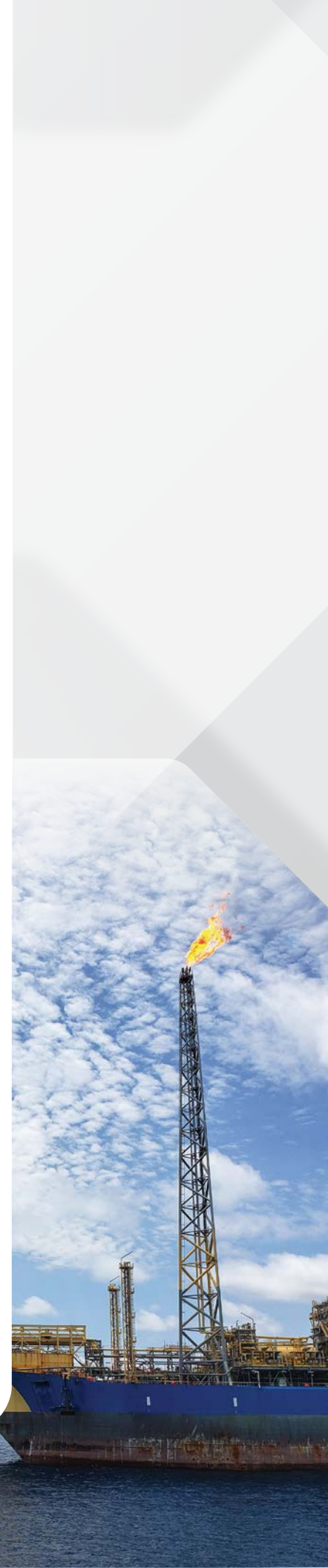




# Cybersecurity challenges and strategies in FPSO operations: A lifecycle perspective

Floating Production Storage and Offloading (FPSO) vessels are pivotal in offshore hydrocarbon production, especially in deep-water and remote locations. While their advanced systems enhance operational efficiency, they also introduce significant cybersecurity vulnerabilities. This paper examines the complexities of integrating Industrial Control Systems (ICS), Operational Technology (OT), and Information Technology (IT) within FPSO operations, which complicate cyber defense strategies. We propose a targeted mitigation approach throughout the FPSO lifecycle, emphasizing the importance of frameworks such as the Zero Trust model, ISA/IEC 62443, SOC 2, and the NIST Cybersecurity Framework (CSF) in building essential organizational competencies. Through analysis of real-world incidents, we demonstrate the severe consequences of inadequate cybersecurity measures and underscore the urgent need for proactive risk management in FPSO operations.





## Introduction

Floating Production Storage and Offloading (FPSO) vessels play a vital role in advancing offshore hydrocarbon extraction, particularly in deep-water and remote areas where conventional infrastructure is inadequate. These vessels are equipped with state-of-the-art systems such as process control and safety instrumented systems (SIS), designed to enhance operational efficiency and increase productivity. However, the complexity of these sophisticated systems also brings about substantial cybersecurity challenges.

Cyberattacks on FPSOs can have far-reaching impacts. They have the potential to cause equipment failures, trigger environmental disasters, and create safety hazards, thereby endangering personnel and the surrounding ecosystem. Operational disruptions can lead to significant unplanned downtime, resulting in financial losses and reputational harm. Additionally, environmental damage from oil spills or gas leaks can lead to regulatory scrutiny and have long-term consequences. Given that FPSO vessels can produce up to 200,000 barrels of oil per day, a cyber incident could have profound implications in terms of financial cost, safety, environmental impact, and reputation.

The remote and isolated locations of FPSOs further complicate efforts to respond to and recover from incidents. In this paper, we delve into the cybersecurity challenges throughout the FPSO lifecycle and offer strategic approaches to mitigate these risks.

# 1. Cybersecurity incidences in oil and gas operations

The integration of complex systems in FPSO operations brings numerous cybersecurity challenges that must be addressed to achieve safe and efficient production. Understanding these challenges is crucial for developing effective strategies to help protect these critical assets from cyber threats.

