Operational Technology Outlook 2026

Innovations, security challenges and regulatory requirements

—

June 2026

KPMG Middle East

KPMG

Contents

Foreword

Operational technology (OT) is undergoing a profound transformation, driven by rapid technological advancements and increasing interconnectivity across industries. This evolution is not just a future consideration. It is a present-day imperative that demands immediate attention and strategic action. The first-ever KPMG OT Outlook provides a comprehensive analysis of the current landscape, offering insights into the critical trends, innovations, security challenges, and regulatory requirements that are shaping the future of OT.

As organizations integrate technologies like AI, 5G, and digital twins, they unlock new levels of efficiency and innovation. However, these advancements also expand the attack surface, making robust cybersecurity measures more crucial than ever. This report highlights the importance of asset discovery and management in maintaining operational integrity and compliance with stringent regulations such as NIS2, NCA OTCC, NIST and ISA/IEC 62443.

Furthermore, this publication addresses the challenges posed by legacy systems and the need for strategic solutions to enhance resilience and security. It provides a detailed overview of the global regulatory landscape, helping organizations navigate the complexities of compliance and safeguard their critical infrastructure.

“

For energy, defense, healthcare, and beyond, securing OT is more than protection, it is the gateway to innovation. By embedding AI-driven cybersecurity and advanced monitoring, organizations can converge IT and OT with confidence, accelerate digital transformation, and shape a future where industrial systems are intelligent, resilient, and sustainable.

Hossain Alshedoki

Global IOT Security Leader,
KPMG
Partner, KPMG Middle East

Executive summary

Transformation and momentum

69%

of CEOs now identify Gen AI as a top priority to reshape operational processes and unlock step-change efficiency.

Amid a pivotal transformation, industrial organizations are reframing their ambitions. OT has become the backbone of digital acceleration, no longer confined to the factory floor but integral to enterprise-wide resilience and growth. This resolve is not born of hype but from hard-won experience modernizing operations and the proven returns of connected systems.

Leaders are doubling down on execution at scale. As investments in connected infrastructure surge, OT is shifting from an isolated shop-floor necessity to a strategic pillar. Momentum is evident: over the past two years, organizations have signaled a decisive move from experimentation to measurable impact.

Gen AI and Digital Twins

52%

of organizations now place OT oversight under the CISO.

The technology agenda has matured in parallel. Gen AI, 5G and digital twins are graduating from pilots to enterprise deployment, redefining asset visibility, decision velocity and value capture. The strategic weight of this shift is clear: it aims to reshape operational processes and unlock step-change efficiency. Yet this acceleration brings a security paradox. The rapid convergence of IT and OT unleashes unprecedented productivity while simultaneously expanding the digital attack surface.

For 50 percent of decision-makers, legacy systems remain the principal barrier to securing modern infrastructure. The risks are tangible and cross-sectoral. In healthcare, for example, 99 percent of organizations operate devices with known exploited vulnerabilities.

OT security governance

55%

of organizations have increased their OT budgets.

Interconnected supply chains compound exposure, demanding end-to-end cyber resilience that safeguards both digital data and physical assets. Industry leaders are professionalizing OT security, elevating it from a technical task to a board-level imperative. Governance is shifting accordingly. The share of organizations with dedicated OT security leadership has risen significantly, up from 16 percent in 2022. Spurred by regulatory pressures such as NIS2 and ISA/IEC 62443, robust security architecture is becoming the foundational layer of resilient, intelligent industrial systems.

While the journey is complex, leaders remain resolute. By scaling next-generation technologies, hardwiring security into the core and aligning governance to the new operating reality, they are positioning their organizations not merely to navigate the transition, but to emerge stronger and more resilient.

Key observations

Trends

55%

Of organizations have seen **OT budget growth** in the past two years. [1]

Importance of the human factor

The human factor plays a crucial role in the successful adoption and efficient use of new technologies. Being open to these innovations and understanding how to work effectively with them is essential.

Asset discovery

Automation and AI: Enhancing accuracy and efficiency in asset discovery.

Cloud adoption: Tools evolving to manage cloud resources.

Real-time monitoring: Increasing demand for quick response to changes and threats.

Innovations

Digital Twins for network optimization

E.ON has successfully implemented a digital twin for its extensive **700,000 km grid in Germany.**

Investment in generative AI

69% **of surveyed CEOs** have identified investment in generative AI as one of their top priorities.

Emerging technologies

- Artificial Intelligence
- Edge computing
- Blockchain
- Quantum computing
- Digital Twins
- 5G

OT cybersecurity innovations

- Zero Trust for OT environments
- AI-driven OT threat detection
- OT-integrated SOC and XDR
- Continuous OT asset and vulnerability monitoring

Security challenges

50% OT and ICS decision-makers identify **legacy systems as major obstacles.**

Integration of advanced technologies

Organizations are increasingly integrating advanced technologies like AI, 5G, and digital twins to enhance efficiency and innovation.

Supply chain vulnerabilities

The convergence of IT and OT expands the attack surface, exposing systems to IT-borne threats with potential for physical damage and widespread disruption. Ensuring robust security measures across both domains is essential.

99% Number of healthcare organizations operating devices with known exploited vulnerabilities.

Regulatory

Global variability

Diverse legal frameworks and industry standards across regions.

Enhanced legislation

New directives impose rigorous requirements.

Interoperability gaps

Rapid innovation outpaces standardization.

Regulatory pressure and growing board-level interest

52% Of organizations have their responsibility of OT security under the CISO up from 16% in 2022.

98% nearly every company now includes the OT cybersecurity profile in general risk assessments for management and the board.

Integrated methodology for OT insights

The KPMG OT Outlook employs a comprehensive analytical approach, integrating both external and internal factors to provide a strategic perspective. This methodology is designed to ensure a well-rounded strategic outlook, essential for future readiness.

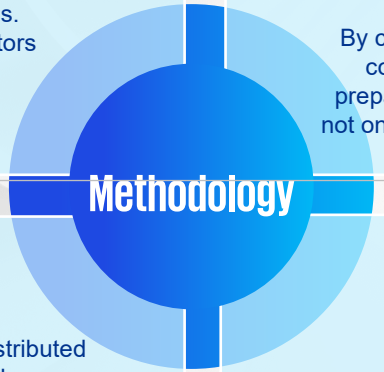
External analysis

Our methodology commences with a detailed SWOT analysis, placing particular focus on *threats* and *opportunities* that are instrumental in shaping the operational technology environment. This analysis is enhanced by the application of an expanded PESTLE framework, known as PESTLIM, which introduces industry and military dimensions. Collectively, these frameworks help us understand the broader environmental factors influencing OT across various sectors.

Vendor input

To further enhance our analysis, we have also sent out questionnaires to international leading vendors. The input from these vendors provides valuable perspectives on industry trends, challenges, and innovations, adding depth to our strategic outlook.

By combining these external and internal analysis, the KPMG OT Outlook offers a comprehensive view that is crucial for understanding the current landscape and preparing for future developments. This methodology ensures that our insights are not only thorough but also actionable, helping businesses navigate the complexities of operational technology with confidence.



Internal insights

Our approach is enriched by insights gathered through detailed questionnaires distributed to OT experts and global KPMG leaders. These questionnaires target sectors such as automotive, transportation and infrastructure, industrial manufacturing, energy, and healthcare, spanning regions including EMEA, APAC, and the Americas.

Industry input

As part of our comprehensive approach, the Outlook draws on expert perspectives from leading industrial organizations. Their contributions, grounded in extensive OT operations and transformation programs, provide real-world validation of the Outlook's findings and shed light on sector-specific innovation priorities, investment trends, and governance developments shaping the OT landscape.

Leading regions across sector

Global innovation and digital transformation are reshaping industries worldwide, with countries and regions accelerating progress in advanced technologies, automation, and next-generation infrastructure. Below are some of the leading regions driving this transformation.

USA

Rapid EV market growth with strong policy support: The US is home to Silicon Valley, a major center for tech innovation, including digital health startups.

Tech innovation and autonomous leadership: Extensive use of AI and big data analytics in healthcare for predictive modeling and personalized medicine.

Asia

EV Sales: 8.1 M China's electric car sales hit 8.1 million in 2023 – more than one in three new cars – making Asia the global EV leader.

Auto Exports: 4 M
China became the world's top auto exporter in 2023, shipping 4 million vehicles abroad (including 1.2 million EVs).

Europe

~30% of global industrial automation installations, reflecting Europe's leadership in advanced manufacturing, infrastructure modernization, and technology adoption across sectors.

Strong regulatory and policy harmonization, enabling scalable digital transformation, sustainability, and cross-border integration.

Australia

~49% of global lithium production, positioning Australia as a **strategic supplier** of critical minerals that enable advanced technologies and industrial value chains worldwide.

National focus on infrastructure and resilience, supporting long-term digital and industrial transformation across sectors.

Cross-sector insights

Global cloud adoption trends

21.2%

compound annual growth rate from 2025 to 2034

According to Precedence Research, the global cloud computing market growth rate is expanding. This growth is driven by the following factors.

Scalability and efficiency: Cloud solutions offer scalable resources and efficient management, which are attractive to businesses looking to optimize operations and reduce costs.

Innovation and flexibility: The ability to quickly deploy new applications and services in the cloud supports innovation and flexibility, allowing companies to adapt to changing market demands.

Security and compliance: As regulatory requirements become more stringent, cloud providers are enhancing their security measures to ensure compliance, making cloud adoption more appealing to organizations in regulated industries.

Integration of IoT and cloud platforms

The integration of IoT technologies and cloud platforms is fundamentally changing operational environments. This shift moves beyond isolated SCADA systems to interconnected networks, increasing vulnerability to external risks. IoT devices are often linked to cloud environments, whether through public providers like AWS or Azure or private setups. While cloud adoption boosts efficiency and scalability, it also expands the attack surface, introducing new threat vectors.

