The expanding cyber attack surface of IoT, IIoT and critical infrastructure

Enabling effective operations through cyber management

The better the question.
The better the answer.
The better the world works.

Shape the future with confidence

The expanding cyber attack surface of IoT, IIoT and critical infrastructure

Enabling effective operations through cyber management

The term Internet of Things (IoT) has become synonymous with home devices that connect to the internet, from closed circuit television (CCTV) systems to fridges and air conditioning units. But the application of sensors and smart devices is not limited to the home. In the modern era, they are present in almost every walk of life, from defense sectors to hospitals, and across the critical infrastructure that allows industrial societies to function at scale.

In today's environment in the energy sector, industrial facilities are awash with these devices. They help identify potential failures and enable preventative maintenance activities. These capabilities also support condition and corrosion monitoring, real time performance optimization, sustainability management, safety monitoring and the remote oversight of equipment, both onshore and offshore. IoT devices can function on their own or depend on other devices. These capabilities are no longer optional; they are becoming essential to everyday operations for cost and efficiency savings, supporting better data-driven decisions using historical and current data while helping to predict the future.

Throughout this article, the terms IoT and industrial IoT (IIoT) are used interchangeably. In practice, technology is often similar. The difference is in the application. IIoT is generally used to describe IoT deployed in industrial, operational and safety critical environments, where availability, uptime and reliability matter far more than convenience. Furthermore, IoT and IIoT devices often lack the security capabilities commonly found on personal computers (PCs) or mobile devices, meaning they can be the weakest link in the security chain.[1] When such devices are connected to mission critical systems and are less secure than standard PCs, they offer a tempting target for both state and non-state actors.

IIoT is now deeply embedded across sectors such as oil and gas, utilities, manufacturing and telecoms and forms a significant part of modern critical national infrastructure. At the same time, this increased connectivity has introduced new risks. Sensors, controllers, gateways and data pipelines are increasingly targeted as attack vectors, particularly in environments where security controls have not kept pace with digitization.

As attacks powered by artificial intelligence (AI) increase exponentially, IIoT forensics is becoming an essential part of incident response and resilience planning. When people hear the word "forensics," many still think of traditional crime scene investigation: one location, a secured perimeter and clearly defined evidence. Early IT forensics followed the same mental model adopted from law enforcement: one computer, one disk image and one chain of custody.[2] IoT and IIoT environments break that model entirely and often span multiple jurisdictions, as data may reside in completely different countries, operating under different laws and regulations.

IIoT takes the idea of everyday smart devices and applies it to environments where safety and uptime are non negotiable. Instead of fridges and toasters, it includes sensors on production lines, analytic devices running plant operations, monitors attached to heavy equipment, smart meters across utilities and the conduits to cloud platforms that connect all over the world. These IIoT devices sit on systems that run in harsh conditions, interface directly with physical processes, and can integrate with legacy operational technology that was never designed to be connected.

The result is a wide and complex evidence surface. When an incident occurs, the subsequent investigation can span small edge devices, engineering workstations, technician tools, local gateways, on premise systems and vendor managed cloud platforms. Some data may be retained for months, while other records are overwritten in hours or days. In many cases, evidence disappears simply because normal operational activity continues. For this reason, forensic readiness needs to be considered from the start, not as something bolted on after an incident has already happened.

Recent research by the global EY organization shows that IoT is now one of the fastest-growing emerging technologies worldwide, with enterprises ranking it alongside 5G and quantum computing as a top investment priority. IoT adoption in energy grew by more than 12% year-over-year (YoY), reflecting how deeply utilities, grids, substations and metering systems now depend on connected industrial devices.[3] In sectors like energy and manufacturing, this means operational continuity is inseparable from IIoT resilience and investigation. When failures or attacks occur, these devices can often be the missing link in post-incident investigation. Investigations are increasingly stalled not because evidence never existed, but because it was not preserved long enough to be useful.

This changes the question organizations need to ask. It is no longer just "Can we detect and respond to an incident?" but also "Can we actually investigate when something goes wrong?"