## Safety and operational risks

Cyberattacks on FPSOs can compromise control systems, resulting in equipment malfunctions and environmentally destructive spills. Such incidents pose significant safety risks to personnel and can lead to catastrophic events, including explosions and fires. Additionally, operational disruptions can cause significant downtime, affecting production schedules and leading to substantial financial losses. Effective cybersecurity measures are essential to mitigate these risks and maintain dependable FPSO operations.

## Financial and environmental impacts

Cyberattacks on FPSOs can result in substantial downtime and environmental damage, translating into significant financial losses and reputational harm. Prolonged operational disruptions can lead to deferred revenue and increased costs associated with repairs and recovery efforts. Environmental incidents, such as oil spills or gas leaks, not only incur cleanup expenses but also attract regulatory fines and legal liabilities. The long-term reputational damage from such events can affect stakeholder trust and market position, emphasizing the need for robust cybersecurity measures to help protect against these financial and environmental risks.

### Cyber event: European Oil Tankers and Storage Sites (2022)

A substantial ransomware attack negatively impacted at least 17 ports and oil terminals in Western Europe. The ransomware/malware attack also affected oil storage and transport. Several companies affected by the attack declared force majeure, an emergency legal clause that is used when a company cannot fulfill its supply contracts because of an unforeseeable event.

### Cyber event: Offshore Rig Tilting (2015)

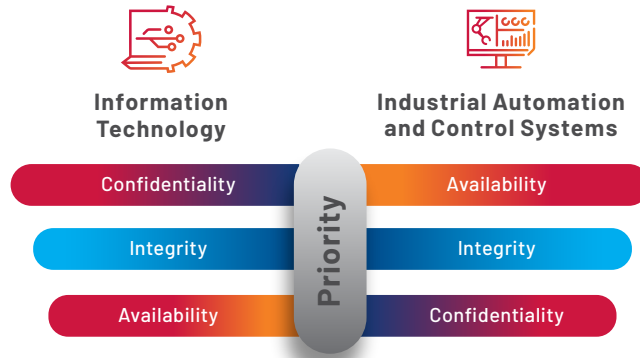
An offshore oil rig near the African coast was breached, causing the platform to tilt resulting in a week-long shutdown. This incident highlights the physical and operational impacts of cybersecurity breaches. The vulnerability was found in the control systems responsible for managing the pontoons that keep offshore rigs afloat. A hacker infiltrated a pontoon control system draining the ballast on one side, causing the platform to tilt over.

### Cyber event: Colonial Pipeline Ransomware Attack (2021)

The attack led to a shutdown of operations, causing fuel shortages across the East Coast. The attack was highly publicized, with the company paying \$4.4 million in ransom to regain access to its systems.

## 2. Operational technology vs. information technology

In FPSO operations, understanding the distinctions between Operational Technology (OT) and Information Technology (IT) is crucial for developing effective cybersecurity strategies. These two domains serve different purposes and face unique challenges, especially in high-stakes environments like FPSOs.



### Fundamental differences

IT focuses primarily on data processing, management, and communication, delivering the smooth flow of information across networks and systems. In contrast, OT is integral to cyber-physical systems, directly interfacing with the physical world to monitor and control industrial processes. In OT environments, priorities are centered on safety and the continuous availability of operations, with less emphasis on data confidentiality. These systems often rely on each other to provide a vessel with a seamless and informed operation. However, fundamental differences in cybersecurity priorities demand tailored approaches to address the specific needs and vulnerabilities of each domain effectively.

### Rethinking cybersecurity for OT

Traditional IT security models, such as the CIA Triad (Confidentiality, Integrity, Availability), are often inadequate for addressing the unique requirements of OT environments. In FPSO operations, where OT systems directly interact with physical processes, the primary concerns extend beyond data confidentiality. The (S)AIC framework—Safety, Availability, Integrity, and Confidentiality—provides a more suitable approach, aligning with the critical priorities of OT systems. This framework places a greater emphasis on achieving operational safety and continuous availability, while still maintaining the integrity and confidentiality of data. By adopting the (S)AIC framework, organizations can develop more effective cybersecurity strategies that address the specific needs and vulnerabilities of OT environments within FPSO operations.