Use of AI and ML in Cybersecurity

AI and machine learning (ML) are becoming central to cybersecurity strategies. For defense, **AI enhances anomaly detection, predictive analytics, and automated threat mitigation**, enabling real-time monitoring and rapid response.

Asset discovery and visibility

Asset discovery is a critical component of OT cybersecurity, requiring both automated and manual methods to ensure comprehensive visibility. Across various regions, organizational culture and resistance to change are common barriers to adopting new technologies, emphasizing the need for strategic asset discovery. Here are examples of how different regions approach asset discovery:

Australia: Regulatory requirements continue to drive cybersecurity improvements. There is significant focus on asset discovery and vulnerability management driven by cybersecurity frameworks and regulatory requirements for reporting and resilience. Maturity varies by sector, and many challenges remain due to legacy systems and resource constraints.

Saudi Arabia: While advanced technologies are deployed for asset discovery, many assets remain off the radar. Conventional methods continue to be essential to overcome this, and without a cultural shift, the reliance on outdated infrastructure will remain the status quo.

> One of the key challenges in OT is the significantly longer life cycle of the physical part of the systems – often spanning several decades – compared to IT-based control and automation components. As a result, these IT components reach end-of-life much sooner, with manufacturers ceasing to provide updates and patches. The increasing complexity of modern OT environments, driven by the integration of IT technologies and replacing older proprietary bus systems, introduces unpredictable risks for the future. This presents a major challenge for both plant operators and manufacturers, who must ensure that software updates and, where necessary, adaptations to new operating system versions are supported over a period of 20 years or more.

Markus Schumburg
Group CISO – Germany
DHL

Semiconductor dependency and resilience

~2×

Expected growth in demand for power semiconductors by 2030

Semiconductors have become a critical dependency for OT environments, enabling industrial control systems, sensors, edge computing, and advanced automation. Growing reliance on specialized and power-efficient chips is reshaping OT performance, resilience, and digitalization across critical infrastructure sectors.

At the same time, **global supply-chain concentration and geopolitical pressures** have elevated semiconductors from a procurement issue to **a strategic OT risk**, with disruptions directly **impacting OT asset availability, lifecycle management, and operational continuity**.

Importance of human factors

Despite technological advancements, the human factor remains crucial for cybersecurity. Training and security awareness are important across all sectors to empower employees to recognize and respond to threats effectively. Human factors play a pivotal role in several areas:

Employee training: Regular training programs are essential to equip staff with the knowledge and skills needed to recognize and respond to cyber threats effectively.

Security awareness: Cultivating a culture of security awareness helps employees understand the importance of cybersecurity measures and their role in maintaining them.

Behavioral analysis: AI models can enhance identity authentication and resilience against spoofing by assessing behavioral patterns, but human oversight is crucial to interpret and act on these insights.

Incident Response: Human judgment is vital in incident response scenarios, where quick decision-making can mitigate the impact of a breach.

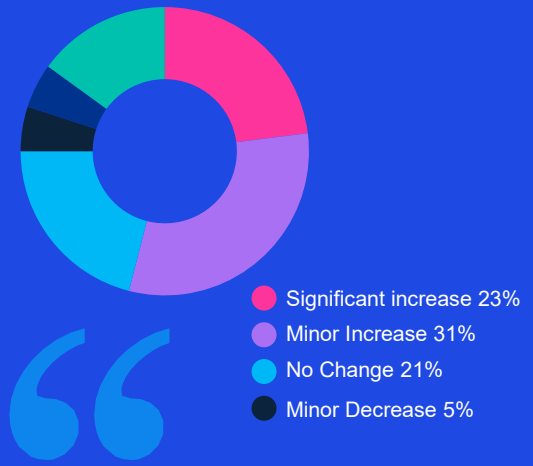
Business and regulatory impact

The focus on ROI for security spending highlights OT security as a business enabler. Regulatory efforts like the NIS2 Directive further drive investment growth. A recent survey involving over 180 professionals from various critical infrastructure sectors worldwide revealed that 55% of organizations have seen OT budget increases in the past two years. This trend reflects a growing executive-level understanding of OT risks, influenced by:

Internal risk awareness: Recognizing the importance of OT security.

External market pressure: Responding to demands from insurance carriers and other stakeholders.

Change in the OT budget from organizations over the last two years



OT security is no longer a topic for the future - it's critically important today. A single attack can halt production for weeks or months, resulting in millions in damages.

Thomas Gronenwald
Partner, Product (CRA) and Production (OT) Cybersecurity and Resilience
KPMG Germany

OT trends in automotive

The automotive industry is currently undergoing a comprehensive digital transformation. This is being driven by the integration of advanced technologies. According to the *State of Smart Manufacturing: Automotive Edition* report published in 2024, at least 81% of respondents stated that they had already introduced network hardware, industrial computers and networked devices, including sensors and actuators, or were planning to introduce them in the next few years. The automotive sector is at the forefront of several significant OT trends driven by increasing digitalization, automation, and connectivity in both vehicle production and operation:

IT/OT convergence

The traditional separation of IT (information systems like ERP, cloud, network) and OT (machines, robots, production lines) is increasingly being dissolved. This interconnectedness enables greater efficiency, real-time data analysis, and automation in automotive production and vehicle operation.

> In OT, the objective is not to see everything, but to protect what matters most in the physical world. Security must follow the process, not the inventory.
>
> **Antoine d'Haussy**
>
> Head – OT Cybersecurity EMEA
>
> FORTINET

Industry 4.0 & Smart Factory

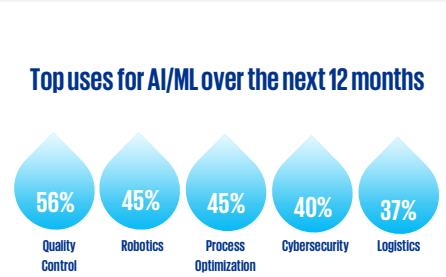
Automated production, cyber-physical systems, and IoT-enabled machines are making automotive manufacturing smarter. For example, robots on the production line automatically exchange data with central control systems, significantly improving the efficiency and precision of manufacturing processes.

Edge computing in production

Data is processed directly at the machine or in the vehicle ("at the edge" of the network). This enables real-time analysis, low latency, and reduces data traffic to the cloud, which is crucial for applications like predictive maintenance and autonomous driving functions.

AI and machine learning

AI and ML are used in the automotive sector to optimize processes, for example, for predictive maintenance of production facilities or to optimize manufacturing processes and improve the driving experience through data analysis.



Source: https://www.rockwellautomation.com/en-us/industries/automotive-tire/technology-challenges/State-of-Smart-Manufacturing-Report-Automotive-Edition.html

OT trends in healthcare

The healthcare sector is rapidly evolving, driven by the need for improved efficiency, enhanced patient care, and cost reduction. This transformation is characterized by several key drivers and strategic approaches that are reshaping the industry.

Key drivers of transformation

Digitalization and automation: Emphasizing interoperability to streamline operations and improve patient outcomes. This includes the integration of IoMT devices and network-capable medical-grade devices such as insulin pumps, CT scanners, and ECG monitors. These devices enable real-time data collection and analysis, improving patient outcomes and operational efficiency.

Advanced threat detection and response: Leveraging national cybersecurity strategies to implement sophisticated threat detection and response mechanisms.

Openness to new technologies: Facilitating rapid pilot projects and digital health transformation, including edge computing for real-time, decentralized threat response in clinical environments and AI and IoMT integration. For example, the UAE has successfully conducted surgical procedures using AI and robotics, showcasing the potential for advanced medical procedures and improved patient care.

Strategic approaches

AI-driven diagnostics and anomaly detection: Utilizing AI-based anomaly detection for proactive threat mitigation enhances security and operational efficiency. In healthcare, AI-driven diagnostics can identify irregularities in patient data, allowing for early intervention and improved patient care outcomes.

Regulatory compliance and frameworks: Strong frameworks like GDPR, NIS2, and MDR accelerate the adoption of secure digital health innovations, ensuring compliance and safety. Healthcare organizations must navigate these complex regulations to protect sensitive patient information and maintain operational integrity.

Integration of IoMT and edge computing: The integration of IoMT devices and edge computing allows for real-time data processing and decentralized threat response, enhancing the ability to manage and secure medical devices and patient data in clinical environments.

Current and planned implementation of AI for clinical decision support

	AI has already been implemented	Plan to implement AI in the next three years	%* Not implemented or don't know
In-hospital patient monitoring	43	31	26
Medication management	37	37	25
Treatment planning	37	35	28
Radiology	36	35	29
Preventive care	36	36	28
Pathology	35	33	33
Remote patient monitoring	33	41	26
Clinical command centres	32	37	32

*Due to rounding, totals may add to more or less than 100%

Source: Philips Future Heath Index 2024 with responses from almost 3000 healthcare leader across 14 countries around the world

OT trends in industrial manufacturing

Digital health transformation is a global phenomenon, with several countries and regions taking significant strides in integrating technology into healthcare. Here are some of the key players:

Smart factories

Siemens: At the Amberg Electronics Plant, Siemens uses automation, robotics, and digital twins to streamline production, automate 75% of the supply chain, and achieve a 99.9% quality standard.

Bosch: Bosch's factory uses digital twins and the Nexeed software suite to connect sensors, boosting production efficiency by 25% and reducing costs by up to 50%.

Source: https://www.cyngn.com/blog/smart-manufacturing-the-future-of-smart-factories

AI-powered security

Rockwell Automation: Rockwell Automation's FactoryTalk Analytics platform uses AI to detect anomalies in network traffic, enhancing cybersecurity.

Honeywell: Honeywell's cybersecurity solutions for industrial environments use AI to identify and mitigate potential security risks.

Predictive maintenance

SKF: SKF's Enlight AI system monitors bearing health and predicts maintenance needs, reducing unexpected breakdowns.

