OT cybersecurity: The essential guide to securing oilfields

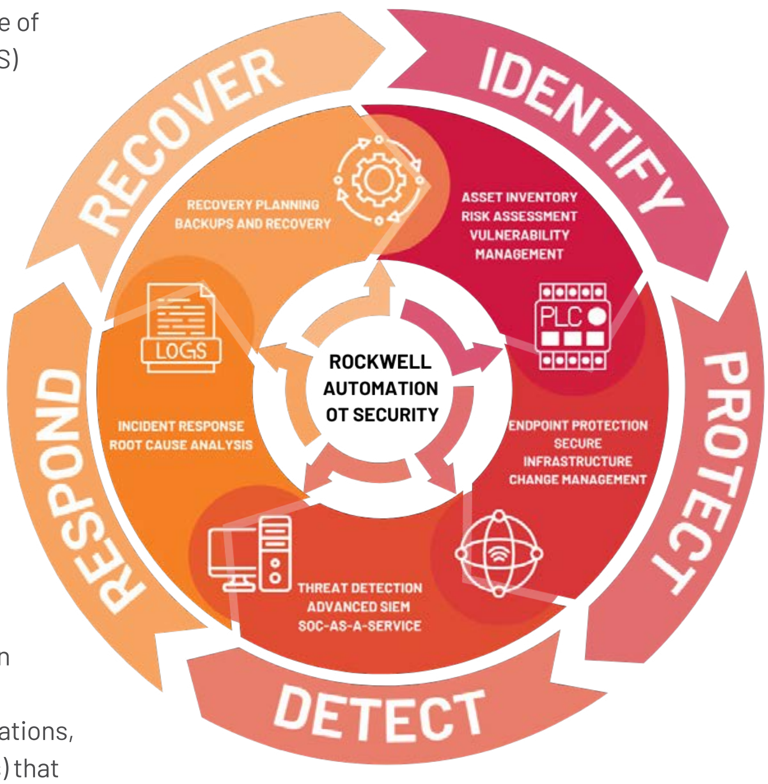
Rockwell Automation

In the past two decades, **digital transformation has revolutionized the oil and gas sector**, driving unprecedented innovation and efficiency in oilfield operations. Yet, this increased connectivity has also opened the door to a new era of threats. Cyberattacks targeting Operational Technology (OT) systems have become alarmingly successful, putting critical infrastructure at significant risk and demanding immediate action from organizations.

This guide is your **comprehensive roadmap to understanding OT cybersecurity** in the oilfield. We'll delve into its vital importance, explore the challenges that lie ahead, and uncover key strategies for protection. Whether you're a seasoned professional or just starting your journey in OT cybersecurity, this guide is your essential companion in safeguarding the future of oilfield operations.

Understanding OT cybersecurity: Definition and scope

OT cybersecurity, or Operational Technology cybersecurity, is fundamentally the practice of safeguarding industrial control systems (ICS) and the associated hardware and software that manage critical infrastructure within oil and gas operations. At its core, OT cybersecurity is purpose-built to aid in protecting the technologies that control physical processes across the oilfield, including exploration, extraction, and transportation of product. Its primary objectives are to deliver safety, reliability, and availability (SRA) for oilfield operations and to defend the specialized devices, networks, and processes that are essential for keeping oil production running. It safeguards a wide range of oilfield infrastructure, such as Supervisory Control and Data Acquisition (SCADA) systems used for monitoring and controlling processes across dispersed locations, and Programmable Logic Controllers (PLCs) that automate specific tasks.



Why OT cybersecurity matters

The critical importance of OT cybersecurity in the oilfield becomes clear when considering the potentially severe consequences of a cybersecurity breach. Key reasons why OT cybersecurity is paramount in this sector include:

Physical safety

OT cybersecurity breaches can result in tangible harm, impacting the safety of personnel on oil rigs and in processing facilities, as well as the public. This is a critical operational challenge in oilfields.

Economic impact

Incidents can lead to massive financial losses stemming from operational disruptions, damage to equipment, and the cost of recovery. Operational challenges like declining production rates and increased operating costs are exacerbated by cyber incidents.

