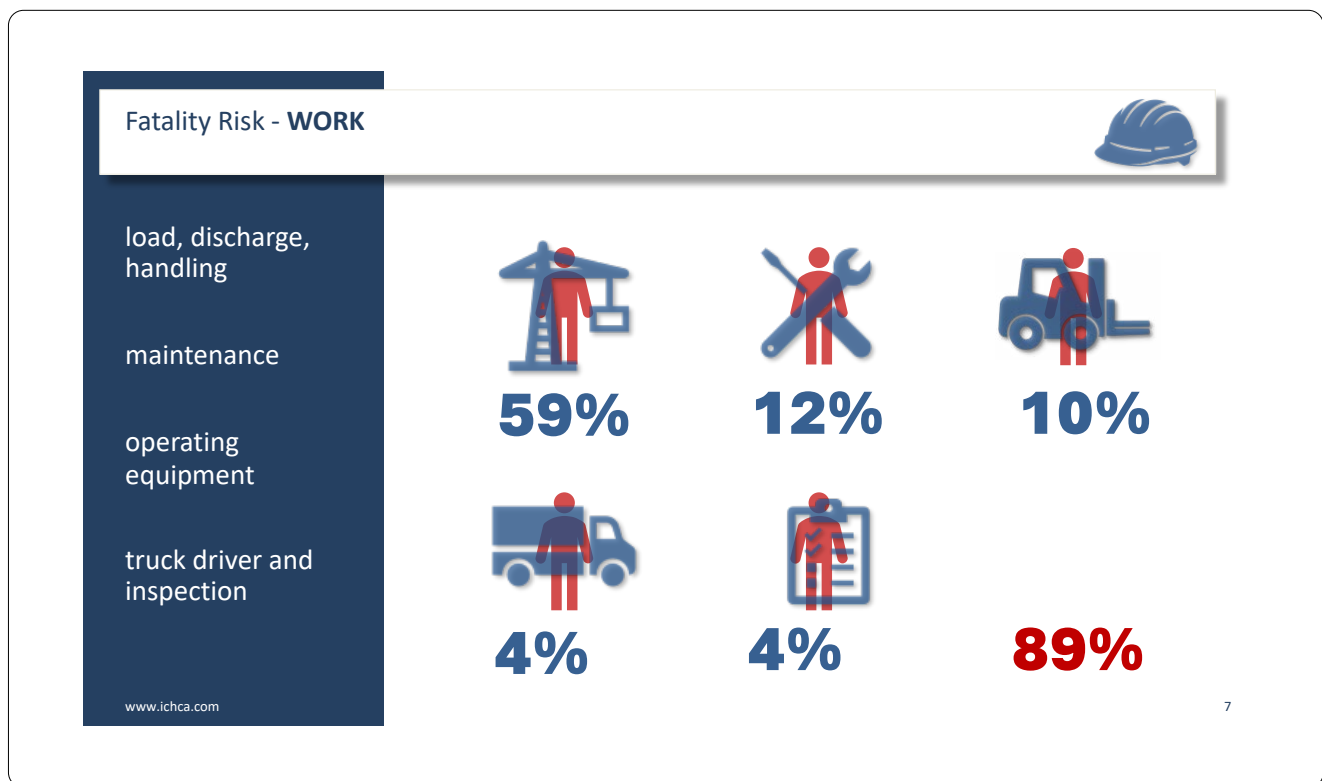


Figure 2: Activities being undertaken

Loading, discharge and cargo handling account for almost 60 per cent of workplace fatalities in the industry. Maintenance activities contribute a further 12 per cent, while equipment operation accounts for 10 per cent. Together, these activities represent almost 90 per cent of fatal events in port work.

These findings are significant because they challenge the notion that fatal accidents arise primarily from unusual situations. The opposite is true. Severe risks are embedded within normal work carried out every day by experienced people.

Cargo handling inevitably brings together people, vehicles, machinery, suspended loads and changing conditions. Maintenance and inspection activities introduce additional exposures, potentially at times when safeguards may be weakened or equipment partially isolated.

Operational pressures, changing circumstances and normal human variability are realities of port work. Effective organisations recognise these realities and design systems that are resilient to them rather than assuming perfect compliance.

The purpose of investigating fatalities should therefore not be to understand how people failed, but to understand how systems failed to protect people.

One Operating Environment

Another important finding is the almost even split between port worker fatalities occurring ashore and those occurring aboard vessels.

Fifty-three per cent of port work fatalities occur on shore and 47 per cent on the ship side of operations. This balance provides an important reminder that the port–ship interface should not be viewed as separate domains.

Workers experience terminals, quays and vessels as one continuous operating environment. Historically, some of the most serious incidents have occurred not neatly within one organisation's area of responsibility, but in the spaces between responsibilities.

Hazards do not recognise organisational boundaries, and neither should the measures designed to control them.

This is why collaboration across terminal operators, shipowners, workforces, contractors and regulators is so important. Shared risks require shared ownership.

Where Fatal Risks Concentrate

The analysis also helps identify where attention should be focused.

Container cargo accounts for 34 per cent of fatalities, followed by bulk cargo at 23 per cent and breakbulk cargo at 14 per cent. More than half of all fatalities are associated with container, bulk and breakbulk handling activities.

Quays account for 19 per cent of fatalities, followed by ship holds at 17 per cent and terminal areas at 16 per cent. These are environments where moving equipment, suspended loads, changing cargo configurations, restricted visibility and proximity to the water's edge combine to create particularly demanding conditions.

These findings should not be interpreted as evidence that any one cargo sector or location is inherently unsafe. Rather, they help identify where critical controls deserve the greatest attention.

From Data to Action

The value of analysing fatal accidents lies in preventing tragedies, not in counting them.

Data, dashboards and statistics do not make people safer in themselves. Their importance lies in the decisions they inform and the actions they encourage. 25 years