Caterpillar: Caterpillar's "Cat Connect" technology employs machine learning to predict equipment failures and optimize service schedules.

Energy efficiency and sustainability

Schneider Electric: Schneider Electric provides energy management solutions that help industrial facilities reduce their carbon footprint.

ABB: ABB's energy-efficient motors and drives are used in industrial applications to improve sustainability.

> OT security is not just about technology - it's about people, processes, and precision. As a Chief Operations Security Officer, I believe that resilient industrial infrastructure depends on clear responsibilities, well-defined procedures, and seamless collaboration between IT, OT, and production. Tools like IDS, asset and vulnerability management, or OT-SOCs only deliver value when they are understood and embedded into operational workflows. As we often say: *A fool with a tool is still a fool.* Security must be applied with expertise, accountability, and continuous testing to be effective in real-world scenarios.

Georgios Spyros
Chief Operations Security Officer
ALTANA

OT trends in transportation and infrastructure

Increasing Digitization and Connectivity
The transportation and infrastructure sectors are crucial for national security, economic stability, and public safety, making them prime targets for cyberattacks. The digitization and interconnectedness of systems like roads, bridges, airports, seaports, and railways expose them to risks from geopolitical actors and hacktivism. As these sectors evolve into complex cyber-physical systems, integrating Industrial Internet of Things (IIoT) and OT, the challenge of securing them becomes increasingly intricate. The risk posed by cyber threats often surpasses traditional safety concerns, highlighting the need for a comprehensive approach to security. Cyberattacks can lead to severe disruptions, economic losses, and threats to human life, underscoring the importance of addressing these vulnerabilities with innovative and robust security measures.

Rise in OT Dependence
The transportation sector is increasingly reliant on OT. Businesses are connecting OT infrastructure, such as SCADA systems, with IT networks to boost efficiency and profitability. However, this convergence increases risks as the "air gap" between OT and IT diminishes, making OT systems vulnerable to traditional IT threats.

Key trends in sub-sectors

Road transportation
Smart Infrastructure and Digital Twins: The use of digital twins and smart technologies is revolutionizing transportation infrastructure management, optimizing asset performance and urban services.

Rail transportation
Automation and AI: Robotics and AI are enhancing efficiency and safety in rail transportation, with autonomous systems handling maintenance and inspections.

Aviation
Remote Digital Towers: Innovations like the remote digital tower at London City Airport are enhancing operational efficiency and safety, allowing air traffic controllers to manage flights from a distance using high-definition cameras and sensors.

Maritime transportation
Autonomous Ships: The maritime sector is experiencing growth driven by AI/ML integration for navigation and control systems, with autonomous ships offering efficiency and safety benefits.

Logistics and supply chains
Automated Supply Chains: Blockchain and cloud-hosted platforms are enhancing tracking and efficiency in logistics operations, with smart warehouses leveraging IoT and automation to optimize processes.

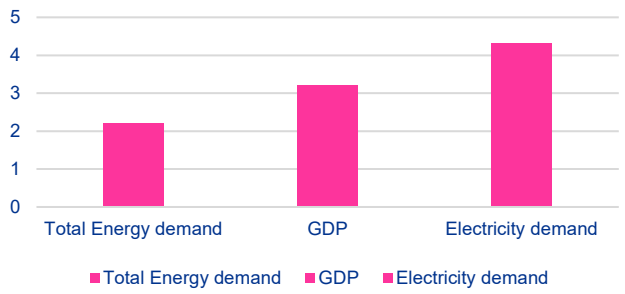
Urban mobility and smart cities
Intelligent Transportation Systems (ITS): Deployment of ITS is minimizing traffic congestion and enhancing urban mobility, with the global ITS market projected to grow significantly, driven by government funding and collaboration with private partners.

OT trends in energy

Growth and demand dynamics

Global energy demand: In 2024, global energy demand grew by 2.2%, faster than the previous decade's average of 1.3%. Notably, electricity demand grew by 4.3%, reflecting the sector's shift towards electrification. Despite this, overall energy demand lagged behind the global economy's 3.2% growth rate.
Global investment: Globally, there is a significant investment of US$ 3.3 trillion in the energy sector.
Age of electricity: Investment trends are being shaped by the onset of the 'Age of Electricity' and the rapid rise in electricity demand for industry, cooling, electric mobility, data centers, and AI. Investment in the electricity sector is set to reach US$1.5 trillion in 2025, 50% higher than the total amount being spent on bringing oil, natural gas, and coal to market.

Key global growth rates by source, 2024



Impact of electrification and renewables

Smart grid solutions: The shift towards electrification and renewable energy sources is significantly impacting grid operations. Smart grids are at the forefront of this transformation, integrating modern technologies like sensors, smart meters, cyber-physical systems, and IoT devices. These systems enhance energy efficiency, manage resources effectively, and support sustainability, facilitating eco-friendly systems with low carbon emissions.
Renewable energy goals: The global energy landscape is actively shifting from fossil fuels to renewable sources. Solar investment is leading this change, with spending on low-emissions power generation nearly doubling over the past five years.

Regional insights

- World energy consumption is projected to increase almost 50% from 2020 levels by 2050.
- EU Electricity Generation: The EU generates 2,572 TWh of electricity.
- Saudi-Arabia: Saudi-Arabia is investing US$ 8.3 billion to 15 GW Renewable Energy Projects by 2028.
- USA: US$ 300 billion clean energy investment in 2023.

Source: https://www.iea.org/reports/global-energy-review-2025

"As the energy sector faces surging demand, a new wave of regulatory scrutiny, and escalating cyber threats, companies are turning to technological solutions as force-multipliers for small OT cybersecurity teams. Energy leaders have a generational opportunity to build new infrastructure that is secure by design, with continuous monitoring and visibility across digital and physical systems, and better planning for updates as digital innovation continues. My company like many others using AI to enhance automation and big data analysis, with promising results for both security and performance.

Leo Simonovich
Vice President and Global Head, Industrial Cyber and Digital Security – USA
SIEMENS energy

Recap of OT trends

The chapter on trends in OT provides a comprehensive look at the transformative changes across various sectors, driven by rapid technological advancements and growing interconnectivity. In the automotive industry, the shift towards electrification and autonomy requires smarter and more connected OT systems, with edge computing playing a crucial role. Healthcare is rapidly evolving with digital health technologies improving patient care and operational efficiency, while industrial manufacturing is embracing smart factories and automation to optimize production and sustainability. Transportation and infrastructure are modernizing with smart technologies, improving efficiency and safety. Finally, the energy sector is focusing on sustainable solutions, with significant investments in renewable energy sources like solar and wind power. As these renewables, including small-scale installations like balcony photovoltaics, contribute to the grid, the risk of overloading increases. Smart grid technologies are being implemented as a solution to manage this complexity, ensuring resilience and efficiency. However, these advancements also introduce new attack surfaces, necessitating robust cybersecurity measures to protect against potential threats.

Understanding current trends sets the stage for innovation in various industries. The energy sector, with AI-driven digital twins, and increasing use in operations, illustrates how systems can be redefined, pointing towards a heavier technical ecosystem and resilient future.

> The potential of AI is shifting left the capabilities for incident response driving automation in cyber response, with faster real-time analysis and organizational interspersion of AI agents, the only constant will be a continual evolution as Agentic AI adoption accelerates.

Jason Haward-Grau,
Lead for Energy, Natural Resources and Chemicals and Incident Response and Recovery
KPMG in the US

Cross-sector insights into emerging technologies

As we transition from exploring trends to delving into innovations in OT, our outlook highlights a pivotal transformation driven by emerging technologies across sectors.

	AI	Digital Twins	Edge computing	Blockchain	5G	Quantum computing
Description	Serves as a universal engine for increasing efficiency and creating new, data-driven services.	Acts as a strategic tool to secure innovations and systems in a safe, virtual space.	Shifts data processing from the central cloud to the "edge" of the network, directly to the data source.	Creating a "Trust Layer" through transparent and tamper-proof supply chains and transaction logs.	Functions as the nervous system of digitalization, providing the foundation for real-time connection of billions of devices.	Poses a long-term threat to all established encryption standards (e.g., RSA, ECC).
Prominent use cases	AI-powered diagnostics in healthcare, predictive maintenance in manufacturing, automated threat detection in automotive.	Testing AI implementations, optimizing operational processes, simulating resilience against cyber-attacks before physical systems are affected.	Supports real-time applications, decentralized intelligence for IoT, autonomous systems.	Ensures transparent supply chains, tamper-proof transaction logs.	Enables telesurgery, autonomous driving (V2X), connected manufacturing (IIoT).	Cryptography, optimization problems in logistics and finance, drug discovery in healthcare.
Challenge	Complexity of algorithms and potential new attack vectors, such as Adversarial AI.	Ensuring accurate representation and integration with real-world systems.	Balancing data processing efficiency with security and privacy concerns.	Faces regulatory uncertainty and high implementation costs.	Managing network security and ensuring reliable connectivity in diverse environments.	Migration to Post-Quantum Cryptography (PQC) is inevitable but complex, especially for long-lifecycle systems in critical infrastructure.

> The future of energy lies in embracing emerging technologies that bring our operations closer to real time, whether it's predictive insights through AI, connected assets through 5G, or the immersive simulations of digital twins. These tools unlock enormous value, yet they also expose us to new risks at the intersection of IT and OT. Our responsibility as leaders is to ensure that innovation and protection move forward hand in hand.

Saeed AlSaeed
CEO

Cyberani by aramco digital

Innovation in automotive

As the automotive industry accelerates toward electrification, autonomy, and software-defined vehicles, OT is undergoing a profound transformation. No longer isolated, OT systems are becoming smarter, more connected, and more secure blurring the lines between the physical and digital worlds of production.

Automated production and cyber-physical systems

IoT-enabled machines: The integration of IoT devices in manufacturing processes allows machines to communicate and coordinate with each other and central control systems. This connectivity enhances the precision and efficiency of production lines, enabling real-time adjustments and optimizations.

