Number 115 | June 2026

NTT DATA

Radar

The Cyber Security Magazine

When Machines Learn to Attack Real Infrastructure

By Luís Guillen

The convergence of artificial intelligence and operational technology systems has created a new hybrid battlefield, where protecting data alone is no longer enough: the continuity of the physical world itself is now at stake. A credit card data breach is not the same as disrupting the electricity supply of an entire community, shutting down a water treatment plant, or triggering a cascading failure in a refinery.

In the first case, we are dealing with a serious incident, whereas in the second we are facing a potentially catastrophic scenario, with a direct impact on public safety. For years, cyber security kept the digital world separate from the physical one, but today that boundary has virtually disappeared, and artificial intelligence is tearing down the last remaining barriers.

Operational technology systems are the nervous system of industry. We are talking about programmable logic controllers (PLCs), SCADA systems, industrial sensors, and the entire digital infrastructure that governs physical processes, including components that control smart buildings and medical equipment, from the opening of a valve or the management of rail traffic to the operation of lifts, CCTV systems, medical imaging equipment, and connected ventilators. For decades, these environments remained relatively isolated from corporate networks

Their security relied, to a large extent, on that separation, the famous air gap, the physical divide that shielded them from external threats. That model is now history. The push for operational efficiency, remote monitoring, and integration with enterprise systems has gradually eroded that distance. Today, most OT and IoT environments are connected, in one way or another, to networks that have contact with the outside world. And that makes them targets.

AI as a Threat Multiplier

If the exposure of these environments was already a cause for concern, the emergence of artificial intelligence within the cyber attack ecosystem takes the threat to an entirely new level. This is not science fiction. These are tools that already exist, that are becoming more sophisticated every month, and that are now within reach of actors with resources that, until recently, were available only to the most advanced states.

AI enables attackers to automate the reconnaissance of infrastructure, identify specific vulnerabilities in industrial protocols such as Modbus, DNP3, or IEC 61850, and generate exploits tailored to specific environments at a speed that no human team can match.

But perhaps the most disturbing aspect is not the speed, but the subtlety. Machine learning models can analyze the normal behaviour of an OT and IoT system over weeks or even months, learn its operational patterns, and design attacks capable of slipping past traditional detection systems. A slight deviation in pipeline pressure. An almost imperceptible variation in the frequency of a turbine. Anomalies that no human operator would detect in time.

The Bright Side, AI as a Shield

It would, however, be a mistake to reduce the role of artificial intelligence to that of a mere threat. The very same technology that can be weaponized by malicious actors is also the most powerful tool the sector has to defend itself.

AI based anomaly detection systems can monitor thousands of variables across an industrial environment in real time, establish baselines for normal behaviour, and raise alerts whenever even the slightest deviation occurs, before it develops into an incident.

Vulnerability management, event correlation across hybrid environments, and automated incident response are areas where artificial intelligence not only improves efficiency but may become the only viable means of operating at the speed demanded by the most sophisticated attacks.

A human analyst cannot process millions of records from a SCADA system in a matter of seconds. A well-trained model can.

The Challenge Nobody Wants to Name

But there is a structural problem that continues to loom over the industry: OT environments were not designed with cyber security in mind. Many of the systems currently in operation are decades old, run on unsupported operating systems, lack encryption capabilities, and cannot be patched without disrupting critical production processes. Integrating AI solutions into these environments is, from a technical perspective, an enormous challenge. And culturally, operations teams and security teams still speak different languages, with priorities that often conflict.

This is compounded by the shortage of specialized talent. Professionals who combine deep knowledge of industrial systems, OT operations, and cyber security are still relatively scarce, as this is a highly specialized field that has only recently begun to mature within the market. Without this internal or external expertise, even the most sophisticated solutions can end up becoming black boxes that are difficult to manage when a critical incident occurs.

A Matter of Strategic Priority

Protecting OT environments against AI enhanced threats can no longer remain an issue confined to technical departments. It is a matter of national security, economic continuity, and social responsibility. The attacks recorded in recent years against critical infrastructure, including power grids, water treatment plants, and healthcare systems, are not isolated incidents, but clear warning signs of a growing risk.

The response cannot come once the attack has already taken place; it must be built in advance through compliance with regulatory frameworks that establish minimum requirements according to the criticality of each environment, through sustained investment in specialized training, through genuine collaboration between the public and private sectors that goes beyond reports filled with good intentions, and through a technology industry that designs solutions with the real complexity of OT and IoT environments in mind, rather than focusing solely on the elegant and idealized scenarios of a laboratory.

Artificial intelligence has arrived in the industrial world to stay. The question is not whether it will transform OT cyber security, but whether we will be capable of guiding that transformation before others do it for us.