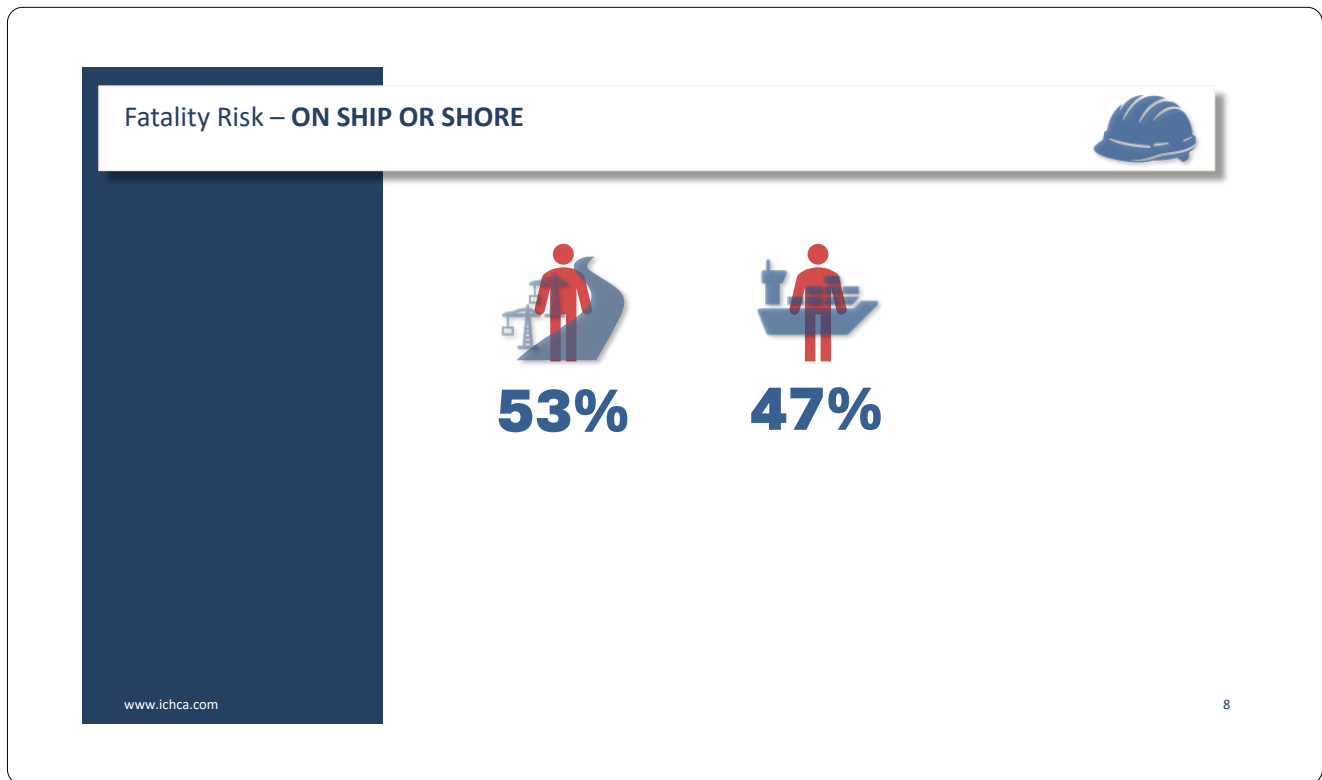


Figure 3: Ship versus shore

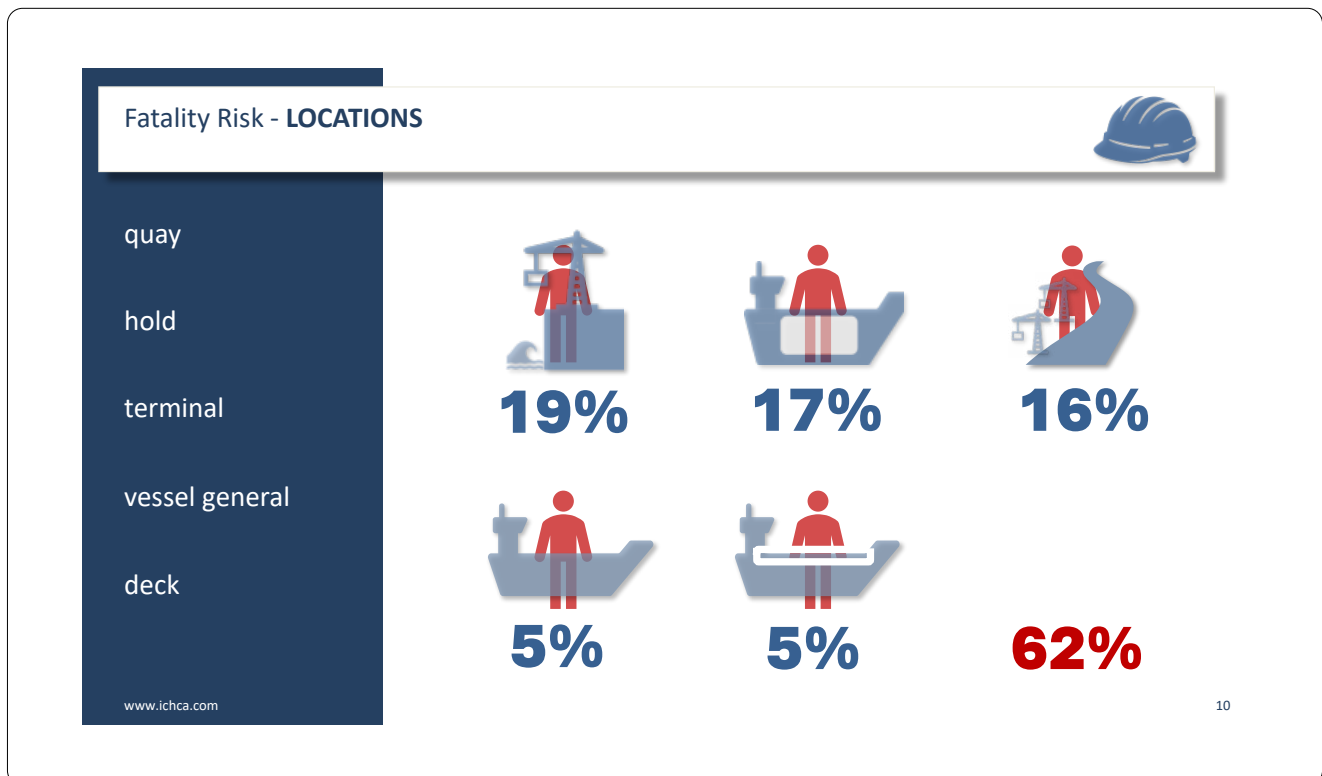


Figure 4: Where fatalities occur

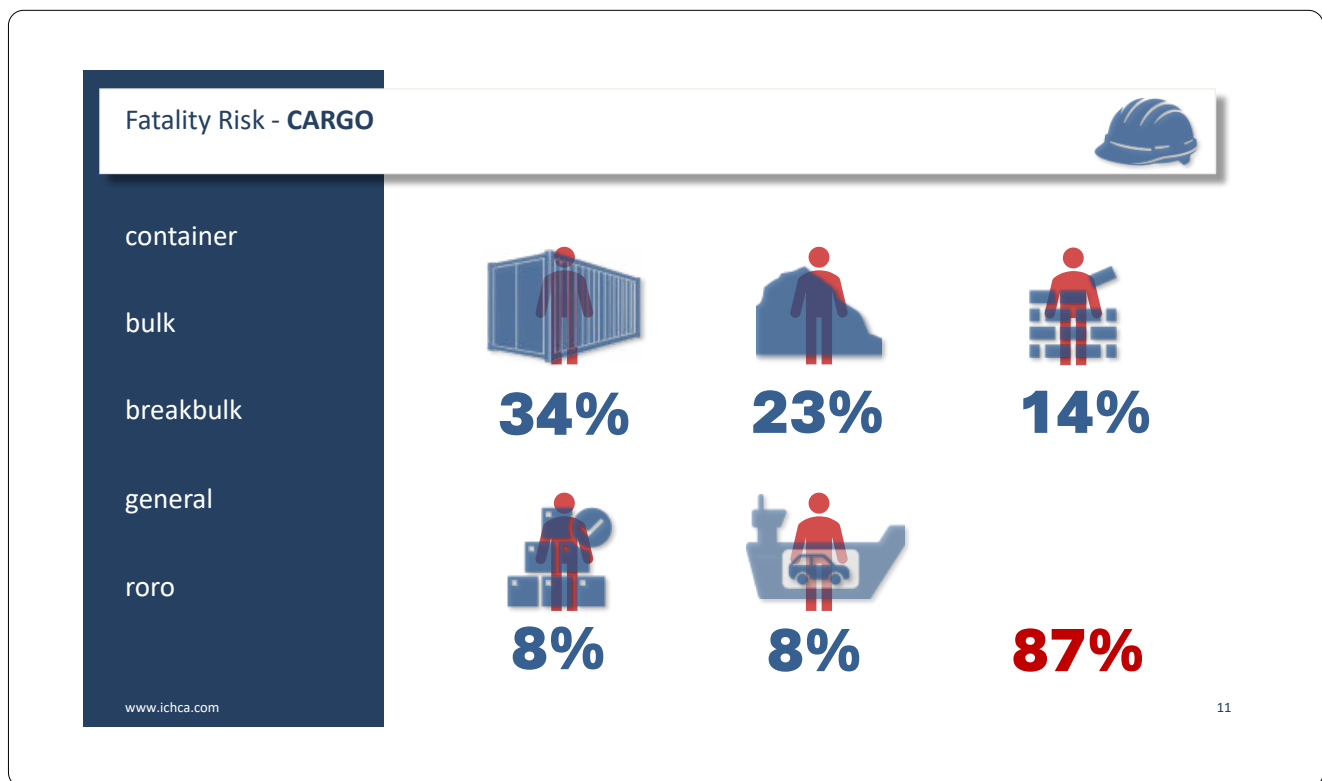


Figure 5: Cargo sectors

of evidence provide an opportunity to focus attention on the hazards that matter most and to strengthen the critical controls that stand between people and catastrophic outcomes.

Importantly, the objective of understanding severe risk is to learn, not to allocate blame. Every fatal accident represents a personal tragedy, and we owe it to those affected to better understand how systems, processes and organisational arrangements can be strengthened.

The consistency of the patterns identified by ICHCA should give the industry confidence. The challenge facing ports and terminals is not one of discovering unknown hazards, but of sustaining the leadership, collaboration and discipline required to manage known risks effectively.

In the end, this data should serve a single purpose: to reduce exposure to risk and strengthen the controls that protect people in everyday operations.

Leadership, Culture and Critical Controls

Perhaps the most important lesson emerging from 25 years of evidence is that compliance alone is not enough. Most

organisations involved in fatal accidents have procedures, training programmes and management systems. The persistence of the same hazards over a quarter of a century suggests that preventing fatalities requires more than rules. It requires a deeper understanding of the critical controls that stand between people and catastrophic outcomes, and a commitment to ensuring those controls remain effective under real operating conditions.

The hierarchy of controls provides an essential framework. Wherever possible, organisations should seek to eliminate hazards, introduce engineering solutions and design safer systems before relying solely on procedures, warnings and individual behaviour. Effective separation of pedestrians and vehicles, exclusion from crush zones, improved access arrangements and engineered safeguards all reduce reliance on human perfection.

Safety should never depend solely upon people remembering not to make mistakes.

Creating safer ports and terminals is fundamentally a leadership challenge. Leadership, however, should not be confined to management positions. Genuine safety culture exists when people at every level are encouraged and

empowered to participate actively in their own safety and the safety of those around them. In such environments, everyone becomes a safety leader.

Importantly, this does not mean transferring responsibility from organisations to individuals. Quite the opposite. Leaders create the conditions in which proactive participation becomes possible. They encourage speaking up, support learning, value operational experience, and create trust rather than fear.

People are an essential part of the solution and should be engaged, not treated as a problem to be controlled. The strongest cultures are characterised not by blame, but by curiosity and continuous improvement. The purpose of learning from fatal accidents is not to understand how people failed, but to understand how systems, processes and organisational arrangements failed to protect them.

Every incident represents an opportunity for the wider industry to strengthen its understanding of severe risk and improve the safeguards designed to prevent future harm.

Learning should not stop at organisational boundaries. Better sharing of information, lessons learned, and examples

of effective practice can help ensure that known failures are not repeated elsewhere. Fatality prevention is ultimately a collective endeavour, requiring leadership, trust and collaboration across the entire port and maritime logistics chain.

Looking Forward

There are good reasons for optimism.

The patterns are visible. The principal hazards are known. The high-risk activities and locations are identifiable. Arguably, few industries possess such clarity about the mechanisms responsible for their most serious outcomes.