Cyber-physical systems: These systems combine physical processes with digital control, creating a seamless interaction between machinery and software. In automotive manufacturing, cyber-physical systems facilitate automated decision-making and process optimization, reducing human intervention and increasing production speed and accuracy.

Smart factory implementation

Digital Twins: The use of digital twins in automotive manufacturing allows for virtual simulations of production processes. These digital replicas help manufacturers test changes and optimize operations without disrupting actual production, accelerating time-to-market for new vehicle models.

Automation and robotics: Smart factories employ advanced robotics and automation technologies to streamline production. Robots equipped with sensors and AI capabilities can perform complex tasks with high precision, reducing errors and increasing output.

Vehicle innovations

Autonomous driving: The development of autonomous vehicles is rapidly advancing, with AI and machine learning driving capabilities that allow vehicles to operate without human intervention. This innovation is transforming transportation, offering enhanced safety and efficiency.

Over-the-air (OTA) updates: OTA updates are becoming standard in modern vehicles, allowing manufacturers to remotely update software and improve vehicle functionality without requiring physical intervention. This capability enhances vehicle performance and security.

Connected vehicles: The integration of advanced connectivity solutions enables vehicles to communicate with each other and infrastructure, supporting features like real-time traffic updates and enhanced navigation systems.

Regional insights

Europe: The German automotive industry faces competition from Asian manufacturers who have embraced innovation, particularly in electric vehicles and automated systems. This highlights the need for European industries to adapt to rapid technological advancements to remain competitive.

India: Strong R&D capabilities enable OEMs and Tier-1 suppliers to embed cybersecurity throughout the vehicle lifecycle, including secure architectures and OTA updates. AI models enhance identity authentication and resilience against spoofing, aligning with global standards like ISA/SAE 21434.

Innovation in healthcare

As healthcare embraces AI, connected devices, and advanced medical technologies, OT is transforming rapidly. Systems that were once isolated are becoming smarter, more integrated, and more secure—driving new levels of efficiency, safety, and quality in patient care.

The role of OT in healthcare

OT in healthcare **is critical**, encompassing from basic patient monitoring tools to sophisticated diagnostic devices like MRI and CT scanners. These technologies are integral to patient care and clinical outcomes, ensuring the smooth operation of healthcare facilities.

Innovation in healthcare

Healthcare is experiencing a transformative wave of innovation across multiple domains:

- **Telemedicine and AI:** Revolutionizing remote care and diagnostics, enabling personalized treatment plans.
- **Wearable devices and IoT:** Enhancing patient monitoring and data collection, leading to more informed healthcare decisions.
- **3D printing and robotics:** Innovating surgical procedures and prosthetics, offering customized solutions for patients.
- **Blockchain and nanomedicine:** Ensuring data integrity and advancing medical research, providing new avenues for treatment.
- **Advanced medical devices and IoMT:** Integrating cutting-edge technologies to improve healthcare delivery and efficiency.

Challenges in healthcare innovation

Despite rapid progress, new challenges arise:

- **Data security and privacy:** Protecting sensitive patient information amidst increasing digitalization.
- **Regulatory compliance:** Navigating complex regulations like MDR, HIPAA, and NIS2.
- **Ethical considerations:** Addressing concerns in AI-driven diagnostics and treatment.
- **Secure medical IoT and edge computing:** Ensuring robust security for interconnected devices and systems.

Innovation in industrial manufacturing

Current landscape

69%

of 175 worldwide surveyed CEOs said that investment in generative AI is at the very top of their company's investment priorities. To redesign their processes, rethink client experiences and interactions, and ultimately increase efficiency and agility.*

Industrial manufacturers are at a critical inflection point. With supply chain pressures easing and digital infrastructure maturing, the opportunity to transform OT environments is both real and necessary. However, manufacturers face challenges in adopting new technologies for early risk detection, including:

Legacy systems: High integration costs and complexity in aligning cybersecurity controls with operational uptime.

Early detection and risk management: Integrating predictive analytics with legacy OT systems while maintaining operational continuity.

AI integration and cybersecurity: As AI-driven production systems are embraced, cybersecurity becomes paramount. The convergence of IT and OT creates new attack vectors, requiring sophisticated security frameworks

*Source: https://hub.kpmg.de/en/global-industrial-manufacturing-ceo-outlook-2024

Regional insights

- **Saudi Arabia**: Advanced technologies are used for asset discovery, but many assets remain outside the network due to lack of networking capabilities. Manual methods are still necessary for discovering non-networked assets.
- **Spain**: Focuses on OT security assessments, governance models, and network segmentation for asset discovery and classification, following models like ISA/IEC 62443.
- **India**: AI technologies expand the attack surface by requiring connectivity to cloud platforms and external data sources. Legacy systems often lack secure interfaces, and AI models depend on high-quality data, which is often fragmented.
- **Germany**: AI acts as a virtual security employee, automating routine tasks and enhancing team efficiency. It provides transparency on critical IT and OT components through machine communication. The integration of AI technologies introduces new cybersecurity risks but also enhances control capabilities, enabling advanced anomaly detection and automated threat response.

> AI is the driving force behind the manufacturing industry – with clear guidelines and well-trained employees, its full potential can be realized.

Serjoscha Keck
Partner, Head of Industrial Manufacturing
KPMG Germany

Innovation in transportation and infrastructure

The transportation and infrastructure sector is undergoing a significant transformation, driven by innovation that extends beyond digitalization. This evolution is reshaping how goods and people move across cities, regions, and continents, emphasizing efficiency, sustainability, and enhanced safety.

Digitalization and advanced connectivity

The transportation industry's reliance on digital systems is a primary driver of innovation. This includes connected vehicles, smart warehouses, and automated supply chains, aimed at boosting operational efficiency and profitability. The diminishing "air gap" between OT and IT networks leads to integrated systems enabling real-time data analysis and automation.

Automation and AI

Automation and AI drive efficiency and safety in transportation. Autonomous Vehicles are evolving rapidly, capable of operating without human intervention, including freight transport trucks. The autonomous ships market is growing, driven by AI/ML integration for navigation and control systems. Robotics in rail handle maintenance and inspections, improving precision and safety.

Key areas of Innovation

Smart infrastructure and Digital Twins

Smart infrastructure leverages digital technologies to enhance urban services and optimize asset performance. Digital Twins create virtual replicas of physical assets like roads, bridges, tunnels, and airports, revolutionizing Transportation Infrastructure Management.

Sustainable transportation innovation

Sustainability is a key focus, with efforts to reduce carbon footprints and promote environmental responsibility. Electric Mobility is expanding, driven by government incentives and decreasing battery costs. Green Infrastructure investments aim to manage environmental challenges, contributing to improved air quality and biodiversity.

Regional insights

Germany: The integration of IoT sensors and edge devices for real-time asset monitoring is combined with predictive analytics and machine learning to identify anomalies early. Digital twins enable continuous simulation and issue detection, while integrated SCADA and ICS monitoring tools track operational deviations. SIEM systems aggregate data from IT and OT for prompt incident detection, supported by automated alerting and response platforms to ensure rapid reaction.

India: The integration of early detection technologies like Cylus, ETAS/Escrypt, Nozomi, and Device Authority is crucial for identifying disruptions. However, challenges persist in adapting these technologies to vehicle form factors and communicating the value of security investments to consumers. Additionally, the sector faces hurdles in merging new technologies with legacy systems, especially in continuously mobile assets like cars, trains, and ships.

Innovation in energy

The energy sector is undergoing a profound transformation, driven by the imperative for sustainability, resilience, and efficiency. OT stands at the core of this evolution, serving as the critical infrastructure that monitors and controls physical processes within energy systems. As utilities strive to keep pace with digital transformation, the market for energy OT cybersecurity solutions is projected to grow significantly from US$1.5 billion in 2024 to US$3.1 billion in 2033, at a compound annual growth rate of 8.1% [1]. This growth underscores the increasing importance of robust cybersecurity measures in safeguarding energy systems.

Keys areas of innovation in energy OT

Smart grids and renewable energy integration

Smart grids represent a cutting-edge advancement in electrical power systems, designed to maximize energy efficiency, manage resources effectively, and enhance reliability and sustainability. These systems integrate modern technologies like sensors, smart meters, cyber-physical systems (CPSs), and IoT devices, all interconnected via robust communication networks. A primary benefit is their ability to improve energy management and grid resilience, facilitating eco-friendly systems with low carbon emissions.

Digital Twins for network optimization

Digital twins are sophisticated virtual replicas of physical plants, processes, or systems, providing a comprehensive, real-time view of energy flow and consumption patterns. They allow operators to simulate scenarios, perform diagnostics, and optimize strategies without disrupting operations. For example, E.ON has implemented a digital twin for its 700,000 km grid in Germany, using technology from smart grid software subsidiary envelio [2]. This digital twin evaluates data from millions of network components and measuring devices, enabling rapid processing of grid connection requests and identifying urgent grid expansion needs. The TwinEU project is a key initiative in Europe, aiming to create a federated ecosystem of digital twins to enhance infrastructure resilience and cost-effectiveness across the continent [3].

AI-driven network operations and resilience

AI and machine learning (ML) are crucial for optimizing smart grid operations, enabling real-time monitoring, sophisticated analysis, and precise control of energy systems. Applications include improving short-term load forecasting, optimizing generation planning, and managing variable renewable resources. AI can autonomously detect and isolate faults, reconfigure energy flows, and restore supply in real time, significantly enhancing grid resilience and reliability. The ENTSO-E-DSO Entity joint task force is developing a digital twin of the EU electricity system, focusing on AI-driven solutions to address real-world challenges and improve operational strategies.