### 3. Mitigation strategies across the FPSO lifecycle

Effective cybersecurity for FPSO operations requires comprehensive mitigation strategies that align with the (S)AIC framework. By focusing on safety, availability, integrity, and confidentiality, these strategies can be integrated throughout the FPSO lifecycle to address specific vulnerabilities at each phase.

#### Design phase

The design phase is crucial for embedding security into the core architecture of FPSO systems. A lack of security considerations and insecure coding practices at this stage can introduce significant risks. To mitigate these, adopting a “security by design” approach confirms that security principles are integrated from the outset. Conducting thorough risk assessments helps identify potential vulnerabilities early, while establishing secure software development lifecycle practices help to ensure that security remains a priority throughout the development process.



By addressing these elements during the design phase, FPSO operations can build a strong foundation for maintaining safety, availability, integrity, and confidentiality across their systems.

**Lifecycle tip:** Engaging with cybersecurity consulting services during the design phase of FPSO operations can significantly enhance the security posture of the project from the outset. Here are some key strategies to leverage these services effectively:

- Implement network segmentation
- Adopt a defense-in-depth strategy
- Deliver redundancy and resilience
- Incorporate secure remote access solutions
- Plan for scalability and future growth

#### Construction and commissioning phase

The construction and commissioning phase is critical for verifying that FPSO systems are configured securely and function as intended. Misconfigurations and inadequate testing during setup can introduce vulnerabilities that compromise Safety, Availability, Integrity, and Confidentiality. To address these challenges, implementing secure configuration management practices is essential to maintain consistent and secure system settings. Comprehensive testing and security audits should be conducted to identify and rectify any potential security flaws before systems go live. Additionally, enforcing strict access control measures for third-party contractors is crucial to help prevent unauthorized access and mitigate potential risks associated with external parties. By focusing on these strategies, FPSO operations can strengthen their cybersecurity posture during this pivotal phase.

**Lifecycle tip:** Optimizing network design and architecture during the construction and commissioning phase

during the construction and commissioning phase of FPSO operations, careful attention to network design and architecture is crucial for establishing a secure and efficient operational environment.

Here are key strategies to consider:

- Early involvement
- Risk assessment and threat modeling
- Security by design principles
- Framework alignment
- Training and knowledge transfer

## Operation phase

During the operation phase, FPSO systems often face challenges related to legacy systems and insecure remote access, which can compromise the overall security of the operation. To mitigate these risks, several strategies are recommended.

First, conducting regular cybersecurity awareness training for all personnel to inform employees about current threats and best practices for maintaining security. Second, conducting regular audits and assembling a comprehensive asset inventory creates visibility into OT assets and identifies potential vulnerabilities. Implementing a robust patch management process is essential to keep all systems and software up to date with the latest security patches and updates, reducing the risk of exploitation. Lastly, deploying intrusion detection and prevention systems (IDPS) helps to monitor network traffic and detect any malicious activities, allowing for timely responses to potential threats. By adopting these strategies, FPSO operations can enhance their security posture and deliver the ongoing protection of their systems throughout the operation phase.



**Lifecycle tip:** Utilizing managed network and threat detection services during the operations phase

In the operations phase of FPSO systems, maintaining a robust cybersecurity posture is critical to continuous and safe functioning of operations. Leveraging managed network and threat detection services can significantly enhance security measures, keeping your team focused on core operations.

Here are key strategies to consider:

- Comprehensive asset inventory
- Real-time threat detection
- Scalable solutions
- Comprehensive reporting and analytics
- Outsource to a managed security services provider (MSSP)

## Maintenance phase

The maintenance phase of FPSO operations is critical for the continued security and functionality of systems. However, using unsecured maintenance tools and the absence of robust incident response plans can introduce significant vulnerabilities. To address these concerns, several actions are recommended.