The challenge is not discovering what needs to be done. It is sustaining the leadership, collaboration and commitment necessary to do it consistently.

25 years of evidence point to a simple truth. The measure of success for ports and terminals is not just how much cargo is successfully moved, but whether everyone involved in cargo handling returns home safely at the end of every shift.

If the industry continues to strengthen critical controls, embrace learning and foster a culture in which everyone plays an active role in safety, there is every reason to believe that the next 25 years can be safer than the last.

About the author

Richard Steele is Chief Executive Officer at the International Cargo Handling and Coordination Association – ICHCA. Reporting directly to the Board, Richard leads the organisation, which provides a focal point to improve cargo handling health and safety throughout international supply chains. ICHCA also represents members and the cargo handling industry, as a recognised non-government organisation at international bodies such as the International Maritime Organisation, UNECE and other agencies and regulatory bodies.

About the association

Established in 1952, ICHCA International is an independent, not-for-profit organisation dedicated to improving the safety, productivity and efficiency of cargo handling and movement worldwide. ICHCA's privileged NGO status enables it to represent its members and the cargo handling industry at large in front of national and international agencies and regulatory bodies, while its Technical Panel provides best practice advice and develops publications on a wide range of practical cargo handling issues.

Operating through a series of national and regional chapters, including ICHCA Australia, ICHCA Japan and Correspondence and Working Groups, ICHCA provides a focal point for informing, educating, lobbying and networking to improve knowledge and best practice across the cargo handling chain.

Disclaimer

This publication has been prepared using information available at the time of publication and is provided for general guidance only. It is intended to support the sharing of safety knowledge and industry good practice within the cargo handling and logistics sectors.

The information does not constitute professional, technical or legal advice and should not be relied upon as such. Users are responsible for assessing the suitability of the information for their particular circumstances and for ensuring compliance with all applicable laws, regulations, standards and codes of practice.

While reasonable efforts have been made to ensure the accuracy of the information, it is provided without warranty of any kind. To the fullest extent permitted by law, ICHCA International and the authors accept no liability for any loss or damage arising from reliance on the information contained in this publication.

Further Advice and Information

Contact secretariat@ichca.com for further information or visit the website www.ichca.com. ICHCA International Ltd Registered address: 57 Spyvee Street, Hull, E. Yorks, England, HU8 7JJ. Company number 04450611 - Incorporated on 29 May 2002.

ICHCA International also offers a technical advisory service, with input from the ICHCA Technical Panel, to answer member regulatory and operational cargo handling queries. For more information, contact secretariat@ichca.com or visit www.ichca.com



Connecting Minds: How Collaboration is Strengthening Safety Across the Port Industry




Beatrice Björk, CEO, sfPORTEQ,
Neil Dalus, Risk Assessment
Manager, TT Club
Supported by **Pat O'Leary**,
Head of Technology, PEMA

The saying "if you have seen one port, you have seen one port" reflects the unique nature of every terminal operation. Different layouts, equipment fleets, cargo profiles and operating environments create distinct challenges from one facility to another.