OT = Obsolete Technology
mostly, relies heavily on compensating controls in IT components. Control IT, Secure OT (CISO)

Paul Schneider
Global OT Security Leader – Netherlands

Shell

Recap of innovation research

> *"Innovation research **has opened up new technological possibilities**, but it also brings to light the security challenges associated with OT."*

The chapter on innovation delves into how emerging technologies are reshaping various industries, focusing on the integration of AI, digital twins, and cybersecurity measures. Across sectors, AI and digital twins are pivotal in enhancing efficiency and innovation, enabling predictive analytics, optimizing production processes, and facilitating real-time data processing.

In the automotive sector, the shift towards electrification and autonomy necessitates smarter and more connected OT systems, with digital twins and edge computing playing crucial roles in flexible manufacturing and real-time data processing, enhancing resilience and cybersecurity.

Healthcare is experiencing a transformative wave of innovation, with telemedicine and AI revolutionizing remote care and diagnostics, wearable devices enhancing patient monitoring, and 3D printing innovating surgical procedures. Despite rapid progress, challenges such as data security, regulatory compliance, and ethical considerations persist.

In industrial manufacturing, AI-driven production systems are transforming processes but also introduce new cybersecurity risks, requiring sophisticated security frameworks to protect against emerging threats. The transportation and infrastructure sectors are modernizing with smart technologies, improving efficiency and safety, while the energy sector focuses on sustainable solutions, with significant investments in renewable energy and smart grid technologies driving resilience and efficiency.

Innovation research has opened up new technological possibilities, but it also brings to light the security challenges associated with OT. As industries embrace increased interconnectivity and technological integration, the convergence of IT and OT expands the attack surface for critical infrastructure. This exposes systems to IT-borne threats with the potential for physical damage and widespread disruption. Ensuring robust security measures across both domains is essential to safeguard operational continuity and resilience. This chapter will delve into the cybersecurity threats and regulatory pressures that industries face as they adopt these emerging technologies, highlighting the importance of understanding OT risks to maintain a secure and resilient operational environment.

> Taking care of a better climate starts with secure operations. At Vaillant, OT security is built on people and trust. Through active community engagement and transparent governance, we create resilience, uphold compliance, and enable innovation – delivering smarter, sustainable heating solutions for the future.

Raphael Reiss
Head of Group Information Security Germany
VAILLANT GROUP

Security challenges across sectors

Legacy systems and infrastructure

Many industries rely on outdated OT systems that lack modern security features. These legacy systems are often unpatchable, making them vulnerable to cyber-attacks. The challenge lies in modernizing these systems without disrupting operations, which requires significant investment and strategic planning.

Supply chain vulnerabilities

Insecure Tier 1 and Tier 2 suppliers pose significant risks, as they can introduce vulnerabilities through outdated components and insufficient security measures. Ensuring secure procurement and supply chain management is critical to reducing these risks.

Integration of advanced technologies

Digital transformation introduces a security paradox, as existing OT systems weren't designed with modern cybersecurity in mind, amplifying vulnerabilities. To address this, organizations must adopt a "Secure by Design" approach, embedding security measures from the outset to ensure new technologies are inherently secure and resilient against threats.

Workforce skill gaps

A shortage of skilled cybersecurity personnel is a common challenge across sectors. This gap affects the ability to monitor and protect OT environments effectively, necessitating increased investment in workforce training and retention.

Regulatory compliance

Stricter regulations such as ISA/SAE 21434, NIS2 Directive, and GDPR impose rigorous cybersecurity requirements. Ensuring compliance across diverse and complex OT environments is challenging, especially for small and medium enterprises (SMEs) that may lack the resources to implement comprehensive security measures.

Security challenges across sectors

In your opinion, what are the most important challenges in the field of OT security and how can they be addressed?

Majida Dere
Director- OT Security Management
Germany
WEST FLEISCH

Food stays safe when lines stay secure. In food production, uptime protects freshness and trust, so OT security must be a hygiene factor: quiet, constant, and effective. The playbook is simple: see first, then segment; model IEC 62443 aligned zones and conduits; enforce allow-listed, purpose-bound communication. Integrate legacy via secure gateways, not broad exceptions. Vendor access is MFA-protected, time-boxed, and audited. With continuous monitoring, testing, and periodic recertification, controls work on real lines - delivering measurable risk reduction without breaking the line rhythm.

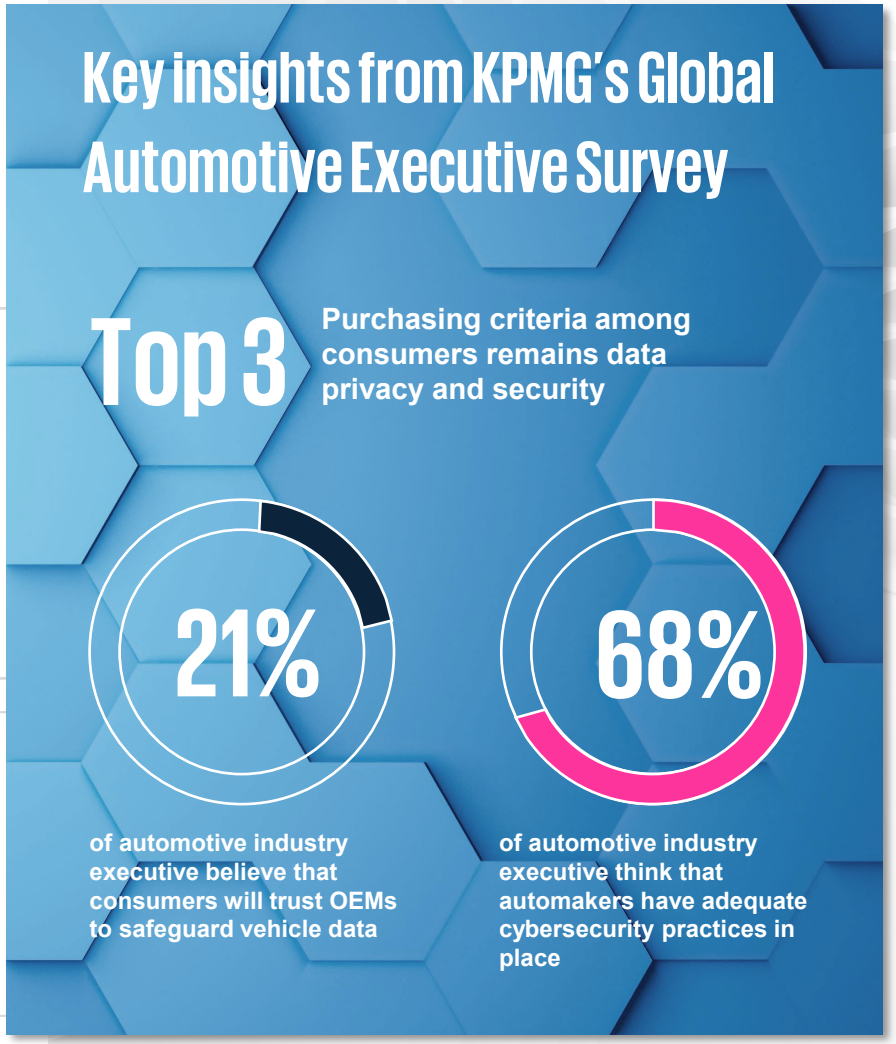
Security challenges in automotive

Surge in cybersecurity threats

As electric, autonomous, and connected vehicles become more prevalent, the automotive industry faces a significant surge in cybersecurity threats. Modern cars operate using approximately 100 million lines of code, enabling advanced functionalities such as intrusion detection, anomaly recognition, communication protocols, and over-the-air (OTA) updates. However, these digital innovations introduce vulnerabilities, making vehicles susceptible to unauthorized data access, cyber intrusions, and breaches in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, as well as telematics systems.

Impact on consumer trust

Data security and consumer privacy are increasingly influencing purchasing behavior and brand trust. According to KPMG's 24th Annual Global Automotive Executive Survey, only 21 percent of industry executives (down from 40 percent the previous year) believe that consumers trust OEMs to protect vehicle data. This underscores a growing responsibility for automotive manufacturers to implement robust cybersecurity measures and build secure infrastructures to maintain consumer confidence more appealing to organizations in regulated industries.



Security challenges in industrial manufacturing

In your opinion, what are the most important challenges in the field of OT security and how can they be addressed?

Marco Merche
Business Information Security Officer - OT & ICS – Germany
FESTO

The central challenge in OT security today is integrating and operationalizing regulatory requirements such as NIS2 and the Cyber Resilience Act within heterogeneous and long-lived production environments, alongside other region-specific regulatory requirements. Many security measures have been understood for years, yet real progress is only emerging as regulatory pressure increases. Effective OT security depends above all on organizational capability: a reliable asset inventory and qualified on-site personnel who can translate requirements into daily operations. These foundations enable meaningful implementation of network segmentation, vulnerability management, and lifecycle management. Without them, OT security remains theoretical rather than operational practice.

Security challenges in healthcare

The healthcare sector is rapidly embracing digital transformation, marked by the widespread adoption of Internet of Medical Things (IoMT) devices and other clinical operational technology. This includes network-capable medical-grade devices such as insulin pumps, CT scanners, and ECG monitors, alongside wearables for health monitoring and remote care systems

Vulnerabilities and risks

A 2025 analysis by Claroty assessed over 2.25 million IoMT devices and 647,000 OT devices across 351 healthcare organizations, revealing:

- **High exposure**: 99% of healthcare organizations have devices with Known Exploited Vulnerabilities (KEVs).
- **Insecure connections:** 89% of IoMT devices are insecurely connected to the internet, risking ransomware and data breaches.

High-risk devices

- **Imaging systems:** 8% have ransomware-linked KEVs; 85% of healthcare delivery organizations are affected.
- **Hospital information systems (HIS):** 20% have KEVs, risking patient records and care continuity.
- **Patient monitoring devices:** Though only 0.5% had severe exposures, this represents thousands of vulnerable endpoints.
- **Surgical devices:** Even one compromised device can endanger patient lives.
- **Non-medical OT systems:** 65% have KEVs, offering potential access points into hospital networks.