Luís Guillen
Cybersecurity Director

The Spring of 2026 Did Not Arrive Alone

Cyber Chronicle by Alicia Isabel Martínez Vera

As Europe began preparing for the summer and companies accelerated their digitalisation processes, cyberspace once again proved that there are no quiet seasons. From mid April until today, the cyber security landscape has been shaped by increasingly aggressive ransomware campaigns, massive data breaches, attacks on supply chains, and a new generation of threats driven by artificial intelligence.

The prevailing feeling throughout these weeks has been unmistakable: attackers are no longer seeking only to steal information; they are aiming to paralyze operations, erode trust, and turn digital dependence into a weapon.

During April, a trend that had already begun to emerge throughout 2025 continued to intensify: technology providers became the preferred point of entry for cyber criminals. Intelligence reports and sector analysis warned of an increase in attacks targeting third parties with privileged access to corporate infrastructure.

One of the most symbolic episodes was the attack suffered by Inditex. The fashion giant confirmed unauthorized access to databases hosted on the servers of an external provider, reigniting the debate around the security of interconnected ecosystems and the difficulty of controlling risks beyond the corporate perimeter.

Almost at the same time, the gym chain Basic Fit suffered an intrusion that ultimately exposed the personal data of thousands of European users. Names, email addresses, telephone numbers, and banking details were compromised in one of the most high-profile attacks against the retail and services sector so far this year.

Behind these incidents, the same pattern kept emerging: attackers were not always striking the primary victim directly. They were entering through forgotten integrations, connected applications, or suppliers with weaker defenses. The traditional perimeter had definitively disappeared.

Another troubling trend was the widespread use of artificial intelligence by malicious actors.

Experts began warning that phishing had changed forever. The old emails filled with spelling mistakes gave way to polished, personalized messages that were almost impossible to distinguish from legitimate communications. Generative AI started to be used to automate social engineering campaigns, clone voices, and generate hyper realistic messages at scale.

At the same time, ransomware evolved towards virtually autonomous models. Some campaigns detected in April revealed malware capable of identifying critical systems, encrypting information, and exfiltrating data with minimal human intervention.

If April was defined by corporate breaches, May painted a different picture: public administrations once again became a priority target for ransomware groups.

The most visible case was that of Valdemoro Town Council. The municipality near Madrid suffered an attack that partially paralyzed essential services, affecting the municipal register, management systems, and payment platforms.

Days later, it emerged that the group Kairos had claimed responsibility for the intrusion and stated that it had obtained nearly 1.8 TB of sensitive information. The incident reflected an increasingly common trend: “double extortion”.

As the month progressed, another reality became impossible to ignore data breaches had ceased to be exceptional events. Figures published in Spain showed that more than 2,600 security breaches were reported during 2025, affecting over 200 million records. Symbolically, that amounted to more than four breaches per citizen. Attacks were no longer affecting only large multinationals. Any organization with data, connectivity, and technological dependence could become a target.

While attacks continued to increase, so too did regulatory pressure. During April, European institutions intensified the debate surrounding the implementation of the NIS2 Directive and the need to harmonize cyber security obligations across the European Union.

If these past weeks had to be summarized in a single idea, it would be this: digital trust has become the attackers' primary target.

Companies no longer fear only the loss of data; they fear operational paralysis, reputational damage, and the breakdown of relationships with customers and partners. Cyber criminals have learned that psychological and operational impact can be just as valuable as financial gain.

Between mid April and May 2026, the landscape delivered one unmistakable conclusion: cyber security has definitively entered a new era. An era in which offensive AI, automated ransomware, and the exploitation of third parties are redefining global digital risk.

Alicia Isabel Martinez Vera
Cybersecurity Consultant

Zero Trust and Defence in Depth with ISA 62443

Article by Jhon Jaire Medina Davis

Critical infrastructure cyber security can no longer rely solely on the perimeter. IT/OT convergence, the remote control of distributed facilities, third party remote access, the presence of legacy assets, and the requirement for service continuity make it necessary to adopt more granular, risk based models. In this context, Zero Trust introduces a valuable principle: eliminating implicit trust and continuously verifying identities, devices, communications, and access. However, its direct transfer from IT into OT environments is limited by availability constraints, deterministic operations, remote management requirements, and extremely long technology life cycles. This article argues that the most effective way to bring Zero Trust into industrial environments is not to replicate IT controls, but to integrate it with Defence in Depth and implement it through the ISA/IEC 62443 methodology. It explains the relationship between both concepts, their connection to process safety and availability, the coverage provided by the seven foundational requirements of ISA 62443-3-3, and the importance of risk analysis in accordance with ISA 62443-3-2 to define zones, conduits, target security levels, and proportionate controls. The approach is presented in language designed to be especially accessible to operators, enabling strategic principles to be translated into technical and organisational measures that are auditable, prioritised, and aligned with the operational reality of industrial systems.