Despite these differences, there is remarkable consistency in how container terminals operate. PEMA, as the global representative body for port equipment

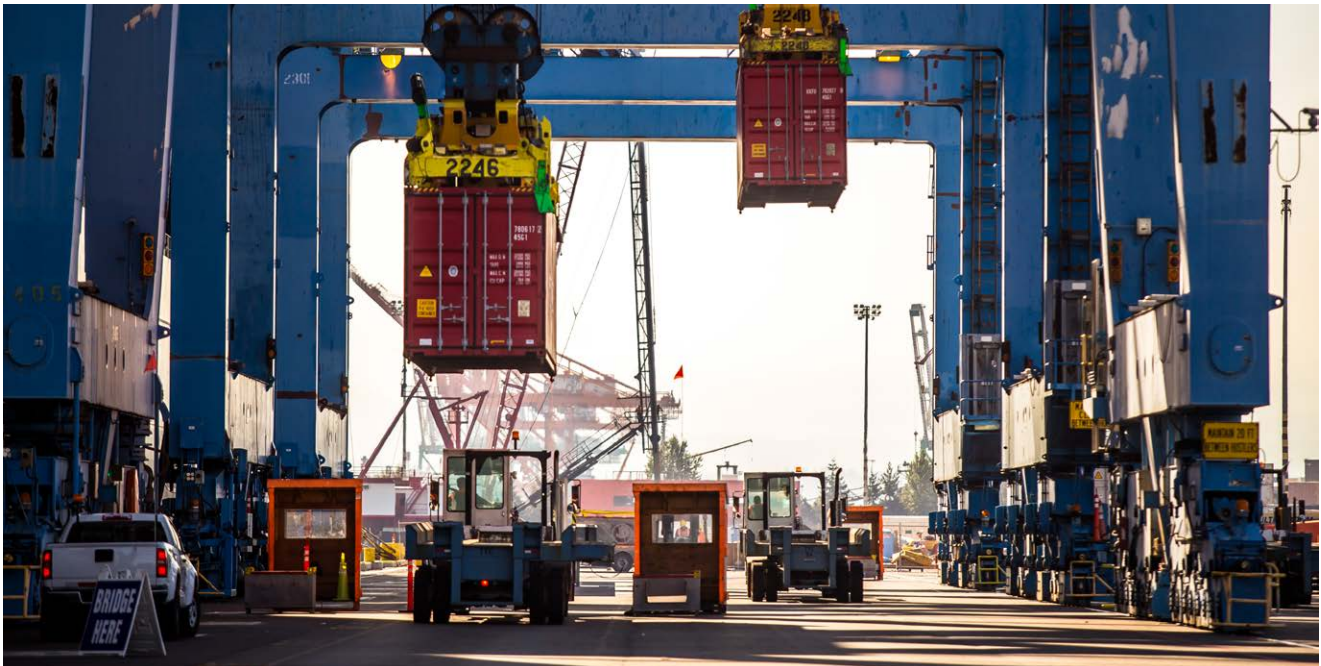
manufacturers, is an integral stakeholder directly involved in global activities where cranes load and discharge containers, terminal vehicles move cargo through busy operational areas, and workers interact with increasingly sophisticated equipment and systems. It also plays an active role in supporting overall operational safety. The operational rhythm may vary, but the fundamental processes

remain strikingly similar.

Unfortunately, so do many of the incidents that affect safety and performance.

Collisions between equipment, contact with infrastructure, cargo-handling errors, and personnel exposure to operational hazards continue to occur across the industry. These are rarely unexpected events. Rather, they are recurring challenges within a complex operating environment

"Improving safety and operational performance requires a more holistic understanding of how people, equipment and systems interact."



where people, equipment and processes must work together safely and efficiently.

Learning from Experience

The port industry is rich in operational experience. Decades of cargo-handling activity have generated valuable insights into how incidents occur and, more importantly, how they can be prevented.

Analysis of insurance claims and operational incident data consistently reveals familiar patterns. Most losses arise not from unknown hazards, but from recurring interactions among equipment, people and operational processes. Environmental factors such as severe weather may contribute to outcomes, but they often expose existing vulnerabilities rather than create entirely new risks.

The challenge facing the industry is therefore not a lack of knowledge. It is ensuring that lessons learned in one organisation, terminal or region are shared broadly enough to benefit the wider industry.

The Value of Collaboration

Ports and terminals operate at the intersection of numerous stakeholders. Equipment manufacturers, terminal operators, technology providers, insurers and regulators each develop a detailed understanding of operational risk from their own perspective.

Historically, much of this knowledge remained within organisational boundaries. Valuable lessons were learned, but they were not always transferred effectively across the wider industry.

As terminals become more connected and technologically sophisticated, this approach becomes increasingly limiting. Improving safety and operational performance requires a more holistic understanding of how people, equipment and systems interact.

This is where industry collaboration plays a critical role.

PEMA's Role in Connecting Expertise

The Port Equipment Manufacturers Association (PEMA) provides a platform for equipment manufacturers, technology specialists and industry experts to collaborate on shared challenges.

By bringing together diverse expertise, PEMA helps create opportunities for knowledge exchange that might not otherwise occur. Technical insights from manufacturers can be considered alongside operational experience from terminal environments and lessons derived from incident analysis.

This collaborative approach helps develop a more complete understanding of industry risks and supports the identification of practical solutions

applicable across different operating environments.

Much like the global supply chain itself, progress is built on relationships, communication and trust. The ability to share experience openly and constructively is increasingly important in helping the industry address common challenges.

A Broader View of Safety

Safety is no longer viewed solely through the lens of procedures, training and compliance, important though these remain.

Today's discussions increasingly focus on the interactions between people, equipment and digital systems. Questions are being asked not only about whether equipment functions correctly, but also about how effectively operators understand machine behaviour, how systems communicate information and how technology supports safe decision-making.

This systems-based perspective reflects the growing complexity of modern terminals, where automation, digitalisation and operational efficiency must coexist with the realities of a busy working environment.

Accelerating Industry Learning

Physical infrastructure changes slowly. Equipment investments are measured in decades, and operational changes must be carefully managed to avoid disruption.



Knowledge, however, can move much faster.

When organisations share experiences, successful practices can be adopted more rapidly and common mistakes avoided. Collaboration enables the industry to learn collectively, reducing uncertainty and supporting more informed decision-making.

This ability to transfer knowledge across organisational and geographical boundaries may be one of the most powerful tools available for improving safety and operational performance.

Looking Ahead

As container terminals continue to evolve, the need for shared understanding will only increase. The integration of advanced equipment, automation and digital systems creates new opportunities, but also new interfaces that must be understood and managed effectively.

No single organisation possesses a complete view of this increasingly complex ecosystem. Building that understanding requires collaboration across disciplines, companies and regions.

Through initiatives that connect expertise and encourage knowledge sharing, organisations such as PEMA are helping to create a stronger foundation for the future of port operations.

The most significant advances in safety rarely come from a single breakthrough. More often, they emerge from the collective application of knowledge, experience and continuous improvement.

In an industry built on coordination, connecting minds may be one of the most important ways to create safer, more resilient and more efficient terminals.

The Port Equipment Manufacturers Association (PEMA) is a non-profit organisation that has 127 members and five associate members, 22 years after its founding.

Hosting in-person events worldwide, with recent events held in Gdańsk, Antwerp, Ravenna, Hamburg, Kuala Lumpur, Dubai and Miami, members can take part in two days of conferences, port tours, technical workshops, guest speaker presentations, networking and more. While the benefits of PEMA's two annual events are highly sought after, members also have exclusive access to online resources, including market surveys, information and white papers, annual reports and other meeting papers, which span more than 20 years of the association's existence.

PEMA's members range from companies involved in the design, manufacture and supply of port equipment and technology, including port and terminal equipment, components or attachments for port equipment, technology that controls or interfaces with port equipment, and consultants in port and terminal equipment design, specification and operations.

Learn more about becoming a PEMA member at pema.org.