National cybersecurity

Attacks on critical infrastructure managed by OT systems in the oilfield can have significant implications for national cybersecurity and societal stability.

Regulatory compliance

A growing body of regulations and standards mandates robust OT cybersecurity practices, and non-compliance can lead to penalties.

The focus of OT cybersecurity in the oilfield differs from traditional IT cybersecurity, primarily prioritizing safety, reliability, and availability over confidentiality. OT systems in this sector also typically have a much longer lifespan, often 15-20 years or more, with updates being infrequent and carefully planned due to potential operational impacts.

IT vs. OT explained: Differences, challenges, and convergence

With the increasing interconnectedness between OT and IT in the oilfield, the traditional boundaries are blurring.

This convergence presents both opportunities and challenges.

- **Priorities:** IT typically prioritizes the confidentiality and integrity of data, embracing rapid technological advancements. OT in the oilfield, conversely, places a higher emphasis on maintaining the stability and reliability of physical operations and adopts new technologies cautiously.
- **System characteristics:** OT systems in oilfields often involve legacy equipment with long lifespans and infrequent updates, whereas IT systems generally have shorter lifecycles and more frequent updates.
- **Risk perception:** IT cybersecurity often focuses on digital risks, while OT cybersecurity in the oilfield evaluates the potential impact of cybersecurity actions on physical processes and safety, including environmental risks. OT environments also face unique challenges like zero-day vulnerabilities in embedded devices.
- **Regulatory environment:** IT cybersecurity operates within a well-established framework of cybersecurity laws and standards, while OT in the oilfield is increasingly subject to specific industrial cybersecurity regulations.

The blurring lines necessitate synergy and collaboration. Integrating teams and establishing shared understanding are crucial steps in navigating this convergence effectively, particularly in establishing an OT/IT unified data flow.

Aspect	Information Technology (IT)	Operational Technology (OT)
Focus area	• Data management and security • Digital technology solutions	• Direct control of physical devices and processes • Reliability and continuity of operations
Devices	• Commodity Windows servers. PCs, mobile devices running standard OS and apps • Refresh cycle 3–5 years	• Customized OS devices running OEM apps, OT-proprietary embedded devices, custom production systems • Refresh cycle 2030 years
Uptime and redundancy	• Common redundancy and failover mechanism • Rebooting user devices with minimal impact	• Minimal redundancy • Rebooting operational devices highly disruptive due to potential impact on critical processes
Infrastructure	• Cloud-based or hybrid cloud solutions	• On-premises solutions, early steps towards cloud for certain functions
Remediation	• Simple threat remediation (e.g., system reboots) with minimal impact • Lower operational risk	• Complex threat remediation • High operational risk; incorrect actions can halt production for extended periods
Threat identification	• Extensive public database for vulnerability identification • Lower zero-day vulnerability exposure	• Challenges in identifying domain-specific threats • Highter exposure to zero-day vulnerabilities, especially in embedded devices
Compliance	• Stringent cybersecurity compliance regulations	• Early stages of compliance adaption, except in sectors like energy (NERC CIP)

Key challenges in OT cybersecurity

CHALLENGE 1 • Gaining comprehensive asset visibility

Without a clear understanding of your OT assets in the oilfield, including those on and off the network, their configurations, and key specifications, protecting them is extremely difficult. An ideal OT asset inventory should include detailed information about hardware, software, network connections, users/accounts, vulnerabilities (including CVSS scores and attack vectors), and configuration settings. The lack of a robust inventory makes crucial cybersecurity tasks like patching, secure configuration, and user access controls much harder. This visibility gap makes identifying vulnerabilities that threat actors could exploit difficult. Maintaining a comprehensive asset inventory is a key activity in defining a cybersecurity strategy.