Critical infrastructures operate on automation and remote control systems whose historical design has prioritized process safety, availability, and service continuity.

For many years, this reality favoured relatively closed architectures, with a limited number of interconnections and clearly defined operational boundaries. However, industrial digitalization, connectivity with corporate systems, remote access for operation and maintenance, the incorporation of advanced analytics, and the need to integrate operational data with business processes have eroded that traditional separation.

At the same time, the threat landscape has evolved. Today, concerns extend beyond opportunistic attacks to include targeted campaigns, ransomware with operational impact, the abuse of remote access, third party compromise, and lateral movement exploiting credentials, flat networks, and assets with limited protection capabilities.

The traditional assumption that “everything inside the control network is trustworthy” is no longer sustainable.

In this context, Zero Trust has gained relevance as a guiding principle of modern cyber security. However, within OT environments it cannot be implemented simply by copying corporate IT patterns. The challenge is not to import a catalogue of technologies, but to reinterpret its principles for an environment where an authentication delay, aggressive scanning activity, or an unplanned reboot can result in loss of process visibility, incorrect operational actions, degradation of quality, or service interruptions.

The central argument of this paper is that the practical convergence between Zero Trust and Defence in Depth is already embedded within ISA/IEC 62443, provided that its methodology is applied correctly and with a clearly risk oriented interpretation.

Zero Trust in OT Environments: Principles and Limits of Application

The Zero Trust model is based on a simple idea: there should be no implicit trust merely because a user, device, or communication resides within a particular network. The Cybersecurity and Infrastructure Security Agency (CISA) structures this approach around pillars such as identity, devices, networks, applications and workloads, and data, supported by cross functional capabilities including visibility, analytics, automation, and governance (CISA, 2023).

NIST, meanwhile, emphasizes that Zero Trust seeks to reduce areas of implicit trust, base access decisions on granular authentication and authorization, and preserve availability by minimizing the temporary delays associated with verification mechanisms (NIST, 2020).

The difficulty arises when these principles are transferred into the OT world. CISA itself warns that its Zero Trust Maturity Model does not specifically address the challenges associated with operational technologies, certain classes of IoT, or the constraints of devices with limited authentication, visibility, and security capabilities (CISA, 2023). This warning is particularly relevant in critical infrastructures, where PLCs, RTUs, HMIs, engineering workstations, communication equipment, and distributed assets coexist with long operational lifecycles, inconsistent support, and dependence on remote control links.

For this reason, in OT environments Zero Trust should be understood as an architectural and governance principle rather than as a uniform prescription. It will not always be feasible to install agents, perform continuous contextual authentication across every asset, or demand the same level of telemetry expected in a modern IT network.

What is feasible, however, is the elimination of implicit trust between zones, the strengthening of human and service identities, the rigorous control of remote access, the restriction of connectivity to what is strictly necessary, the enforcement of traceability, the protection of change integrity, and the use of compensating controls where assets cannot support advanced security mechanisms. In other words, in OT environments Zero Trust is not implemented "in the same way as in IT"; it is implemented in an adapted manner, preserving the principle while adjusting the mechanism to the criticality and operational requirements of the process.

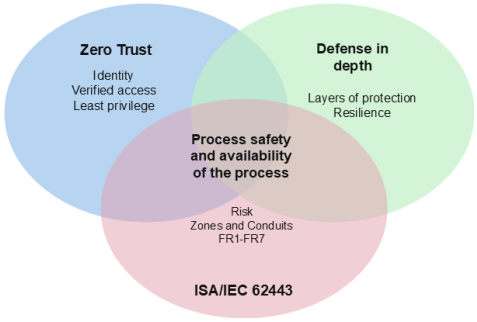


Figure 1: Conceptual convergence between Zero Trust, Defence in Depth, and ISA/IEC 62443.

Defence in Depth and Its Relationship with Process Safety and Availability

Defence in Depth is particularly well suited to critical infrastructures because it aligns with the traditional way in which process safety and operational continuity have been managed. As in operational risk analysis, the assumption is that no single safeguard is sufficient to control high consequence scenarios; true resilience comes from the combination of technical, operational, and organisational barriers. In treatment plants, pumping stations, reservoirs, distribution networks, and sanitation systems, risk does not depend on a single piece of equipment or one isolated control, but on the interaction between multiple measures that must remain effective over time. From this perspective, the logic of industrial cyber security naturally converges with the logic of safe operations: preventing a single failure, error, or malicious action from compromising quality, service continuity, or the operational integrity of the process.

In practical terms, Defense in Depth in OT environments combines layers of governance, physical protection of remote sites, segmentation between corporate and operational environments, hardening of servers and workstations, protection of PLCs, RTUs, and field devices, control of third party remote access, monitoring, incident response, and backup and recovery capabilities.