About the authors

Beatrice Björk is a Partner at SF PortEQ with more than 20 years of international experience across heavy-duty industries. Her background includes roles as a management consultant, investor, CEO, and board advisor. She has extensive experience supporting organisations through business transformation, automation, and operational excellence, with a particular focus on optimising the interaction between people, technology, and machines in complex industrial environments.

Neil is a Risk Assessment Manager for TT Club's Loss Prevention Team. Neil joined TT Club in 2023 and has extensive experience managing port and port-related infrastructure and assets, having more than 20 years of engineering experience, which includes local authority, consultancy and 11 years in the port industry in various technical and engineering leadership roles.

Pat O'Leary is PEMA's Head of Technology, where he supports and

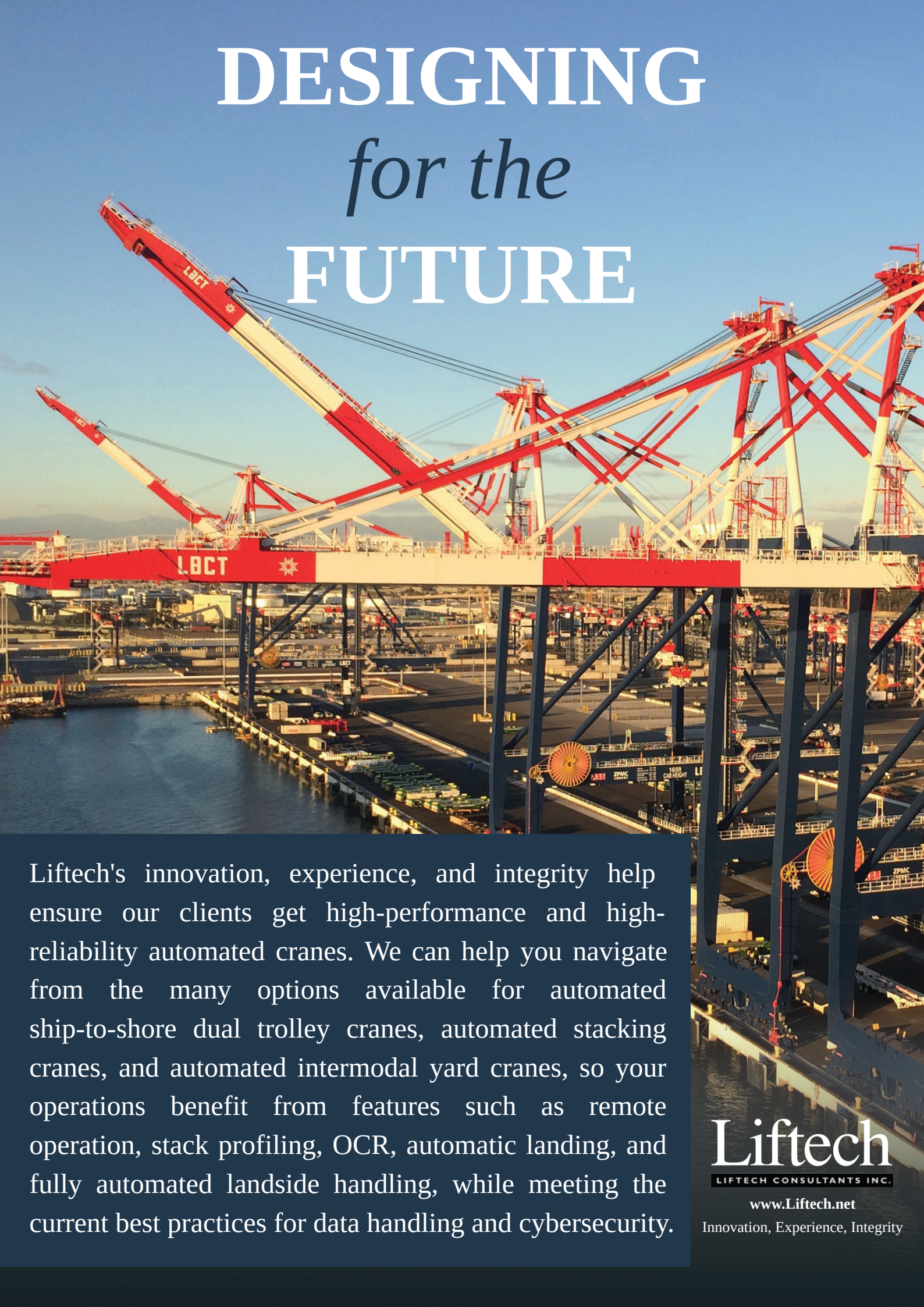
coordinates the Association's four technical committees: Safety & Environment, Automation & Control Technologies, Equipment Design & Infrastructure, and Port Bulk Handling. Working closely with committee chairs and members, Pat brings extensive industry experience to help drive technical collaboration, share best practices, and support innovation across the global port equipment sector.

About the association

The Port Equipment Manufacturers Association (PEMA) is a non-profit industry association representing 127 members and five associate members worldwide. PEMA connects professionals through global conferences, technical workshops, networking, and exclusive online resources. Its membership includes leading companies specialising in port equipment, technology, components, and consultancy for port and terminal operations.



Cargo Integrity and Control



DESIGNING *for the* FUTURE

Liftech's innovation, experience, and integrity help ensure our clients get high-performance and high-reliability automated cranes. We can help you navigate from the many options available for automated ship-to-shore dual trolley cranes, automated stacking cranes, and automated intermodal yard cranes, so your operations benefit from features such as remote operation, stack profiling, OCR, automatic landing, and fully automated landside handling, while meeting the current best practices for data handling and cybersecurity.

Liftech
LIFTECH CONSULTANTS INC.

www.Liftech.net

Innovation, Experience, Integrity



Verified Data for Hazardous Cargo Risk Management:

Supporting Safer
Declaration Checks
and Operational
Decisions



Bertrand Chen,
CEO, GSBN

“Coordination will depend on the ability of participants to rely on the same set of facts, established at source and shared with confidence.”



In February 2022, a car carrier named *Felicity Ace* caught fire in the Atlantic. What followed was not just a safety incident, but a total loss. The vessel sank with an estimated \$155 million worth of cargo for car manufacturers. Three years later, in June 2025, the *Morning Midas* saw a fire break out mid-voyage, forcing its crew to abandon ship.

The common factor in both incidents was lithium batteries. Both incidents escalated rapidly beyond the capacity of onboard firefighting systems. Both also highlighted a deeper issue that continues to challenge the maritime industry.

The safe transport of hazardous goods has long depended on accurate declarations submitted at the start of a shipment's journey. That model is under strain. With demand for consumer electronics, electric vehicles and energy storage accelerating, the lithium battery market is expected to grow by more than 30 per cent annually through 2030. As volumes rise, so does risk exposure, placing increasing pressure on a system that relies on the accuracy of what is declared.

Reducing misdeclaration requires a shift in approach. It calls for moving from self-declared cargo information towards certification data that is verified at source and shared across the supply chain in a way that is consistent, traceable and usable.

Rising Risks of Misdeclaration

Lithium batteries are now embedded across modern trade flows. They power consumer electronics, electric vehicles and energy storage systems, and they are increasingly shipped in different forms, including new, used, damaged and end-of-life units. Each category presents a different risk profile, but these distinctions are not always clearly reflected in shipping documentation.

When lithium batteries are exposed to thermal stress, mechanical damage or improper handling, they can trigger a chain reaction that leads to thermal runaway. Once initiated, these fires are difficult to contain and can spread rapidly across a vessel, releasing toxic gases that are dangerous to the crew.