CHALLENGE 2 • Managing legacy systems

Oilfield control systems often utilize legacy or outdated equipment and software that may no longer receive cybersecurity updates, leaving them vulnerable. Strategic prioritization is key; not everything can be fixed at once. It is important to identify legacy systems, their configurations, known vulnerabilities, and their operational criticality. For high-risk legacy systems where immediate updates or replacements are not feasible, isolating them through network segmentation and implementing compensating controls like strict access policies, approvals, and continuous monitoring are necessary.

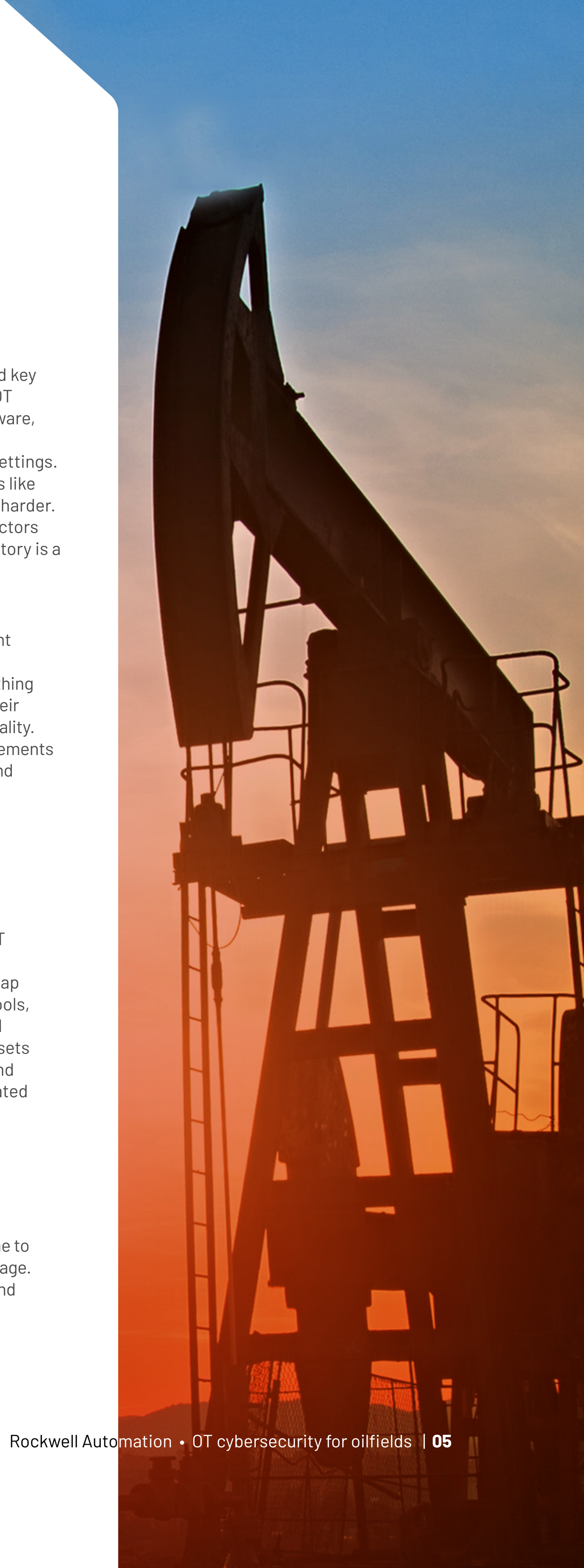
CHALLENGE 3 • Bridging the IT/OT divide

The historical separation of IT and OT in oil operations has led to differences in culture, priorities, and expertise. Effective collaboration is often hindered, yet it is crucial for successful OT cybersecurity. IT understands the technical cybersecurity side, while OT knows oilfield operations and its needs. Bridging this gap requires open communication, regular joint meetings, shared tools, and team members who understand both environments. Shared risk assessments, where IT and OT teams jointly map critical assets and prioritize vulnerabilities based on both cybersecurity risk and operational impact, foster a shared understanding and coordinated response. Building an OT/IT Unified Data Flow is essential for seamless integration.