**Lifecycle tip:** Enhancing cybersecurity during regular maintenance workovers of FPSO vessels

During regular maintenance workovers of FPSO vessels, it is essential to focus on maintaining and enhancing the cybersecurity systems to help ensure the ongoing protection of critical operations.

Here are key strategies to consider:

- Security audits and assessments
- Update and batch management
- Testing and validation of incident response plans
- Secure configuration management
- Training and awareness programs

Implementing secure remote access solutions is essential to help protect maintenance activities from unauthorized access and potential threats. Establishing strict protocols for the use and management of maintenance tools helps ensure that they do not become vectors for malware or unauthorized modifications. Additionally, regularly testing incident response plans confirms that the organization is prepared to respond swiftly and effectively to any security incidents that arise. By focusing on these actions, FPSO operations can maintain a strong security posture during the maintenance phase, safeguarding both their systems and the broader objectives of safety, availability, integrity, and confidentiality.



## 4. Zero Trust cybersecurity architecture

In the context of securing complex industrial environments like FPSO systems, the Zero Trust Cybersecurity Architecture offers a comprehensive and proactive approach. Rooted in the principle of “never trust, always verify,” Zero Trust assumes that no entity—whether inside or outside the network—should be inherently trusted. Every access request requires rigorous authentication and authorization, delivering robust security across all layers of the network.

### Key principles of zero trust

**Micro-segmentation:** This principle involves dividing the network into smaller, isolated segments to contain and mitigate breaches. In OT environments, micro-segmentation is critical for maintaining strict partitioning between IT and OT networks, helping prevent IT-based attacks from affecting critical operational processes. Additional controls may include application-layer firewalls with deep packet inspection and the blocking of unused protocols and services.

- **Principle of Least Privilege (PoLP):** Access rights are allocated based on the minimum permissions necessary for users and devices to perform their designated roles. This minimizes the potential impact of compromised accounts by limiting access to only what is essential.

- **Assume breach:** Operating under the assumption that adversaries have already compromised the environment, this principle emphasizes the need for continuous threat hunting, proactive control validation, and regular security audits to identify and mitigate vulnerabilities.
- **Multi-factor authentication (MFA):** Critical systems should require MFA wherever feasible, adding multiple layers of identity verification before granting access. This enhances security by verifying that even if credentials are compromised, unauthorized access is still prevented.
- **Continuous monitoring and logging:** Comprehensive logging and monitoring mechanisms across all assets are essential for detecting and responding to suspicious activities in real-time. This continuous oversight allows for timely identification and mitigation of potential threats, maintaining the integrity and security of FPSO operations.

By integrating these principles, Zero Trust cybersecurity architecture provides a robust framework that enhances the security posture of FPSO systems. This approach is especially advantageous for FPSOs due to their unique circumstances, such as their remote and isolated locations, complex industrial processes, and critical dependency on continuous operations. Implementing stringent security measures helps safeguard against evolving threats, maintaining the safety, availability, integrity, and confidentiality of their operations in these challenging environments.



## 5. Relevant standards and best practices

To maintain robust cybersecurity measures for FPSO operations, adherence to internationally recognized frameworks and standards is essential. These frameworks provide structured guidance and best practices to secure complex industrial environments effectively.

- **ISA/IEC 62443:** A comprehensive standard for securing Industrial Automation and Control Systems (IACS), addressing security lifecycle requirements, zones and conduits, and defense-in-depth strategies. This standard is particularly relevant to securing FPSO operations.
- **NIST Cybersecurity Framework (CSF):** A high-level strategic framework that categorizes cybersecurity efforts into five core functions: Identify, Protect, Detect, Respond, and Recover. This adaptable framework is widely used across multiple industries, including oil and gas.
- **ISO 27001:** An international standard outlining best practices for establishing and continuously improving an Information Security Management System (ISMS), delivering a structured approach to risk management.