As volumes grow, the variability and uncertainty associated with these shipments grow alongside them. This places increasing pressure on existing processes, particularly those that rely on the accuracy of information provided at the point of declaration, which cannot fully mitigate the risks associated with improper handling.

Misdeclaration sits at the centre of this challenge. In some cases, it reflects a lack of clarity or understanding. In others, it arises from fragmented processes or inconsistent standards across jurisdictions. Regardless of the cause,

the result is the same. Hazardous cargo moves through the supply chain without being fully recognised or managed according to its risk.

Fragmented Data Flows Limit Verification at Scale

Despite ongoing digitisation efforts, the management of hazardous goods remains heavily dependent on manual workflows. Cargo declarations are often supported by documentation that exists in static formats, which limits the ability of downstream stakeholders to verify or reconcile information in real time.

The structure of data exchange contributes to this limitation. Information is typically shared between adjacent parties, with each participant holding a partial view. There is no shared layer that enables consistent validation of data across the entire chain. As a result, discrepancies can persist undetected across multiple handovers.

Verification itself is also constrained. Certificates may be submitted as part of the booking process, but confirming their authenticity or relevance often requires manual review. At scale, this becomes impractical. It introduces delays, increases operational burden and creates opportunities for errors to pass through unnoticed.

A further challenge lies in how emerging cargo types are governed. Existing guidelines for used, damaged, defective

or waste batteries often lack explicit or operationally realistic parameters. This makes it difficult to apply them consistently across different stakeholders and environments, particularly when conditions such as temperature and cargo handling vary widely in practice.

These limitations highlight a deeper issue in the system, where information is distributed but not aligned. As a result, key participants depend on processes originally designed for a far less complex environment than the reality we face today.

Redefining Risk Management in Practice

To address the shortcomings of current processes, the industry has long recognised the need for more consistent and universal protocols for the handling of hazardous cargo. That need has become more apparent as the risk profile of shipments evolves. Despite this broad acknowledgement, universal standards have not fully materialised in practice. Instead, different organisations have introduced their own approaches to monitoring and governing temperature-sensitive cargo.

These efforts reflect a necessary shift in mindset, but they also introduce new complexities. Variations in how protocols are defined, applied and enforced can lead to inconsistent handling across the supply chain. In environments where temperature fluctuations can significantly affect cargo stability, these inconsistencies can

themselves become a source of risk. What is intended to improve safety can, in certain conditions, create gaps in how that safety is maintained from origin to destination.

The problem is not merely that the rules differ. It is that different parties across the supply chain may view the same cargo in very different ways. The challenge is the absence of a common and reliable way to interpret and act on the available information.

Safe Transport Certificates play an important role in this context. They are designed to confirm that hazardous cargo meets the required safety conditions for transport. In theory, they provide assurance that the necessary testing and compliance checks have been completed. In practice, however, they are often embedded in a document-based workflow. Certificates are issued, transferred and reviewed as static files, which limits their ability to inform decisions beyond initial submission. Questions around authenticity, completeness and relevance are not always easy to resolve, particularly at scale.

An emerging direction is the move towards enriched certification. This involves expanding the scope beyond a simple pass or fail outcome. Instead, it can be structured as a set of data attributes that provide a more detailed view of the cargo. For lithium batteries, this may include information on condition, classification and compliance with relevant standards, as well as technical indicators that influence risk. Crucially,

enriched certification links this information directly to the underlying test data and the issuing laboratory. It allows certification to reflect the actual state of the cargo, rather than serving as a detached layer of documentation.

When certification is both enriched and structured, it becomes more than a record. It gives carriers, terminals and regulators information they can actually use, rather than simply a record to file away. Carriers can reference it during the booking process. Terminals can use it to guide handling and storage. Regulators can rely on it for audit and oversight.

Verify at Source

To support this shift, attention has turned towards how certification data is created and shared. One area of development involves connecting carriers more directly with accredited testing laboratories through a shared digital infrastructure, an approach that is beginning to take shape through GSBN's blockchain-enabled platform and its ongoing collaboration with a network of laboratories accredited by the China National Accreditation Service for Conformity Assessment (CNAS).

This enables certification to be issued at source and accessed downstream in a consistent format.

In practical terms, this model changes how information flows. Traditionally, a shipper would obtain a certificate, attach

it to booking documentation and submit it through multiple intermediaries. Each party would review the information independently, often relying on manual checks and limited context. This creates duplication of effort and introduces the possibility of errors or inconsistencies going undetected.

By contrast, when certification data is retrieved directly from the issuing laboratory, it carries a clearer point of reference. Its origin is known, its content is structured, and its integrity can be maintained across systems. Collaboration with accredited laboratories, including those recognised under the China National Accreditation Service for Conformity Assessment, has begun to demonstrate how such a model can work in practice. By linking to a network of these laboratories, carriers can access certification data that is more consistent and easier to validate, without relying on repeated document submission.

The impact of this shift is not limited to efficiency. It supports a more reliable understanding of cargo risk, grounded in information that can be traced back to its source.

Rethinking Trust at Scale

Looking ahead, this direction can be extended further through the concept of a certification pool.

A certification pool is a shared repository of validated certification data contributed by accredited laboratories. In this model, laboratories issue and maintain certification data within a common framework. Carriers and stakeholders access that data as needed, rather than managing individual certificates independently for each shipment. The focus moves from handling documents to interacting with a shared dataset.

Such an approach introduces several advantages. It reduces duplication by eliminating the need to repeatedly submit and verify the same information. It improves consistency by ensuring that all participants refer to a common set of data. It also enhances traceability, as certification can be linked back to its origin and maintained throughout the lifecycle of a shipment.

For laboratories, it provides a way to extend the reach of their assessments beyond the point of issuance. For carriers, it offers access to certification data that is more readily available and easier to interpret.

For the wider ecosystem, it creates the conditions for aligning how risk is evaluated across different stages of the supply chain.

At its core, this represents a shift in how the industry approaches trust. Instead of depending on the transfer of documents between parties, it depends on the ability of participants to access and rely on information that has already been established and validated at source.

Implications for Ports and Terminals

For ports and terminals, access to verified and structured cargo data changes the way operations can be planned and executed.

Greater clarity on the nature of incoming cargo allows decisions to be made earlier. Storage and handling requirements can be aligned more closely with the actual risk profile of the cargo. This reduces the likelihood of incompatible goods being placed together and supports safer yard operations.

The availability of reliable data also plays a role in incident response. When information on cargo characteristics can be accessed quickly and with confidence, it can inform how a situation is assessed and managed. This becomes particularly important in cases where conditions escalate rapidly.

There is also a broader impact on compliance and reporting. Verified data creates a clearer record of what has been transported and under what conditions, supporting both regulatory oversight and internal risk management.

The result is a shift from operating with partial and sometimes inconsistent information to operating with a more complete view of cargo risk.

Data Transition: An Industry Imperative

The risks associated with hazardous cargo are unlikely to diminish, particularly as demand for lithium batteries continues to grow. What can change is how those risks are understood and managed.

Improving outcomes will depend on the ability of the industry to work with information that is accurate, consistent and available where it is needed. This requires more than incremental improvements. It requires alignment on how data is created, validated and shared across the supply chain.

The transition towards verified and shareable data provides a foundation for this shift. It enables earlier identification of risk, clearer accountability and more consistent decision-making.