Regulatory compliance

Healthcare providers must navigate strict data protection regulations, e.g.:

- **HIPAA (USA):** Focuses on Protected Health Information**.**
- **GDPR (EU):** Covers all personal data.

Both require controlled access, unauthorized change detection, data encryption, and a dedicated data protection officer, adding complexity for global providers.

Security challenges in industrial manufacturing

Key recommendations for enhancing security

Implement Zero-Trust security models: A zero-trust framework with hardware security anchors in PLCs and robotics controllers ensures that all network interactions are verified and authenticated. This model is essential for protecting against unauthorized access and maintaining the integrity of industrial systems.

Strengthen network segmentation: Strict segmentation between IT, OT, and IIoT zones prevents lateral movement by attackers, reducing the risk of widespread network breaches.

Upskilling programs: Addressing the OT-security skills gap through targeted upskilling programs ensures that personnel are equipped to handle emerging security challenges. Investing in workforce development is essential for building a resilient security culture within the organization.

Key security challenges

Legacy systems: High integration costs and complexity in aligning cybersecurity controls with operational uptime. Many factories rely on legacy PLCs, SCADA, and DCS platforms without built-in encryption or secure boot, identified by 50% of OT and ICS decision-makers as major obstacles. [1]

Expanding attack surface through IT and OT: Convergence: The integration of IT and OT networks, along with Industrial IoT devices, expands the attack surface. Poor network segmentation allows attackers to move from corporate systems to control environments. This convergence also introduces AI-driven production systems, which, while enhancing operational capabilities, require sophisticated security frameworks to address new attack vectors and ensure secure connectivity to cloud platforms and external data sources

Regional insights

- **Germany:** Integration of OT security with IT using IEC 62443 frameworks. Network segmentation and industrial SOCs enhance detection and containment. Workforce awareness programs and proactive risk-based strategies improve resilience.
- **Australia:** Tier 2 and Tier 3 suppliers face security challenges due to limited resources, with SOCI regulations impacting incident notification.
- **USA:** Vulnerabilities arise from mixed IT and OT networks and immature processes.
- **India:** Manufacturing clients are shifting from reactive to proactive strategies, driven by threat intelligence and regulatory pressures.

> Third party risks often manifest when contracts fail to mandate effective security controls - or when those controls are never assessed or enforced. Too often, fundamental safeguards such as multi factor authentication, identity management, data loss prevention, and logging and monitoring are absent, ineffective, or applied in an ad hoc way.

Ray Griffiths
Partner
KPMG Australia

Security challenges in automotive

The automotive sector is facing a significant surge in cybersecurity threats as vehicles become more connected and autonomous. This transformation introduces several key challenges:

Autonomous driving vulnerabilities

Autonomous vehicles rely heavily on complex software and connectivity systems, making them susceptible to cyberattacks that can disrupt navigation, control systems, and safety features. Ensuring robust cybersecurity measures is essential to protect these systems from unauthorized access and manipulation.

Connectivity risks

The increased connectivity in modern vehicles, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, introduces vulnerabilities that can be exploited by cybercriminals. These systems require secure communication protocols to prevent unauthorized data access and cyber intrusions.

Keyless entry system exploits

Vulnerabilities in keyless entry systems can lead to unauthorized access. Attackers can intercept signals between the key fob and the vehicle, allowing them to unlock and start the car without physical keys. This type of attack is often referred to as "relay attacks" and poses a significant risk to vehicle security.

EV charging infrastructure vulnerabilities

Security gaps in charging stations pose risks to both vehicles and infrastructure. Attackers can exploit these vulnerabilities to manipulate charging processes, potentially leading to unauthorized access to vehicle data or disruption of the charging network. Ensuring secure communication protocols and authentication mechanisms is crucial to protect against these threats.

Compromised third-party aftermarket devices

Devices added post-manufacture can introduce security risks. These aftermarket devices may not adhere to the same security standards as OEM components, making them potential entry points for cyberattacks. Ensuring compatibility and security of third-party devices is essential to maintain vehicle integrity.

Supply chain threats

Broader threats impacting the automotive supply chain can lead to compromised components and systems. As the automotive industry relies on a complex network of suppliers, vulnerabilities within the supply chain can have far-reaching effects on vehicle security and performance. Implementing robust security measures across the supply chain is crucial to mitigate these risks.

Regional insights

- **Europe:** The integration of old and new systems creates vulnerabilities, with legacy systems often neglected.
- **USA:** Cultural and knowledge barriers hinder the adoption of new technologies due to undocumented critical knowledge held by veteran engineers.
- **India:** Tackling cybersecurity risks in legacy vehicle architectures through end-to-end encryption, restricted access during updates, firmware code reviews, and setting security standards for OTA updates.

Security challenges in transportation and infrastructure

The Transportation and Infrastructure sector faces increasingly complex security challenges, including threats such as ransomware, data breaches, malware, Denial-of-Service (DoS) attacks, and phishing. Operators of airports, seaports, rail networks, and logistics hubs are under pressure to enhance cybersecurity investments to counter these sophisticated threats.

Key Challenges

Decentralized and critical OT systems

Transportation networks, including roads, railways, and airports, rely on decentralized OT systems spread across vast areas, often covering entire countries. This widespread infrastructure is difficult to secure, as it involves numerous entry points and potential vulnerabilities that can be exploited by cybercriminals. The reliance on OT for operational efficiency increases the risk as the "air gap" between OT and IT diminishes, making these systems vulnerable to traditional IT threats.

Logistics and supply chain

Automated supply chains, enhanced by blockchain and cloud-hosted platforms, improve tracking and efficiency but also introduce potential incidents without strong security architectures. Ensuring robust security measures in these digital systems is crucial to prevent cyber threats. The use of smart warehouses leveraging IoT and automation optimizes processes but requires comprehensive security strategies to protect against vulnerabilities.

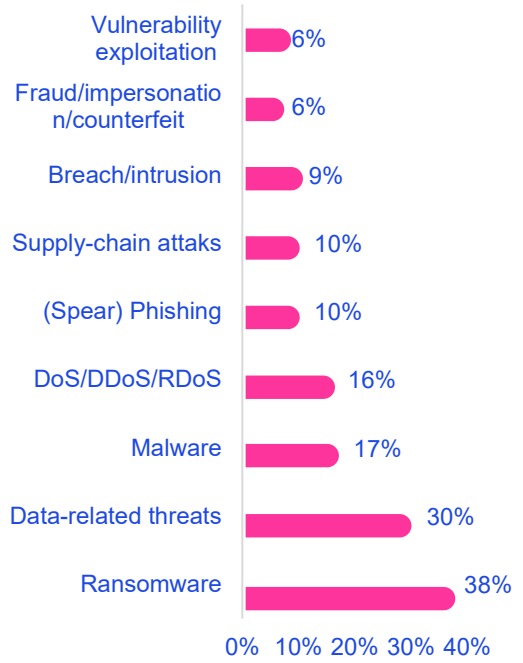
Maritime transportation

The maritime sector is experiencing growth driven by AI/ML integration for navigation and control systems, with autonomous ships offering efficiency and safety benefits. However, these advancements also introduce new cybersecurity risks that must be managed to protect critical maritime infrastructure. The integration of AI and ML requires robust security measures to safeguard against potential cyber threats targeting navigation and control systems.

Urban mobility and smart cities

Intelligent Transportation Systems (ITS) are minimizing traffic congestion and enhancing urban mobility, with the global ITS market projected to grow significantly. However, the interconnected nature of smart cities increases the risk of cyberattacks, requiring comprehensive security strategies to protect urban infrastructure. The deployment of ITS involves collaboration with private partners and government funding, emphasizing the need for robust cybersecurity measures to safeguard urban mobility systems.

Prime threats to the transportation sector (January 2021 to October 2022)



Source: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Transport%20Threat%20Landscape_RECAST2.pdf

Security challenges in energy

The energy sector is undergoing a profound transformation, driven by the imperative for sustainability, resilience, and efficiency. As utilities strive to keep pace with digital transformation, the integration of smart grids and cloud technologies presents both opportunities and challenges. These advancements are crucial for optimizing energy distribution and enhancing operational efficiency, but they also expand the attack surface, necessitating robust cybersecurity measures.

Smart grid and cloud integration challenges

Security-by-design principles: Many smart grid and cloud integration projects lack security-by-design principles, increasing the potential for widespread outages and data breaches. Ensuring that security is embedded from the outset is crucial to protect against cyber threats and maintain operational integrity.

Mix of old and new technologies: Combining new technologies with legacy systems can create vulnerabilities and entry points, which hackers exploit. This integration requires careful management to prevent unauthorized access.

AI-driven network operations: AI and ML are pivotal for optimizing smart grid operations, enabling real-time monitoring, sophisticated analysis, and precise control of energy systems. However, these technologies require connectivity to cloud platforms and external data sources, expanding the attack surface and introducing new cybersecurity risks.

Strategic recommendations

Embrace AI-driven cybersecurity: Organizations should embed AI-driven cybersecurity and advanced monitoring to confidently converge IT and OT, accelerate digital transformation, and shape a future where energy systems are intelligent, resilient, and sustainable.

Strategic planning and immediate action: Given the current necessity of OT transformation, organizations must focus on strategic planning and immediate action to address the evolving landscape and ensure future readiness.

Investment in innovation: Prioritize investment in generative AI and other advanced technologies to redesign processes, rethink client experiences, and ultimately increase efficiency and agility. This is crucial for maintaining competitive advantage and operational excellence

Regional insights

- **Saudi Arabia**: The energy sector is highly targeted due to its critical role in production. Skill shortages and lack of trained resources are significant risks.
- **Malaysia**: Legacy systems are prevalent in OT sites, especially in older facilities. Managing risks associated with legacy systems is crucial, and conventional methods can be effective.
- **India:** Focuses on security-driven infrastructure upgrades, smart grid readiness, and IT-OT convergence frameworks. Resiliency is embedded in both greenfield and brownfield plants to address threats like cyberattacks and supply chain.