Its objective is not merely to block unauthorized access, but to prevent a single weakness, for example a shared account, a poorly located engineering workstation, an exposed remote control gateway, or an overly permissive DMZ, from compromising multiple layers simultaneously. Resilience emerges precisely from the structured combination of barriers and from the relative independence between them.

The relationship with process safety and availability is direct. A cyber incident may alter setpoints, degrade the quality of information, suppress alarms, block communications with remote stations, modify operational parameters, or prevent personnel from responding in a timely manner.

In the water sector, this can translate into incorrect chemical dosing, inappropriate pumping operations, loss of visibility over reservoirs and stations, deterioration in treated water quality, or service interruptions. For this reason, within critical water and sanitation infrastructures, cyber security should not be regarded as a parallel domain, but as a necessary condition for maintaining operations within their intended limits and preserving the effectiveness of the process's technical and organisational barriers.

ISA/IEC 62443 as an Implementation Methodology

The main strength of ISA/IEC 62443 lies in its ability to transform strategic concepts into an applicable methodology. The series is not a flat list of controls; it structures governance, risk analysis, architecture, and technical requirements in a coherent manner. In Part 2-1, aimed at the asset owner, the standard defines the security programme as the combination of process, people, and technology based capabilities intended to reduce the cyber risk of the IACS, while also recognizing that its policies must coexist with those of the corporate ISMS without losing sight of the availability and performance constraints inherent to industrial environments (ISA, 2024).

Part 3-2 is the essential methodological bridge. It requires an initial cyber risk assessment of the system under consideration, the partitioning of assets into zones and conduits according to risk, and the performance of a detailed analysis to determine a Security Level Target (SL-T) for each zone or conduit (ISA, 2020).

For operators in the water sector, this means starting from the actual criticality of each process function, for example abstraction, dosing, pumping, storage, distribution, or remote control, and analyzing the consequences that its degradation could have on operational safety, water quality, regulatory compliance, and service continuity. Cyber security analysis does not begin in the abstract; it begins with an understanding of the process and its consequences.

Finally, Part 3-3 establishes the technical system requirements organized into seven foundational requirements. This structure makes it possible to translate the SL-T into concrete controls, with sufficient granularity to define realistic and auditable measures. In this way, Zero Trust provides the principles, Defense in Depth provides the layered logic, and ISA/IEC 62443 provides the methodology to transform both into architecture, procedures, evidence, and a roadmap for continuous improvement.

Figure 2: Recommended sequence for implementing Zero Trust and Defence in Depth controls through ISA/IEC 62443.

The Seven Foundational Requirements as a Framework for Convergence

The convergence between Zero Trust and Defense in Depth becomes clear when analyzing the seven foundational requirements of ISA/IEC 62443-3-3. Far from being a framework unrelated to Zero Trust, the standard already incorporates its essential principles by requiring robust identification, least privilege, integrity, flow control, visibility, and availability.

At the same time, the way these requirements are distributed across zones, conduits, functions, and procedures makes them a natural implementation of Defense in Depth.

FR	Contribution to Zero Trust	Contribution to Defense in Depth	Typical Example in OT
FR1 IAC	Verified identity; strong authentication; unique accounts; strengthened remote access.	First barrier against unauthorized access by users or devices.	Named accounts in SCADA systems and remote access to DWTPs and WWTPs; MFA for remote maintenance.
FR2 UC	Least privilege, role based access, and segregation of duties.	Prevents a single identity from escalating privileges or affecting multiple layers.	Separate roles for central operations, maintenance, laboratory staff, and suppliers; control of USB devices and laptops.
FR3 SI	Verification of system integrity and relevant changes.	Reduces the likelihood of malicious or accidental alteration of critical assets.	Hardening, configuration control, protection of PLCs and RTUs, and validation of changes to setpoints and firmware.
FR4 DC	Protection of information in transit and at rest according to criticality	Adds a layer of protection for parameters, files, and remote access.	Selective encryption of remote access, secure storage of backups, and protection of configuration files.
FR5 RDF	Granular segmentation and minimal connectivity between trust domains.	Implements zones and conduits as architectural barriers.	Industrial DMZ, separation between the corporate network, process network, and remote control network; exception-based rules.
FR6 TRE	Observability, detection, and timely response.	Adds layers of detection and containment to reduce attacker dwell time.	OT network monitoring, event correlation, and response to anomalous access or loss of communications.
FR7 RA	Maintains resilience and supports access related decisions without compromising continuity.	Ensures that the system continues operating, or can recover safely, after an incident.	Redundancy, verified backups, asset inventory, service continuity, and recovery of remote stations

Table 1: Relationship Between the ISA/IEC 62443 Foundational Requirements, Zero Trust, and Defence in Depth

Taken together, the seven FRs demonstrate that ISA/IEC 62443 does not require organizations to choose between Zero Trust and Defence in Depth. On the contrary, it provides a common language for both. FR1 and FR2 materialize identity management and least privilege; FR3, FR4, and FR5 provide integrity, information protection, and segmentation; while FR6 and FR7 extend the architecture towards detection, response, and operational continuity. This coverage is especially valuable in OT environments because it avoids partial approaches focused solely on firewalls or authentication, and instead requires simultaneous consideration of access control, communications architecture, system integrity, and resilience.