Progress will depend on coordination across stakeholders, as well as continued development of the infrastructure that supports trusted data exchange.

The movement of goods has always depended on coordination. Increasingly, coordination will depend on the ability of participants to rely on the same set of facts, established at source and shared with confidence.

About the author

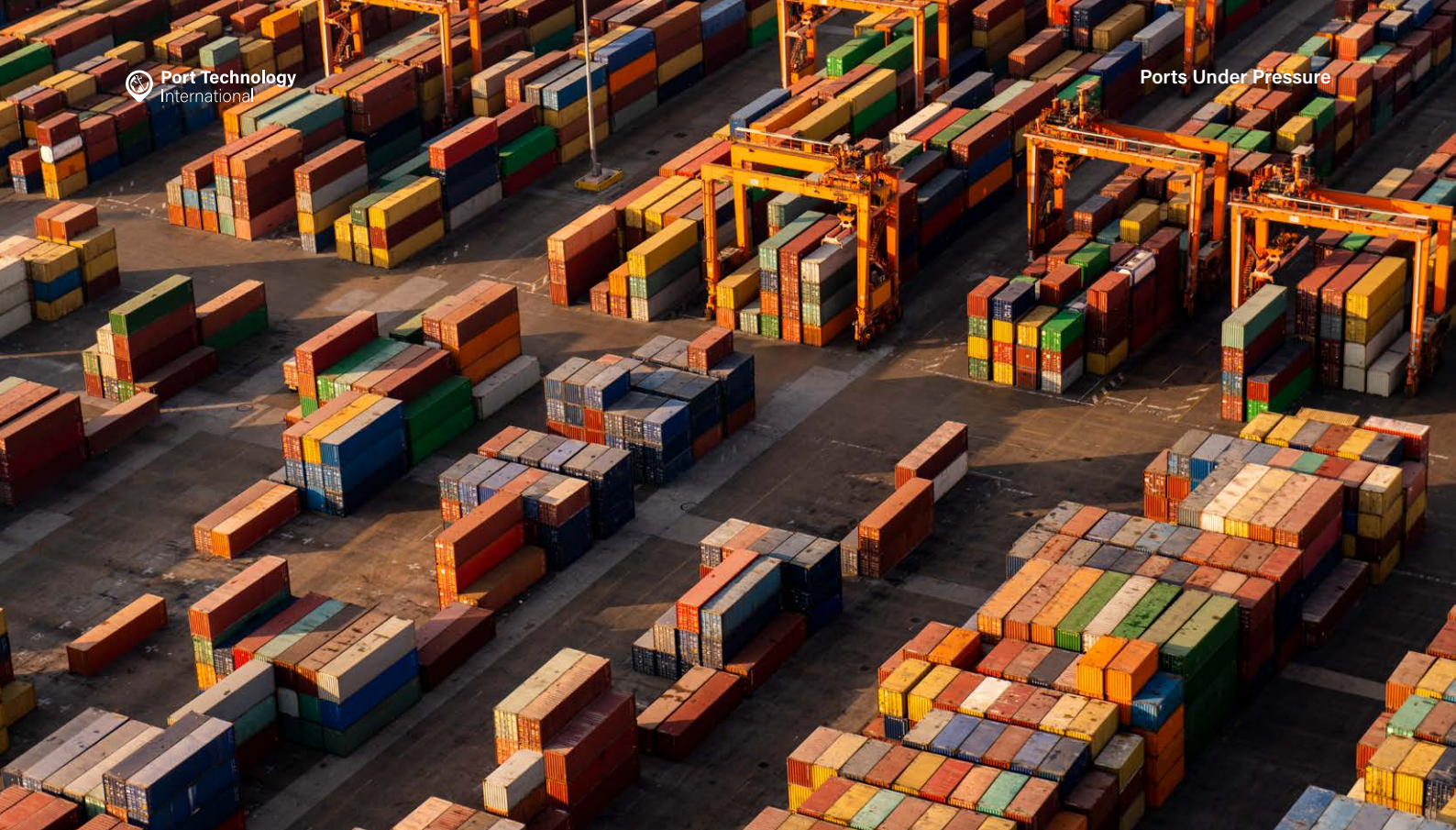
Bertrand Chen is the CEO of Global Shipping Business Network (GSBN), a neutral, not-for-profit blockchain consortium building a paperless, accessible and sustainable trade ecosystem. Its members include shipping lines, terminal operators, banks, insurers and solution providers.

One specific area of focus for GSBN is ensuring that the adoption of electronic Bill of Lading (eBL) can power further trade growth through the tokenisation of trade flows.

About the company

The Global Shipping Business Network (GSBN) is a neutral, not-for-profit consortium whose mission is to enable paperless, accessible and sustainable growth in global trade with its data infrastructure and ecosystem of partners. GSBN facilitates trusted collaboration between participants across the shipping industry to enable greater efficiencies and paperless trade, as well as supporting the shipping industry's decarbonisation transition.

GSBN's ecosystem includes shipping lines, terminals, banks, application developers and other consortia. The entire network accounts for more than half of the containers handled in the world.



Port Resilience Through Integrated Inspection:

What One Container
Reveals About
Transparency,
Control and Revenue
Assurance



Shaleen White,
Vice President for Latin America
Business Development, S2 Global

"The container will keep moving; the question is whether the port can prove it moved through a process worthy of trust."



A container arrives at a port with a declared manifest, a scheduled slot and an expectation of rapid clearance. It has already passed through several hands before reaching the gate. The carrier expects it to keep moving. The terminal has a plan for where it should go. Customs has a responsibility to know what is inside. No one wants delays, but no one can afford uncertainty either.

The container will move. Ports are built for that. What matters after the gate closes behind it is the proof left behind: confirmation that the cargo was verified, the inspection path held, and the clearance decision rested on a record strong enough to withstand review.

For port and customs authorities, that is what transparency now means. It is control at the point where cargo enters the inspection process, discipline in the way the shipment is handled, and an auditable record that follows the transaction from arrival to release. If the container can avoid inspection, if the scan cannot be tied back to the manifest, or if the decision disappears into a disconnected file, the port has movement but not transparency.

The Container Is Called Forward

In a well-run seaport, the container does not drift into inspection because someone remembered to send it there. It is called

forward through a defined operating process. The driver follows a controlled route. The container identification is captured. The manifest is pulled into the inspection environment. The scan is associated with the shipment before the decision is made.

This may sound procedural, but it is where many inspection programmes succeed or fail. Smuggling, misdeclaration and revenue leakage often depend less on dramatic concealment than on small gaps in process. A missed handoff. A manual exception. A scan stored separately from the declaration. A clearance decision that cannot be reconstructed later.

For a terminal operator, these gaps also create operational risk. If inspection is unpredictable, cargo flow becomes unpredictable. Trucks queue in the wrong place. Officers spend time reconciling data rather than making decisions. Legitimate shipments feel the burden of a process designed to catch the exceptions. The port loses confidence in the rhythm of its own operation.

The Scan Is Only One Moment

The container enters the inspection lane. The scanner produces an image, and that image must be tied to the shipment record, the manifest, the analyst's findings and the final disposition. The inspection event only

has lasting value when it becomes part of a complete transaction history.

S2 Global's turnkey inspection model follows the full life of that transaction. Site design, equipment, software integration, staffing, training, maintenance and long-term performance management are brought under one accountable framework. In many cases, the model also gives an authority access to advanced screening capability without requiring it to carry the full capital and operational burden on its own.