This is where forensic readiness by design becomes the next step in IoT security maturity. Rather than treating forensics as a specialist activity that happens later, readiness assumes incidents will occur and focuses on limiting their impact. In IIoT environments, this matters because incidents have real world consequences: operational downtime, uncertainty around root cause, safety implications and regulatory exposure. We now need to examine what data is stored on these IIoT devices that may not be apparent in other areas.

Forensic readiness does not mean turning operational teams into investigators. It means understanding where evidence lives across the environment and setting realistic expectations for logging and retention. It also involves enabling evidence to be accessed, exported and validated in a repeatable and defensible way. Additionally, it means treating investigative access as a controlled, approved, logged and time bound activity, rather than a rushed response under pressure.

The importance of this becomes clear in real world scenarios, with the age-old problem of asset inventory becoming even more critical. Search and rescue operations in remote industrial sites increasingly rely on network telemetry and cellular IoT data to locate missing workers, even where GPS information is unavailable. In utilities and manufacturing environments, time stamped IIoT telemetry, pressure changes, vibration patterns and state transitions often reconstruct incidents more accurately than human reporting or traditional IT logs. Yet this data frequently resides in gateways or vendor clouds with limited retention, making early and structured collection critical.

Guidance from standards bodies is beginning to reflect these realities. The National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA), both based in the US, highlight the importance of preserving evidence integrity. They also emphasize maintaining a defensible chain of custody, particularly in environments where digital data is easily altered or lost. At the same time, emerging IoT standards may improve consistency in how devices are identified and accessed. However, they also introduce governance challenges if forensic access is not tightly controlled.

Ultimately, investigations are not just about attribution. In IIoT environments, they provide the missing link needed to understand what actually failed and how to prevent it from happening again. Knowing whether an incident was caused by equipment failure, misconfiguration, human error or a targeted attack directly shapes future design and resilience decisions. Without reliable evidence, those decisions are made in the dark.

A compressor trip in an offshore facility may initially present as a mechanical failure. However, a cyber-enabled review of telemetry could also reveal a configuration change to the controller or a remote access session from an engineering workstation. Without forensic access to sensor data, controller logs, network telemetry and gateway records, the organization is left guessing. This risks applying a mechanical fix to what is actually a cyber driven issue or leaving a genuine security weakness unaddressed.

The evolution of IIoT has changed the nature of incidents. Evidence is more distributed, more fragile and increasingly tied to systems that keep facilities, infrastructure and economies running. Forensic readiness by design is therefore not a niche technical concern, but a core part of operational resilience. As IT, OT, IIoT and AI environments continue to integrate, leaders face a simple but uncomfortable question at the heart of their security strategy:

Are you building systems you can secure and investigate when it matters most?

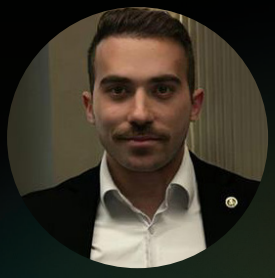
References

1. "Guidelines for Securing the Internet of Things," *ENISA European Union Agency for Cybersecurity*, November 2017.
2. "Chain of Custody and Critical Infrastructure Systems," *Cybersecurity and Infrastructure Security Agency (CISA)*, 2020.
3. "Internet Of Things (IoT) In Energy Market (2024-2030)," *Grand View Research*, grandviewresearch.com/industry-analysis/internet-of-things-iot-energy-market-report, 2024.

Authors

Nicholas S Jones
Partner
Technology Consulting
EY Consulting LLC
nicholas.jones@qa.ey.com

Mohammed Alhajri
Director
Technology Consulting
EY Consulting LLC
mohammed.alhajri@qa.ey.com



Roland Sarrouh
Assistant Manager
Technology Consulting
EY Consulting LLC
roland.sarrouh@qa.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

The MENA practice of EY has been operating in the region since 1923. Over the past 100 years, we have grown to over 8,500 people united across 27 offices and 14 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

EYG no. 112761-26-GBL
ED None.

ey.com