> Third party risks often manifest when contracts fail to mandate effective security controls - or when those controls are never assessed or enforced. Too often, fundamental safeguards such as multi factor authentication, identity management, data loss prevention, and logging and monitoring are absent, ineffective, or applied in an ad hoc way.

Ronald Heil
Global Risk Advisory Lead for ENRC
KPMG Netherlands

OT security challenges

Why is OT security considered critically important today?

Alexander Hauke
Senior Manager, Regional Lead
OT Security
KPMG Germany

OT security has become the defining resilience topic for industrial leaders. The key shift is that cyber risk translates directly into operational risk: production losses, quality issues, equipment damage, and safety exposure. What matters now is reducing uncertainty knowing what's in the environment, detecting abnormal behavior early, and being able to contain incidents without stopping the business. OT security is therefore not an IT add-on, but a core capability for continuity and responsible operations.

Recap of security challenges

The chapter on security challenges in OT provides a detailed examination of the vulnerabilities and threats faced by various industries as they integrate advanced technologies. Across sectors, the convergence of IT and OT expands the attack surface for critical infrastructure, exposing systems to IT-borne threats with potential for physical damage and widespread disruption. Ensuring robust security measures across both domains is essential.

In the automotive sector, legacy systems and unprotected networks increase vulnerability, especially with over-the-air updates as potential attack points. Healthcare faces challenges in data security and compliance, navigating complex regulations like MDR, HIPAA, and NIS2 to protect sensitive patient information. Industrial manufacturing must address the expanded attack surface due to IT and OT convergence, requiring strict network segmentation and continuous threat analysis to secure supply chains. Transportation and infrastructure operators face threats such as ransomware and AI-driven phishing campaigns, necessitating enhanced cybersecurity investments and strategic risk mitigation for legacy OT systems. The energy sector, while focusing on sustainable solutions, must also implement robust cybersecurity measures to safeguard critical infrastructure.

With security challenges laid bare, the narrative naturally leads us to the intricate world of regulatory changes. As industries strive to protect their systems, they must also navigate the complex landscape of global compliance requirements. Organizations face mounting pressure to adhere to stringent cybersecurity and OT standards, driven by enhanced legislation such as the EU's NIS2 and Cyber Resilience Act. These sector-specific regulations mandate precise cybersecurity measures and compliance protocols, underscoring their strategic importance in protecting organizational assets and reputation. Understanding these regulatory demands is crucial for developing strategie that ensure operational continuity and resilience while aligning with evolving standards. The next chapter will explore th global variability in regulatory requirements highlighting both the challenges and opportunities they present. It will also look forward to the increasing regulatory pressure and growing board-level interest, which are driving faster adoption of cybersecurity practices.

> The financial cost element, the feasibility of the regulations and the lack of importance of cybersecurity

Meshari Alosaimi
Head of OT Cyber Operations
KPMG Middle East

aramco

What challenges do you observe among your customers when implementing new regulations such as NIS2, IEC 62443, or regional frameworks?

Global variability in regulatory requirements

Regional insights

Europe

Integrating IT and OT systems in Europe is challenging due to historical divides and outdated technology. Change management is key to aligning business priorities, especially with regulations like NIS2 promoting cybersecurity. In the automotive sector, environmental and cybersecurity mandates shape secure OT designs. Compliance is achieved through risk-based frameworks. Healthcare strategies align with standards like IEC 62443, ensuring security and compliance. Regular updates are essential to meet evolving requirements.

Australia

Companies struggle with retrofitting frameworks like ISO 27001 into OT environments due to budget constraints and logistical issues, particularly given the vast distances involved.

Middle East

Regulations are often tailored to specific industries, such as oil and gas, but may not consider broader applications. There is a need for flexible regulations to accommodate future trends and legacy technologies.

USA

U.S. companies face challenges in interpreting and applying international regulations like NIS 2 and GDPR, which differ from local U.S. standards. The complexity is heightened by the global nature of many U.S. companies.

India

National standards such as AIS 189 and AIS 190 are shaping cybersecurity strategies, while new EU regulations offer opportunities to develop unified frameworks that reduce compliance costs and improve cybersecurity.

Global variability in regulatory requirements

Common challenges

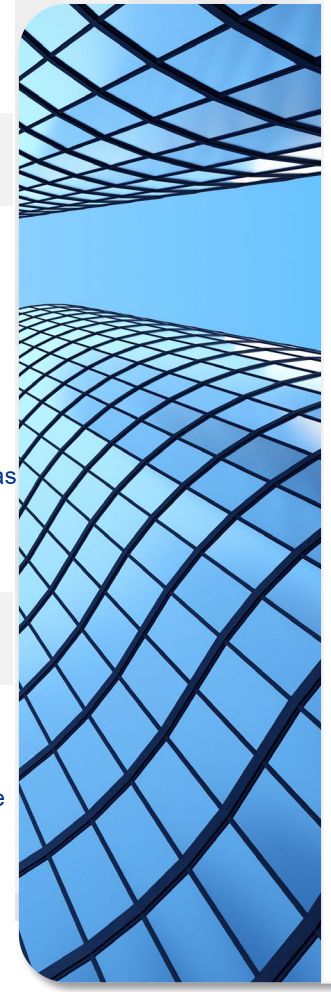
Interoperability and standardization gaps: Rapid technological innovation often outpaces standardization, leading to fragmentation and hindering large-scale deployment of AI-driven systems.
Cybersecurity threats: The convergence of IT and OT expands the attack surface for critical infrastructure, exposing systems to IT-borne threats with potential for physical damage and widespread disruption. Ensuring robust security measures across both domains is essential.
Supply chain due diligence: Global supply chains are vulnerable to geopolitical disruptions, human rights abuses, and environmental concerns, necessitating extensive transparency and due diligence. Organizations must navigate complex regulatory landscapes to ensure compliance and mitigate risks.
Workforce adaptation: Automation can lead to job displacement in traditional roles but creates new opportunities in areas like software development and maintenance. Upskilling and reskilling initiatives are crucial to address the skills gap and ensure workforce readiness for emerging technologies.

Strategic opportunities

Despite these challenges, the variability in regulatory requirements also present opportunities for organizations to innovate and adapt:

Unified frameworks: Developing comprehensive frameworks that align with multiple regulatory standards can streamline compliance and enhance cybersecurity.

Collaborative approaches: Engaging with international bodies and industry groups to harmonize standards and practices can facilitate smoother integration and operational efficiency.



> Relying on compensating controls for unpatched firmware isn't a strategy, it's a regulatory gamble. Modern mandates are shifting the burden of proof from 'did you secure it?' to 'can you prove it is segmented?', no longer leaving room for the security-by-obscurity culture that OT culture has hidden behind for decades.

Dr. Jayne Goble
Partner, Industrial Cybersecurity
KPMG UK

Regulatory pressure and board interest

Increasing regulatory pressure

As global regulatory landscapes continue to evolve, organizations face mounting pressure to comply with increasingly stringent cybersecurity and OT standards. This pressure is driven by:

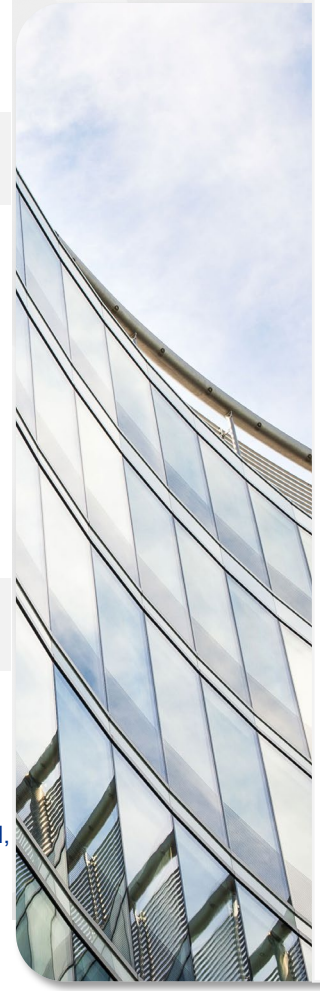
Enhanced legislation: New directives and acts, such as the EU's NIS2 and Cyber Resilience Act, impose rigorous requirements on critical infrastructure and product security. Australia's adoption of IEC 62443 standards demonstrates a proactive approach to regulatory variability, setting a precedent for robust cybersecurity measures that enhance compliance and resilience. This move highlights the need for unified frameworks to streamline compliance across diverse regulatory landscapes.

Sector-specific regulations: Industries like automotive and healthcare are subject to deep vertical regulations that mandate specific cybersecurity measures and compliance protocols. These sector-specific mandates require tailored approaches to cybersecurity, further intensifying the pressure on organizations to adapt and comply..

Growing board-level interest

Board-level interest in cybersecurity and regulatory compliance is intensifying, reflecting the strategic importance of these areas in safeguarding organizational assets and reputation. Insights from two studies highlight this trend:

- The 2023 State of OT and Cyber Security Report, involving 570 respondents globally, found that nearly every company (98%) now includes the OT cybersecurity profile in general risk assessments for management and the board, underscoring the importance of board-level engagement in cybersecurity strategies.
- The 2025 State of Operational Technology and Cybersecurity Report revealed that 52% of organizations place OT security under the CISO, up from just 16% in 2022. This is underscoring the importance of board-level engagement in cybersecurity strategies.



> Regulatory pressure and growing board-level interest are driving faster adoption of cybersecurity practices.