For ports, that accountability changes the work. A scanner at the edge of a terminal still leaves the authority to build the operation around it. A turnkey inspection service defines how the system will be used, maintained, staffed and measured. Throughput, evidence, uptime, officer workflow, and the handoffs between port operations and customs authorities are designed into the process from the start. The container is processed through a controlled workflow that produces a record.

For senior port decision-makers, this is the practical link between inspection and resilience. A resilient port does not depend on heroic manual effort every time a shipment looks unusual. It depends on a process that holds up during normal volume, peak volume, staff turnover, equipment maintenance and scrutiny after an incident.



The Record Follows the Container

As the container is scanned, the inspection system captures more than an image. It links the container number, manifest information, inspection data, analyst observations and clearance outcome into a single inspection record. This is the operational meaning of an auditable record. It lets an authority return to the transaction and understand what happened without relying on memory, informal notes or separate systems that may not agree.

For customs, that record supports enforcement. For the port, it supports confidence in the release. For a tax or revenue authority, it creates a basis for verification when the declared cargo does not match the inspection evidence. The same record that helps clear a compliant shipment quickly also gives authorities the means to challenge a non-compliant one.

Over time, these records become more valuable. They show how cargo moves, where anomalies appear, which lanes carry higher risk, and where operational adjustments may be needed. They also create the foundation for more advanced analytics and AI-assisted inspection. Without reliable inspection data, automation has little to stand on. With it, ports can begin to move from isolated

decisions towards a more disciplined understanding of trade movement.

The container in our story may be entirely legitimate. Most are. The point is that the system should not depend on guessing. If the shipment is compliant, the record helps it move. If it is not, the same process gives authorities a defensible basis to intervene.

A Visible Process Changes Behaviour

Deterrence begins long before a seizure. It begins when the route through the port is known to be controlled and when attempts to avoid inspection are likely to be noticed. A non-bypassable workflow changes the calculation for anyone hoping that inconsistency will work in their favour.

In that environment, the container cannot slip out of the inspection path because a lane is busy or a manual release is easier. The process itself applies pressure. It captures the event, routes the data, requires a decision and leaves evidence of that decision behind. Inspection becomes part of port control because the workflow makes it unavoidable.

For smugglers and those misdeclaring goods, uncertainty is useful. A port that applies inspection unevenly creates room for that uncertainty. A port that applies inspection through a controlled, recorded

process reduces it. The benefit is not limited to what is found on a given day. It is also reflected in what does not attempt to pass through that port tomorrow.

Revenue Is Protected at the Point of Proof

When the container reaches the point of clearance, the question becomes commercial as well as operational. Does the declaration match what has been inspected? Are duties and taxes supported by reliable information? Can a discrepancy be shown clearly enough to act on it?

Misdeclared cargo not only creates a security concern. It affects public revenue and the fairness of trade. Authorities need a process that verifies what has been declared against what has been observed. An auditable inspection record gives that process weight. It turns a concern into evidence and gives the authority a practical means to resolve the shipment.

This is why inspection belongs in the same conversation as trade facilitation and fiscal governance. A port can move cargo quickly and still lose value if declarations cannot be verified. The stronger model is one where compliant cargo moves with less friction because the process is trusted, while suspect cargo is held with evidence that supports action.

What the Model Looks Like in Operation

S2 Global's seaport deployments show how this model performs outside theory. For EMPORNAC in Guatemala, S2 Global supports an integrated turnkey scanning service for imports and exports at the Port of Santo Tomás de Castilla, including 24/7 operations, non-intrusive inspection, remote image analysis, CertScan integration, maintenance, staffing and training. The programme is structured to support high-volume seaport operations, with more than 300,000 containers processed annually through the inspection environment.

At another South American seaport, the same operating discipline has guided cargo screening in a live port environment. The work centres on fitting inspection into the way cargo already moves: routing the container, linking the scan to the shipment record, and giving authorities a reliable basis to clear, question or intervene. For port operators, the lesson is practical. Inspection gains value when it follows the rhythm of the port and leaves behind a record that can be trusted.

These programmes also show why turnkey belongs in the business model discussion. S2 Global can finance, deploy, operate, maintain, train and continuously support the inspection environment. That matters for ports and governments that need stronger control but may not have the capital budget, staffing model or technical structure to build and sustain the full capability alone.

The result is accountability. When the container enters the process, there is a designed path for it to follow. When the image is reviewed, there is a system that connects the review to the shipment. When the container is released, there is a record that explains why.

The Port Still Has to Keep Moving

No terminal operator wants inspection to become the reason a berth plan falls apart or trucks stack up outside the gate. Any inspection model that ignores port realities will eventually be worked around. The more useful approach begins with the operating environment: traffic flow, footprint, staffing, peak periods, maintenance windows, authority roles and the physical points where control can be applied.

That is why the concept of operations matters as much as the equipment. A well-designed CONOPS determines how the container is selected or routed, where it is scanned, who reviews the image, how exceptions are handled, and how the final decision is recorded. It also determines what happens when something breaks, volume spikes, or an officer needs to escalate a finding.

For the container in our story, inspection becomes part of the port's normal movement. The driver follows the route. The system captures the data. The analyst has the information needed to make a decision. The authority receives the outcome. The terminal can plan around a process that behaves consistently.

The Container Leaves, but the Value Remains

At some point, the container is cleared. It exits the port and continues into the supply chain. If the shipment was legitimate, the system has done what it should do: verify, document and release without unnecessary disruption. If the shipment required intervention, the system has given authorities the evidence needed to act.

Either way, the container leaves something useful behind. Its inspection record becomes part of the port's operating memory. It can inform revenue review, officer training, quality control, risk targeting, maintenance planning and future process improvement. One transaction becomes part of a larger picture of how trade actually moves through the port.

That is the quiet strength of an integrated inspection environment. Control is built into the same movement that keeps cargo flowing. Port leaders gain a more reliable way to manage security, compliance and revenue assurance, with less dependence on disconnected steps and more confidence in the integrity of the process.

Conclusion

The container that arrived at the start of this article did not need a dramatic story. Most containers do not. It needed a port environment that could verify what it carried, enforce the path it followed, and preserve the record of how it was cleared. That is the everyday work of port resilience.

For port and terminal operators, transparency has to show up in the record. A shipment enters a controlled workflow. Inspection takes place. The decision is documented. The resulting record gives authorities something they can use for enforcement, audit and revenue assurance.

S2 Global's turnkey model provides a practical way to build that capability into the seaport environment. Operational design, non-intrusive inspection, software integration, trained personnel, maintenance and long-term service accountability work together to give authorities a controlled process with a durable record behind it.

The pressure on ports will continue to grow. Trade volumes will rise, concealment methods will change, and governments will expect stronger proof that revenue and compliance are being protected. Ports that can demonstrate control at the shipment level will be better positioned to meet that pressure. The container will keep moving; the question is whether the port can prove it moved through a process worthy of trust.

About the author

Shaleen White brings nearly 20 years of public sector and international experience, with deep expertise in customs, border security, logistics and trade compliance. Fluent in English and Spanish, she combines government, maritime and private-sector knowledge to support S2 Global's business development across the region.

About the company

S2 Global helps ports turn inspection into a business advantage. With proven seaport deployments, turnkey screening operations and auditable cargo records, S2 Global gives authorities the control to deter smuggling, protect revenue and keep trade moving. The result is stronger port resilience, smarter enforcement and confidence in every clearance decision.