The Importance of Risk Analysis and the SL-T

One of the most common causes of failure in industrial cyber security programmes is attempting to implement controls before fully understanding the specific risk that must be reduced. ISA/IEC 62443-3-2 avoids this mistake by requiring an initial assessment of the risk associated with the system under consideration, with a focus on the worst unmitigated impact on safety, the environment, continuity, production, quality, finance, compliance, and reputation (ISA, 2020). In the water sector, this analysis must also be grounded in concrete effects such as loss of control over dosing processes, unavailability of remote control systems, deterioration of water quality, or service interruptions affecting remote stations and main plants.

This approach connects very naturally with HAZOP and LOPA methodologies. In operational risk analysis practice, the value lies not only in listing threats, but in understanding scenarios: cause, deviation, consequences, existing safeguards, the independence of protection layers, and residual risk. Applied to cyber security, the analysis must answer questions such as: what would happen if a compromised operator workstation altered dosing setpoints? What impact would the loss of communications with remote pumping stations or reservoirs have? What would happen if an unsupervised remote access session executed operations out of sequence? Which layer would be lost if operator visibility were degraded by malware or by the unavailability of the historian? This perspective makes it possible to identify not only vulnerabilities, but also the exact risk reduction requirements.

The determination of the SL-T for each zone or conduit is a practical consequence of that analysis.

Not all zones require the same level of protection or the same countermeasures. A plant process network, a remote control network with distributed stations, an industrial DMZ, or a historian server may share a functional relationship, but they do not share the same threat profile, criticality, or tolerance to failure. When the SL-T is defined correctly, the organization avoids both underprotection and overprotection.

This brings very tangible benefits: it rationalizes investment, facilitates phased implementation, improves communication with operations and maintenance teams, and provides a technical justification for why MFA is required for remote access, why process and remote control domains are separated, or why removable media policies must be strengthened.

In addition, the standard requires the risk analysis to be documented and maintained as a living asset for audits, testing, future reviews, and design evolution (ISA, 2020). This documentation constitutes one of the greatest strengths of the approach. It allows organizations to move from intuitive decisions to demonstrable decisions; from “we believe we are protected” to “we know which risk each control reduces and why it is implemented where it is”.

Common Findings and the Benefits of Correct Implementation

Experience gathered from maturity assessments, document reviews, plant visits, architectural analysis, and technical configuration reviews consistently reveals recurring patterns.

In industrial installations, it is common to encounter generic user accounts on SCADA workstations, exposed credentials, engineering or remote control stations acting as bridges between segments, overly permissive firewall rules, poorly implemented industrial DMZs, insufficiently governed third party remote access, uncontrolled use of USB devices, outdated inventories, and network diagrams that no longer reflect the actual state of the installation. None of these issues is extraordinary; that is precisely what makes them so dangerous.

When the ISA/IEC 62443 methodology is applied correctly, these findings cease to be treated as isolated incidents and instead become recognized as symptoms of an architecture without clearly defined trust boundaries, without a proper allocation of responsibilities, or without sufficient risk reduction.

At that point, it becomes possible to prioritize quick wins, such as unique user accounts, hardening of remote access, reinforcement of industrial DMZs, port control, basic segmentation, and log centralization, while simultaneously defining medium term structural improvements such as redesign based on zones and conduits, segregation between corporate, process, and remote control networks, governance of the vulnerability lifecycle, backup and restore procedures, and OT incident response exercises.

The benefit is not merely technical. It also improves traceability, reduces dependence on tacit knowledge, facilitates audits, structures the relationship between IT and OT, and provides management with an objective basis for deciding where to invest first. In other words, the true value of the approach does not lie in accumulating controls, but in building a security posture that is coherent with the process and sustainable over time.