Slow incident response

Without real-time visibility into OT assets and potential threats in the oilfield, cybersecurity teams struggle to identify and contain breaches quickly. This delay provides threat actors with more time to cause operational disruptions, safety hazards, or significant damage. Developing an incident response plan is crucial to limit damage and speed recovery.

These challenges can compound, as understanding assets lead to identifying vulnerabilities, which necessitates patching or implementing compensating controls, and these controls require backups.



Technologies that impact OT cybersecurity in the oilfield

The oilfield is experiencing a rapid integration of increasingly connected technologies, bringing both transformative potential and new cybersecurity challenges to Operational Technology (OT) environments. Understanding these technologies and their impact is crucial for maintaining robust cybersecurity postures in the face of digital modernization.

Industrial Internet of Things (IIoT) and smart instrumentation

IIoT is expanding rapidly in the oilfield, encompassing a vast network of sensors, actuators, control systems, and data collection points across wells, pipelines, and processing facilities. This includes the increasing deployment of smart instruments that provide more precise and real-time data. This connectivity enables real-time monitoring, predictive maintenance, and optimized operations. However, it also significantly expands the attack surface, introducing numerous new potential entry points for cyber threats through these connected devices. Securing every connected device and delivering secure communication channels are paramount challenges.

Cloud computing

Cloud platforms are increasingly used in the oilfield for data storage, processing, and analytics, enabling remote operations and enhanced collaboration. While offering scalability and accessibility, migrating, or connecting OT data and systems to the cloud introduces risks related to data breaches, unauthorized access, and the cybersecurity posture of cloud service providers. Secure configuration and access management are critical.

Wireless technologies

Various wireless technologies are becoming essential for connectivity in the often remote and challenging environments of the oilfield. 5G offers high-speed, low-latency communication, facilitating real-time data exchange and enabling sophisticated remote control of OT systems, including those involved in artificial lift and multi-well pad automation. Other wireless technologies are also widely used for data transfer, remote monitoring, and connecting dispersed assets. While enhancing operational flexibility and enabling remote management, the widespread use of wireless connectivity significantly increases the attack surface. Cybersecurity risks include signal interception, unauthorized network access, interference, and the need to secure communication links across potentially unreliable or public networks.

Edge computing

Edge computing brings data processing and analysis closer to the source in the oilfield, such as at the wellhead or a remote processing unit, minimizing latency and enhancing responsiveness. This is particularly relevant for automating processes like artificial lift and multi-well pads and enabling localized analytics. While beneficial for real-time decision-making and reducing reliance on centralized systems, securing edge devices and confirming the integrity of data processed at the edge are critical.

Artificial Intelligence (AI), Machine Learning (ML) and advanced analytics

AI and ML are being leveraged in the oilfield for tasks like predicting equipment failures, optimizing production (including artificial lift performance), and enhancing threat detection through advanced analytics. These technologies enable the analysis of vast amounts of operational data from smart instruments and automated systems to gain deep insights, identify unusual patterns that may indicate a cyberattack, and improve decision-making through data-driven predictions. However, integrating AI/ML and advanced analytics into OT environments introduces cybersecurity risks such as data poisoning, model theft, adversarial attacks, and a lack of transparency in decision-making processes.

Digital twins

Digital twins, virtual replicas of physical oilfield assets or processes like multi-well pads or artificial lift systems, are used for simulation, analysis, and optimization. They can also be valuable for cybersecurity by allowing for attack simulations in a safe environment and identifying potential vulnerabilities before they impact the physical system. Analyzing the digital twin can help detect anomalies in system behavior that might indicate a cybersecurity breach. However, the cybersecurity of the digital twin itself and the data it utilizes is crucial.

Electrification

The increasing electrification of oilfield operations, moving away from gas engine systems towards electric motors and controls for applications like artificial lift, introduces new cybersecurity considerations related to power distribution and control systems. Securing these electrified systems and their network connections is vital to prevent disruptions to production and achieve safety.

