

[Opinion](#)[Ports](#)

Ports Can No Longer Treat Disruption as an Exception

By Sudarshan Daga, Senior Surveyor and Risk & Safety Engineer, IRClass / 29 days ago

Modern ports are increasingly dependent on connected operational systems, automated equipment and digital interfaces between vessels, terminals and logistics networks. While this improves efficiency, it also increases vulnerability to cyber incidents.

Published 29 days ago

[Share](#)

For many years, ports approached risk through relatively stable assumptions. Weather patterns were more predictable, cargo profiles evolved gradually, and operational disruptions were usually treated as isolated events. That environment has changed significantly.

Today, ports are operating in a much more complex risk landscape shaped by climate pressures, digitalisation, geopolitical instability, and the introduction of alternative fuels. In my view, the question is no longer whether ports will face a major disruption, but whether they are prepared to respond and recover when it happens.

One of the clearest changes has been the growing impact of extreme weather. Ports in many regions are experiencing more frequent and more intense cyclones, storms and heavy rainfall events. Even where such events remain seasonal, the operational consequences are becoming more severe. Recovery often extends far beyond the duration of the weather event itself, creating prolonged disruptions across cargo flows and wider supply chains.

Modern Ports Challenges

At the same time, geopolitical instability is introducing a different type of operational uncertainty. Changes in trade routes, sudden cargo reallocations and evolving security concerns can alter traffic patterns and operational demand with very little warning. This creates additional pressure on infrastructure, logistics planning and emergency preparedness.

Alongside physical threats, digitalisation is opening a new area of risk exposure. Modern ports are increasingly dependent on connected operational systems, automated equipment and digital interfaces between vessels, terminals and logistics networks. While this improves efficiency, it also increases vulnerability to cyber incidents.

A successful cyberattack can disrupt cargo systems, terminal operations or navigational support functions without causing any physical damage to infrastructure.

Decarbonisation is adding further complexity. The introduction of alternative fuels such as LNG, methanol, hydrogen and ammonia brings fundamentally different hazard profiles into port environments.

Toxicity risks, cryogenic exposure, flammability, and explosion potential all require different approaches to handling, storage, and emergency response. In many regions, however, infrastructure readiness, operational experience, and regulatory frameworks are still evolving.

What concerns me most is that these risks do not exist independently. A severe weather event during a cyber disruption, or an operational emergency involving a low-flashpoint fuel, can

quickly create layered consequences that challenge conventional emergency planning assumptions.

This is why ports can no longer rely on static risk assessments or compliance-driven paperwork alone.

Risk Management

Risk management must become a continuous operational discipline. A meaningful risk assessment should reflect how the port actually functions daily, including vessel movements, anchorage operations, cargo interfaces, storage arrangements, and emergency response capability. It must also evolve as the port changes.

In practice, however, risk studies often become outdated. Ports expand, traffic volumes increase and new cargoes are introduced, but the underlying assumptions within older assessments may remain unchanged. Over time, this can create a significant gap between assessed risk and actual operational exposure.

I also believe that disaster management planning sometimes becomes too compliance-focused. Many ports have plans that satisfy regulatory requirements, but not all plans are operationally credible under real emergency conditions. Effective emergency response depends on clearly defined responsibilities, realistic scenarios and regular drills that test whether procedures actually work under pressure.

The handling of dangerous goods in container terminals remains another area requiring continuous attention. Misdeclared cargo continues to present a serious operational risk because it undermines segregation requirements, firefighting strategy and emergency response planning before an incident even begins. In these situations, risk management depends not only on documentation, but also on terminal layout, traffic management, emergency access and personnel understanding the hazards they are dealing with.

For ports handling liquefied gases and alternative fuels, technical risk tools such as gas dispersion analysis are becoming increasingly important. These studies help operators understand how flammable or toxic gas clouds could spread following an accidental release and support decisions around safety distances, gas detection placement and emergency shutdown systems.

Resilience

At the same time, I would caution against treating modelling results as absolute answers. Such studies are highly dependent on assumptions regarding weather, congestion, surrounding structures, and release conditions. Their real value lies in how the findings are translated into practical operational controls and emergency preparedness measures.

Ultimately, the ports that will perform best in the coming years will not necessarily be those with the largest infrastructure or the most advanced systems. They will be the ports that treat risk management as a living process that evolves alongside operational realities.

Disruption today can emerge from climate events, digital systems, fuel transitions or geopolitical instability, often simultaneously. In that environment, preparedness is no longer simply about meeting standards. It is about understanding how risks interact and ensuring ports are capable not only of responding effectively, but also recovering quickly when operations are disrupted.

Share this article

[Twitter](#)[Facebook](#)[LinkedIn](#)[Copy Link](#)