- **SOC 2 (System and organization controls 2):** A security auditing standard that evaluates data security, availability, processing integrity, confidentiality, and privacy—especially relevant for FPSOs utilizing cloud-based analytics, remote monitoring, and storage solutions.

By adopting these standards and best practices, FPSO operations can establish a solid cybersecurity foundation, enabling them to effectively manage risks and safeguard critical infrastructure in today's increasingly digital and interconnected world.

However, implementing these frameworks in an international context, especially for a dynamic and mobile environment like an FPSO, involves complexities due to diverse regulatory requirements, cultural differences, and the logistical challenges of maintaining security across various jurisdictions. Engaging with experts who possess a deep understanding of these frameworks can significantly ease this process. They offer valuable guidance by simplifying the adoption of these standards into manageable steps, helping FPSO operations seamlessly integrate robust cybersecurity measures while successfully navigating the intricacies of international compliance and operational mobility.

## 6. Conclusion and recommendations for future expansion

Adopting Zero Trust cybersecurity architecture and adhering to internationally recognized standards provide FPSO operations with a solid framework to manage risks and help protect critical infrastructure. This approach is crucial for maintaining both financial stability and environmental safety, as FPSOs operate in sensitive marine ecosystems where breaches could lead to catastrophic events like oil spills, affecting marine life and coastal communities. Protecting these assets is vital for economic and environmental sustainability.

Implementing these frameworks on an international scale, especially for mobile FPSOs, presents challenges due to diverse regulations and logistical complexities. Partnering with IT/OT cybersecurity experts can greatly simplify this process by breaking down standards integration into manageable steps. These partnerships offer valuable insights and streamline cybersecurity implementation, helping FPSO operations effectively navigate compliance while maintaining operational mobility. Expert guidance can make all the difference, providing tailored solutions that uphold financial and environmental protections against evolving threats.

Future research should focus on developing asset inventory, advanced threat detection and response techniques tailored to the unique challenges of the offshore environment, exploring the application of AI and machine learning in cybersecurity, and enhancing collaboration and information sharing within the industry. The increasing convergence of IT and OT, coupled with the growing reliance on cloud technologies, necessitates a continuous evolution of cybersecurity practices to stay ahead of emerging threats.

### Securing critical OT infrastructure

With mounting connectivity of systems and a mobile infrastructure, FPSO teams struggle to stay on top of asset inventory and monitoring networks to evaluate and deploy adequate OT cybersecurity tools or provide awareness training for employees. Most find that they can't do it on their own.

With more than 100 years of industrial automation experience combined with specialized industrial cybersecurity knowledge, Rockwell Automation helps organizations mitigate risk with assessments, vulnerability management, 24/7 threat monitoring, and incident response — helping to protect OT environments worldwide.

To learn more, visit our [Critical Infrastructure Resource Center](#), or talk to a cyber expert today.

## References

Jamie Crandal, Cybersecurity and Offshore Oil: The Next Big Threat, 4 OIL & GAS, NAT. RESOURCES & ENERGY J. 703 (2019),

<https://www.controleng.com/throwback-attack-hackers-take-advantage-of-the-holidays-to-hit-oil-giant-saudi-aramco/>

<https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>

<https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities>

<https://therecord.media/halliburton-reported-cyberattack-company-confirms-issue>





International Society of Automation (ISA), "Cybersecurity Standards for Industrial Control Systems."

National Institute of Standards and Technology (NIST), "Cybersecurity Framework for Critical Infrastructure."

United States Government Accountability Office - Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure

<https://bbc.com/news/technology-60250956>



Connect with us.    

[rockwellautomation.com](http://rockwellautomation.com) — expanding **human possibility**<sup>®</sup>

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800

Allen-Bradley and expanding human possibility are trademarks of Rockwell Automation, Inc.  
Trademarks not belonging to Rockwell Automation are property of their respective companies.

Publication OAG-WP003A-EN-P - April 2025

Copyright © 2025 Rockwell Automation, Inc. All Rights Reserved. Printed in USA.