David Marco Freire
Associate Partner, Cyber Tech Risk for OT & Industrial Cybersecurity
KPMG Spain

Recap of regulatory challenges

The chapter on regulatory delves into the complexities of global standards, highlighting the variability across regions and industries. Organizations must navigate diverse legal frameworks and sector-specific mandates, which require agility and strategic foresight. As regulations like the EU's NIS2 and ISA/IEC 62443 evolve, companies face increasing pressure to comply with stringent cybersecurity measures. This pressure is reflected in growing board-level interest, as executives recognize the strategic importance of safeguarding assets and reputation. Implementing new regulations presents challenges such as scope ambiguity, complex security obligations, and integration with legacy systems. Despite these hurdles, opportunities exist to innovate through unified frameworks and collaborative approaches, enhancing compliance and cybersecurity. As global regulatory landscapes evolve, organizations face mounting pressure to adhere to stringent standards, driving faster adoption of cybersecurity practices and underscoring the importance of protecting organizational assets.

Organizations face significant hurdles when implementing new regulations like NIS2 and IEC 62443. The challenges include ambiguity in scope, complex security obligations, and integration with legacy systems. Resource allocation, organizational buy-in, and regulatory overlap further complicate compliance efforts. Additionally, the cyber talent shortage, cost of compliance, and cultural resistance present ongoing obstacles in achieving robust cybersecurity across sectors.

Jad Abdulsalam
VP Cybersecurity
Saudi Arabia
MAADEN

Conclusion

Overall, the outlook has shown that OT is undergoing a significant transformation across various sectors, driven by rapid technological advancements and increasing interconnectivity. This evolution demands immediate focus and strategic planning to address the challenges and opportunities presented by these advancements. The KPMG OT Outlook provides a comprehensive analysis of the current landscape, offering insights into the critical trends, innovations, security challenges, and regulatory requirements that are shaping the future of OT.

Technological integration

The integration of technologies such as AI, 5G, and digital twins is unlocking new levels of efficiency and innovation. These technologies are essential for optimizing operations and enhancing productivity across sectors. However, they also expand the attack surface, making robust cybersecurity measures more crucial than ever. The convergence of IT and OT systems requires a strategic approach to ensure security and resilience.

Cybersecurity challenges

As organizations integrate new technologies, the importance of asset discovery and management becomes paramount. This is crucial for maintaining operational integrity and compliance with stringent regulations like NIS2, NCA OTCC, NIST, and ISA/IEC 62443. The complexity of modern OT environments demands sophisticated security frameworks to protect against emerging threats.

Legacy systems

Addressing the challenges posed by legacy systems is essential for enhancing resilience and security. Many industries rely on outdated OT systems that lack modern security features, making them vulnerable to cyber-attacks. Strategic solutions are needed to modernize these systems without disrupting operations, which requires significant investment and planning.

Sector-specific requirements

Each industry, including automotive, healthcare, industrial manufacturing, transportation & infrastructure, and energy, faces unique challenges and opportunities as they incorporate advanced technologies. These sectors must navigate specific regulatory requirements, such as those imposed by the EU's NIS2 and ISA/IEC 62443, which demand tailored cybersecurity measures and compliance protocols. The energy sector, for instance, is rapidly transforming through digitalization, driven by smart grids and IoT-connected sensors, which optimize energy distribution but also increase cybersecurity risks.

Key recommendations

Embrace AI-driven cybersecurity

Organizations should embed AI-driven cybersecurity and advanced monitoring to confidently converge IT and OT, accelerate digital transformation, and shape a future where industrial systems are intelligent, resilient, and sustainable. This approach is crucial for optimizing smart grid operations and enhancing resilience across sectors like energy and healthcare.

Investment in innovation

Prioritize investment in generative AI and other advanced technologies to redesign processes, rethink client experiences, and ultimately increase efficiency and agility. This is crucial for maintaining competitive advantage and operational excellence, particularly in sectors like automotive and industrial manufacturing, where digital transformation is rapidly advancing.

Strategic planning and immediate action

Given the current necessity of OT transformation, organizations must focus on strategic planning and immediate action to address the evolving landscape and ensure future readiness. This includes modernizing legacy systems and integrating advanced technologies securely to mitigate vulnerabilities.

Upskill employees and leverage external support

Address workforce skill gaps by investing in upskilling and reskilling initiatives to ensure personnel are equipped to handle emerging security challenges. Until sufficient internal expertise is developed, organizations should leverage external support to bridge the skills gap and enhance security capabilities. This is particularly important in sectors facing rapid technological integration and complex regulatory landscapes.

The importance of OT security

At Beiersdorf, trust is the foundation of everything we do – and trust begins with security. OT security is not just a technical requirement; it is a strategic pillar of our production and quality excellence. As digital and physical processes increasingly converge, safeguarding our manufacturing environments becomes essential to ensure both efficiency and resilience. Our ambition is security that evolves; advancing alongside our technologies, empowering our teams, and meeting the evolving expectations of our consumers.

Jan Pausmer
Industrial IT/OT Expert – Germany
Beiersdorf

About the authors

Hossain Alshedoki

Hossain Alshedoki is one of the leading cybersecurity experts in the Energy and Natural Resources industry with an engineering background. In addition to his role in KPMG Middle East, he serves as the Global Internet of Things (IoT) and Operational Technology (OT) Lead. With over 15 years of experience in Cybersecurity, Emerging Technologies, Artificial Intelligence, and Operational Technology, Hossain brings a profound depth of knowledge and leadership to this role.

He is an internationally focused IT/OT security subject-matter expert with a Saudi security clearance. Specializing in leading cybersecurity teams within a converged business and Operational Technology environment and also advising on Industrial Control Systems and automation incorporating Big Data integration, SCADA, PLC, DCS and Safety Instrumented systems (SIS).

Thomas Gronenwald

Thomas Gronenwald is a partner for industrial cyber security (OT, IoT, IIoT) at KPMG Germany and is one of the leading experts for OT and ICS security in the industrial environment. For over 20 years, he has been advising companies ranging from medium-sized businesses to large international corporations and has been responsible for well over 250 major international cyber security projects.

His core strength is managing complex OT transformation programs in both brownfield and greenfield environments. He develops risk-based security strategies, prioritizes investments according to business-critical risks, and balances cost efficiency, sustainable cost reduction, and secure, stable production.

He uses innovative technologies and a strong partner network to connect management, cyber security teams, and engineering functions, creating shared clarity on risks, priorities, and practical solutions.

Alexander Hauke

Alexander Hauke is a Senior Manager at KPMG Germany specializing in Operational Technology (OT) Security, with more than a decade of experience helping industrial manufacturers strengthen cyber resilience across plants, factories, and connected products.

He supports clients from strategy to execution, translating business, safety, and availability requirements into implementable OT security programs. His focus areas include OT governance and operating models aligned to IEC 62443, risk-based network architectures, asset visibility and OT inventory, secure remote access, and continuous threat and exposure management for OT vulnerability reduction.

Known for bridging management, engineering, and security teams, he creates clarity on risks and decision rights, accelerates remediation in complex brownfield environments, and delivers measurable impact, improving security posture without compromising stable production, quality, or operational excellence.

Contributors

Samir Hajdari, Arton Kastrati, Yakup Tül, Isabel König, Avdi Islami, Mustapha Ejjayah

Our expert contributors

From September to December 2025, we conducted a series of interviews with OT leads across various regions, exploring the latest trends and challenges in operational technology. Complementing these discussions, a survey form was released to our clients, providing additional perspectives and data on the integration of AI-driven solutions to enhance cybersecurity and operational efficiency. These engagements highlighted regional differences in adoption and strategic priorities, emphasizing the need for tailored OT innovation strategies

We extend our deepest appreciation to all experts who contributed to this publication through their participation in the interviews. Their in-depth expertise, candid insights, and commitment to knowledge sharing have been instrumental in shaping the findings and ensuring the robustness and practical relevance of this publication.

20 interviews

Jad Abdulsalam
Vice President, Chief Information Security Officer, Ma'aden

Saeed AlSaeed
Chief Executive Officer, Cyberani by Aramco Digital

Meshari Alosaimi
Head of OT Cyber Operations, Aramco

Leo Simonovich
VP and Global Head, Industrial Cybersecurity, Siemens Energy

Jack Chubb
Head of Industrial Cybersecurity, Siemens Energy

Markus Schumburg
Group Chief Information Security Officer, DHL

Majida Dere
Director OT-Security Management, Westfleisch

Raphael Reiss
Head of Group Information Security, Vaillant

Georgios Spyros
Chief Operations Security Officer, ALTANA

Paul Schneider
OT Security Leader, Shell Netherland

Thomas Gronenwald
Partner, Product (CRA) & Production (OT) Cyber Security & Resilience, KPMG Germany

Alexander Hauke
Senior Manager, Regional Lead OT Security, KPMG Germany

Jason Haward-Grau
Principal, Advisory, KPMG in the US

Hossain Alshedoki
Global IOT Security Leader, KPMG & Partner, Cybersecurity, KPMG Middle East

Serjoscha Keck
Partner and Head of Industrial Manufacturing, KPMG Germany

Ramy Galal
Associate Director. KPMG Middle East

Ray Griffiths
Partner, KPMG Australia

Ronald Heil
Partner, KPMG Netherlands

Dr. Jayne Goble
Partner, KPMG UK

David Marco Freire
Associate Partner, KPMG Spain

Contact us

Hossain Alshedoki
Global IOT Security Leader, KPMG
Partner, KPMG Middle East
halshedoki@kpmg.com

Thomas Gronenwald
Partner
KPMG Germany
tgronenwald@kpmg.com

Ray Griffiths
Partner
KPMG Australia
raygriffiths@kpmg.com.au

Ronald Heil
Partner
KPMG Netherlands
heil.ronald@kpmg.nl

Trevor Niblock
Partner
KPMG Middle East
tniblock@kpmg.com

David Marco Freire
Associate Partner
KPMG Spain
davidmarco@kpmg.es

Jason Haward-Grau
Principal
KPMG in the US
jhawardgrau@kpmg.com

Alexander Hauke
Senior Manager
KPMG Germany
ahauke@kpmg.com