Hallazgo observado	Riesgo dominante	Respuesta prioritaria alineada con ISA 62443
Usuarios genéricos en SCADA/HMI	Pérdida de trazabilidad y facilidad de escalado.	FR1 y FR2: cuentas únicas, roles, MFA donde proceda y revisión de privilegios.
Estación de ingeniería o telecontrol utilizada como puente entre segmentos	Movimiento lateral, punto único de fallo y pérdida de control del acceso.	FR5 y FR3: reubicar la estación, segmentar conduits y endurecer el activo.
DMZ industrial o pasarela de telecontrol permisiva	Acceso directo desde IT a servicios OT críticos.	FR5 y FR1: reglas por excepción, MFA, publicación de réplicas y registro de sesiones.
Acceso remoto de terceros sin control suficiente	Maniobras no supervisadas, exposición de credenciales y baja trazabilidad.	FR1, FR2 y FR5: MFA, jump server, ventanas de acceso y registro de sesiones.
Uso de USB y portátiles sin control	Introducción de malware y alteración de configuraciones.	FR2, FR3 y FR7: política de medios extraíbles, validación previa y procedimientos de escaneo seguro.
Inventario y diagramas desactualizados	Decisiones de riesgo basadas en una arquitectura irreal.	ISA 62443-3-2 y 2-1: inventario fiable, documentación viva y revisión periódica de cambios.

Table 2: Recurring Findings in OT Assessments and Recommended Responses.

Conclusion

Zero Trust and Defense in Depth should not be understood as alternative approaches to the protection of critical infrastructure. Zero Trust provides a necessary discipline: challenging implicit trust, verifying every relevant access request, and reducing connectivity to what is strictly necessary. Defense in Depth contributes a well established engineering logic within the industrial world: no single barrier is sufficient, and resilience depends on the structured combination of technical, physical, and organizational layers.

ISA/IEC 62443 is the framework that makes it possible to integrate both concepts without misaligning them from the operational reality of critical infrastructure. Its value lies in linking governance, risk analysis, zones and conduits, target security levels, and technical requirements within a verifiable methodology. When applied rigorously, it not only improves the cyber protection of the IACS, but also preserves process safety and availability, supports risk based investment decisions, and transforms industrial cyber security into an auditable and manageable discipline.

For organizations operating within the industrial sector, the message is clear: the question is no longer whether Zero Trust principles should be adopted, but how to implement them without compromising availability, service continuity, or maintainability. The practical answer lies in adopting a risk based Defense in Depth strategy and implementing it through ISA/IEC 62443.

Jhon Jairo Medina Davis
Cybersecurity Technical Manager

OT Trends: Quantum Encryption in Industrial Environments

Trends by Miren Ordoñez de Arce

In the world of industrial cyber security (OT), where factories, energy plants, and transport systems coexist, protecting information has never been more critical. As digitalization advances, with sensors, PLCs, and industrial networks becoming increasingly interconnected, the risks continue to grow. And on the horizon, a new disruption is emerging: quantum computing.

This is where one of the most widely discussed trends comes into play: quantum encryption, a technology that promises to redefine how we protect communications in industrial environments.

Why Is Quantum Computing Such a Concern?

Today, most encryption systems, including those protecting industrial communications and corporate networks, are based on mathematical problems that are extremely difficult to solve. However, future quantum computers could break many of these systems in a matter of minutes.

This creates a worrying scenario for industry: production data, recipes, machinery configurations, and even critical infrastructure could become exposed.

What Exactly Is Quantum Encryption?

When we talk about quantum encryption, we are mainly referring to a specific technology: Quantum Key Distribution (QKD).

In simple terms, QKD allows two systems to share a secret key used to encrypt information, but with one crucial difference: it relies on the principles of quantum physics rather than traditional mathematics.

This leads to a very powerful consequence:

If someone attempts to intercept the key, the system automatically detects it, because measuring a quantum state alters its behaviour.

In other words, it not only protects information, but also warns of intrusions in real time.

How Does This Fit into OT Environments?

Although it may sound futuristic, quantum encryption is already being explored in real industrial scenarios. For example, its use has been studied in processes as specific as the secure transfer of programmes to PLCs in factories.

In OT environments, its clearest applications include:

- Protecting communications between plants and control centres
- Securing energy networks and critical infrastructure
- Ensuring the safe exchange of data between suppliers and industrial systems

This is especially relevant because many industrial systems have extremely long life cycles, often between 10 and 20 years, meaning they must begin preparing today for future threats.

What Advantages Does It Offer Compared with Traditional Security?

Quantum encryption introduces a genuine paradigm shift:

- Security based on physics rather than mathematics. It does not depend on a problem being “difficult” to solve, but on physical laws that cannot be broken.
- Detection of espionage. Any interception attempt leaves an immediate trace.
- Preparation for “Q-Day”. The moment when quantum computers become capable of breaking today’s encryption methods.

But… It Is Not That Simple

Like any emerging technology, quantum encryption also faces significant challenges:

- Cost and infrastructure requirements: it demands specialized hardware and, in many cases, dedicated fibre optic links.
- Distance limitations: quantum transmission still faces technical constraints.
- Integration with legacy systems: something particularly complex in OT environments.

For this reason, in practice many organizations are combining QKD with other solutions such as post quantum cryptography, which is software based.

A Passing Trend or an Imminent Reality?