Artificial lift and multi-wellpad automation

The automation of artificial lift systems (ESP, PCP, SRP) and the implementation of multi-wellpad automation rely heavily on connected OT systems. While increasing efficiency and enabling remote management, these automated systems present specific cybersecurity risks related to the control logic, communication protocols, and remote access points. Securing these automated processes is crucial to deter unauthorized manipulation that could lead to operational failures, safety incidents, or environmental damage. The integration of these emerging technologies necessitates a proactive and adapted approach to OT cybersecurity in the oilfield, addressing the unique risks and vulnerabilities they introduce while harnessing their potential for improved operational efficiency and safety.

Key strategies for robust OT cybersecurity

Overcoming OT cybersecurity challenges in the oilfield requires implementing strategic mitigation measures and adopting key cybersecurity practices, often following frameworks like NIST.

Comprehensive asset inventory and visibility:

This is the foundational step. Creating and continuously maintaining a comprehensive asset inventory provides a deep understanding of your assets, including detailed profile data such as criticality to operations, network layer, and remote accessibility. This visibility enables organizations to identify vulnerabilities in their defenses and forms the basis for strong cybersecurity, allowing tools, processes, and future planning to align with specific needs. An effective solution should provide a 360° view and comprehensive risk scoring beyond just CVE or CVSS. Continuous OT network monitoring solutions that understand OT communication patterns are also crucial for real-time alerts on anomalies. A centralized monitoring dashboard can consolidate visibility, simplify risk analysis and streamlining incident response.

Network segmentation for OT:

Dividing the OT network into smaller, isolated segments or zones is a crucial cybersecurity strategy. This limits the spread of cyberattacks by containing potential breaches within a segment, helping to protect critical assets. It also helps optimize performance by helping to alleviate network congestion through isolating high-priority OT traffic. Implementing network segmentation involves steps like mapping the network, designing a segmentation plan (potentially using frameworks like IEC 62443 to guide zone and conduit design), and deploying the plan with testing and backup options. Consistent documentation, monitoring, and adaptation are also necessary.

Strict access control in OT systems:

Implementing stringent access controls is vital to prevent unauthorized access to sensitive OT systems and data in the oilfield.

OT-specific vulnerability management:

This involves assessing assets for known vulnerabilities and broader "insecure by design" risks. It differs from IT vulnerability management due to the nature of OT systems in the oilfield, including legacy equipment and the potential for scans to disrupt operations. Prioritizing vulnerabilities based on possible exploitation and impact is key. Remediation can involve software patches, configuration management, or deploying compensating controls. A powerful asset inventory solution is crucial for effective vulnerability management, providing detailed profile data for prioritization. An approach that allows deep visibility into systems and doesn't solely rely on network traffic for vulnerability determination, potentially using a combined agent and agentless approach, can be more effective and safer in OT environments.

OT-focused incident response planning:

Having tailored incident response plans for the OT environment in the oilfield is essential for reacting quickly and effectively to cybersecurity incidents, minimizing downtime and damage. This includes establishing back-up, recovery, and root cause analysis procedures.

Cybersecurity awareness training:

Tailoring cybersecurity awareness training to each role within the organization and using real-world examples is crucial for educating personnel about OT-specific risks and promoting secure practices in the oilfield.

Overcoming OT cybersecurity challenges: A synthesis

Successfully overcoming OT cybersecurity challenges in the oilfield often involves a strategic combination of the approaches outlined. This includes strategic mitigation, phased modernization for legacy systems, and implementing temporary protections where immediate updates are not possible. The key lies in comprehensive asset discovery and inventory, enabling risk-based prioritization to focus resources effectively. Specialized OT cybersecurity solutions that provide in-depth visibility and granular control are essential for safe monitoring and remediation without disrupting operations. Establishing standardized processes for vulnerability management, incident response, and system updates, along with training personnel in OT-specific cybersecurity best practices, are also critical components of a robust OT cybersecurity program. Building integrated IT and OT teams with clear communication and shared understanding is fundamental, particularly in establishing a unified data flow. Defining a cybersecurity strategy is a key step in modernizing oilfields.

Rockwell Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**®

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

Publication OAG-BR015A-EN-P - July 2025