Although it is not yet a mainstream technology, quantum encryption is already moving beyond the laboratory. European projects such as EuroQCI, together with industrial initiatives, demonstrate that it is becoming a strategic priority, particularly for critical sectors.

In the OT context, this is not merely a technological trend, but a matter of resilience: protecting today the systems that will still need to operate decades from now.

Conclusion: Industrial Security Enters a New Era

Quantum encryption represents a profound shift in how we understand cyber security. For the industrial world, it means moving beyond protecting systems against current threats and beginning to prepare for threats that have not yet arrived.

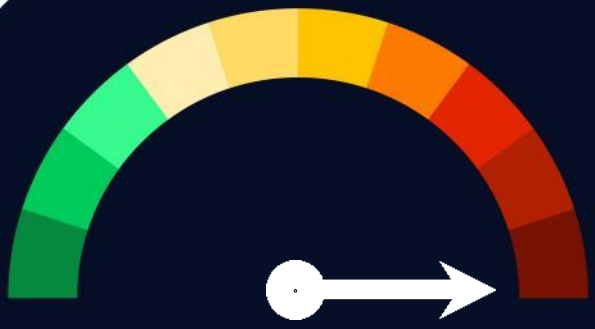
It will not replace existing solutions overnight, but it clearly points towards the future: security will either be quantum safe, or it will not be secure at all.

Miren Ordoñez de Arce
Cybersecurity Lead Analyst

Vulnerabilities

SQL Injection in MegaCMS by CRM Loyalty Systems

Date: 29 April 2026
CVE: CVE-2026-3325



CVSS: 10

CRITICAL

Description

A critical severity vulnerability has been discovered affecting MegaCMS, software used for the management of reservation systems, ticketing, and online sales.

The vulnerability is caused by inadequate validation and sanitization of a user input field. Through a POST request, the parameter 'id_territorio', used immediately after the submission of the registration form, could be manipulated by an unauthenticated attacker to execute arbitrary SQL queries.

The vulnerability has already been fixed in the latest version of the software, and the recommended mitigation is to update to the most recent release.

Solution

- The patch is included in the latest available version of the software.
- It is recommended to update to the latest version as soon as possible and to monitor web server logs for any attempts to exploit the vulnerability

Affected Products

- MegaCMS version 12.0.0.
- Examples include hotel or tourism service websites, event platforms, and ticket sales platforms.

References

- incibe.es
- app.opencve.io

Vulnerabilities

Integer Overflow in Blink / Google Chrome

Date: 6 May 2026
CVE: CVE-2026-7896

CVSS: 8.8

HIGH

Description

A critical Integer Overflow vulnerability has been identified in Blink, the rendering engine used by Google Chrome.

The vulnerability occurs during the processing of specially crafted HTML content and may lead to an integer overflow resulting in heap corruption.

A remote attacker could exploit this vulnerability through a malicious web page, without requiring any additional user interaction beyond visiting or opening the page with a vulnerable version of Chrome.

Successful exploitation could allow the execution of arbitrary code within the context of the affected browser.

Solution

It is recommended to:

- Update Google Chrome to version 148.0.7778.96/97 or later, depending on the operating system.

Affected Products

Some of the affected products include:

- Google Chrome for Windows, Linux, and macOS versions prior to 148.0.7778.96.

Note: Other Chromium based browsers may also be affected if they incorporate a vulnerable version of Blink, although this should be verified against the specific advisories issued by each vendor.

References

- app.opencve.io
- nvd.nist.gov
- chromereleases.googleblog.com

Redis Fixes Vulnerabilities Allowing Code Execution on Its Servers

Date: 6 May 2026
CVE: CVE-2026-23479 and 4 more

High

Description

Redis has identified and fixed a total of five vulnerabilities that allowed attackers to execute code remotely on its servers.

The issue was caused by several memory management vulnerabilities:

- CVE-2026-23479 and CVE-2026-23631, linked to Lua, allowed use-after-free conditions, while CVE-2026-25243 enabled invalid memory access through the RESTORE command. In addition, CVE-2026-25588 and CVE-2026-25589 extended these remote code execution risks to the RedisTimeSeries and RedisBloom modules through the processing of malicious data.

Affected Products

- All five vulnerabilities affect Redis OSS/CE and Redis Software versions up to and including version 8.0.6.
- The fixed versions include Redis OSS/CE 6.2.22, 7.2.14, 7.4.9, 8.2.6, 8.4.3, and 8.6.3.
- For Redis Software, the patched builds include versions 8.0.10-64, 7.22.2-79, 7.8.6-253, 7.4.6-279, and 7.2.4-153.

Solution

- It is recommended to update RedisTimeSeries modules to versions v1.12.14, v1.10.24, or v1.8.23, and RedisBloom to versions v2.8.20, v2.6.28, or v2.4.23.

References

- gbhackers.com
- nist.gov

 |

Update for n8n Due to Prototype Pollution Chainable to RCE

Date: 6 May 2026
CVE: CVE-2026-42231

Critical

Description

A security update for n8n has been released to address a critical vulnerability that could allow remote code execution.

The issue is a Prototype Pollution vulnerability in the processing of XML data within n8n, the open source workflow automation platform based on Node.js.

This vulnerability would allow an authenticated user to submit specially crafted XML content with the aim of polluting the global prototype of JavaScript objects.

Successful exploitation could enable an attacker to chain this pollution with other platform nodes, such as the Git node and its SSH operations, ultimately leading to the execution of arbitrary code on the affected host.

Affected Products

The affected products are:

- n8n versions prior to 1.123.32
- n8n 2.17.x versions prior to 2.17.4
- n8n 2.18.x versions prior to 2.18.1

The official advisory identifies the affected package as the npm package n8n.

Solution

It is recommended to:

- Update n8n to versions 1.123.32, 2.17.4, 2.18.1, or later releases.

References

- incibe.es
- security.snyk.io

Events

Infosecurity Europe 2026
2 June – 4 June

Infosecurity Europe 2026 will take place from 2 to 4 June 2026 in London, further strengthening its position as one of Europe's leading cyber security events. The conference will bring together experts, CISOs, technology vendors, and industry leaders to discuss emerging threats, artificial intelligence applied to security, digital identity protection, Zero Trust, and business resilience. The event will feature more than 300 exhibitors, specialised workshops, and technical sessions focused on the protection of critical infrastructure and cloud environments.

Link

Cyb3rWall 2026
2 June – 4 June

The C1b3rWall 2026 Congress will take place from 2 to 4 June 2026 at the National Police Academy in Ávila, strengthening its position as one of Spain's largest events dedicated to cyber security and digital training. Organized by the Spanish National Police in collaboration with the University of Salamanca, this sixth edition will be held under the theme "Cybercrime 3.0", bringing together national and international experts, law enforcement agencies, technology companies, universities, and professionals from the digital security sector.

Link

DES 2026 – Digital Enterprise Show
9 June – 11 June

The Digital Enterprise Show (DES) 2026 will take place from 9 to 11 June in Málaga, bringing together more than 15,000 international executives and technology leaders. Although primarily focused on digital transformation and artificial intelligence, the event will place significant emphasis on cyber security, digital resilience, and business protection against emerging threats. More than 500 international experts will participate, addressing topics such as cloud security, offensive AI, data governance, and the protection of digital infrastructure.

Link

CCI – The Voice of Industry Asturias
18 June

The Industrial Cybersecurity Centre will host the event "The Voice of Industry Asturias" in Gijón, a specialised conference focused on industrial cyber security and the protection of critical infrastructure. The event will bring together OT experts, industrial security managers, and companies from the energy, manufacturing, and technology sectors to discuss threats to industrial environments, operational continuity, and European cyber security regulation.

Link

Resources

➢ NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick Start Guide (QSG) – NIST

Published by the National Institute of Standards and Technology (NIST), this resource provides practical guidance for integrating cyber security risk management into an organization's broader enterprise risk management (ERM) strategy. The document is aimed at security leaders, executives, and corporate governance teams seeking to align digital resilience with strategic business objectives.
The guide explores areas such as risk governance, the definition of risk appetite, the management of technology risks associated with AI, IoT, OT, and supply chains, as well as the allocation of organizational responsibilities in the field of cyber security. It is an especially valuable resource for organizations operating under NIST frameworks or for those seeking to adapt their security programmes to more mature enterprise management models.

Link

➢ The State of Cloud and AI Security 2025 – Cloud Security Alliance (CSA)

Published by the Cloud Security Alliance in collaboration with Tenable, this report analyses how organisations are adapting their security strategies in response to the rapid growth of hybrid environments, multicloud infrastructures, and artificial intelligence. Based on a global survey of more than 1,000 professionals, the document identifies the main gaps between technology adoption and cyber security maturity. The report examines risks associated with generative AI, identity management, cloud data protection, exposure caused by misconfigurations, and threat automation. It also provides practical recommendations for strengthening organizational resilience and improving visibility across increasingly complex attack surfaces.

Link

➢ CIS Critical Security Controls v8 – Center for Internet Security (CIS)

The CIS Critical Security Controls v8 provide a set of prioritised best practices designed to help organisations prevent, detect, and respond to cyber threats. The framework is intended to deliver actionable and measurable controls that enable risks to be reduced progressively and effectively.

The guide includes recommendations covering asset management, identity protection, continuous monitoring, system hardening, cloud security, incident response, and security awareness training. Its practical and scalable approach has made it one of the most widely adopted standards among companies and public sector organisations for structuring cyber security programmes.

Link

NTT DATA

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com