WHITEPAPER

NIS 2 and Cybersecurity for OT Operations in the Water Industry

Unboxing the NIS 2 Directive: Elevating Cybersecurity to a Top Priority for Water & Wastewater Companies

General Overview

Water utilities are facing an inevitable surge in cyber-attacks, which poses a significant threat to system security and customer data. Due to its criticality and media impact, the sector has become an attractive target for cyber attackers. Furthermore, the expanding realm of digital transformation has widened the threat landscape, particularly in the field of OT.

Against this backdrop, the new Directive 2022/2555, known as NIS 2, aims to enhance the European Union's cyber resilience and awareness by establishing minimum standards for a harmonized regulatory framework and fostering greater cooperation among Member States. NIS 2 introduces mechanisms for effective collaboration between responsible authorities. Member States are required to transpose NIS 2 into their national legislative systems by October 17, 2024.

Unlike its predecessor, Directive NISD (2016), which did not recognize wastewater utilities as critical, NIS 2 encompasses both drinking water supply and distribution utilities as well as wastewater utilities. NIS 2 also introduces substantial changes to cybersecurity-related risk management and reporting obligations for water and wastewater operators. It not only imposes consequences for non-compliance, including fines and comprehensive audits, but also holds company leaders, including Boards of Directors and management teams, accountable. Additionally, it addresses supply chain cybersecurity and supplier relationships.

To ensure compliance with the Directive, companies should promptly initiate preparations to meet the requirements of the new legislation in each country, without delay.

This document delves into the key components of the Directive and proposes insightful suggestions for companies operating in this sector.

In this white paper, we answer:

- What are the main differences between the 2016 NIS Directive and the upcoming NIS 2, set to take effect in 2024.
- How NIS 2 will affect System Integrators and Product vendors.
- Technical Recommendations and Standards to Consider in OT Environments.
- When and How you should start.

What is NIS 2 and Why is it so important

The rapid rise of digital transformation has significantly complicated the cyber threat landscape. The water & wastewater industry, in particular, has become an enticing target for attackers due to its critical importance to society. With the safety of the population at stake and the management of millions of customers' private data, water utilities face an inevitable surge in both the quantity and sophistication of cyberattacks in the coming years. According to a comprehensive analysis conducted by GHD[1], it is projected that approximately a quarter of global water systems will have encountered a cybersecurity breach by 2025.

Furthermore, the European Union Agency for Cybersecurity (ENISA) has documented a significant 17% surge in cyber attacks targeting water supply services since 2018. It is worth mentioning that there have been multiple noteworthy incidents targeting water companies in 2022 and 2023.

- In April 2022, Donau-Stadtwerke Dillingen-Lauingen was hit by a cyber-attack that paralyzed their computer systems.[2]
- In May 2022, Alto Calore Servizi SpA, an Italian company responsible for supplying drinking water to nearly half a million people, encountered technical disruptions due to a ransomware attack. This incident hindered their ability to perform operations or provide any information that required accessing the database.[3]
- In November 2023, the Service public de l'assainissement francilien (SIAAP), responsible for managing 275 miles of pipes across four departments, suffered a suspected ransomware attack. As a precautionary measure to safeguard industrial systems, they were compelled to disconnect all external connections.[4]

> The water and wastewater industry is a prime target for cyberattacks due to its critical importance, with a projected quarter of global water systems facing breaches by 2025.

- In March 2023, Acea, a public holding company in Italy providing energy and services to Rome, was hit by a ransomware cyberattack claimed by the group BlackBasta. Acea confirmed damages but assured users that essential services were unaffected.[5]
- On February 20, 2023, LockBit breached Aguas do Porto, a Portuguese municipal water company. They threatened to release stolen data on March 7. Although the cyberattack affected services, the water supply and sanitation systems remained unaffected.[6]

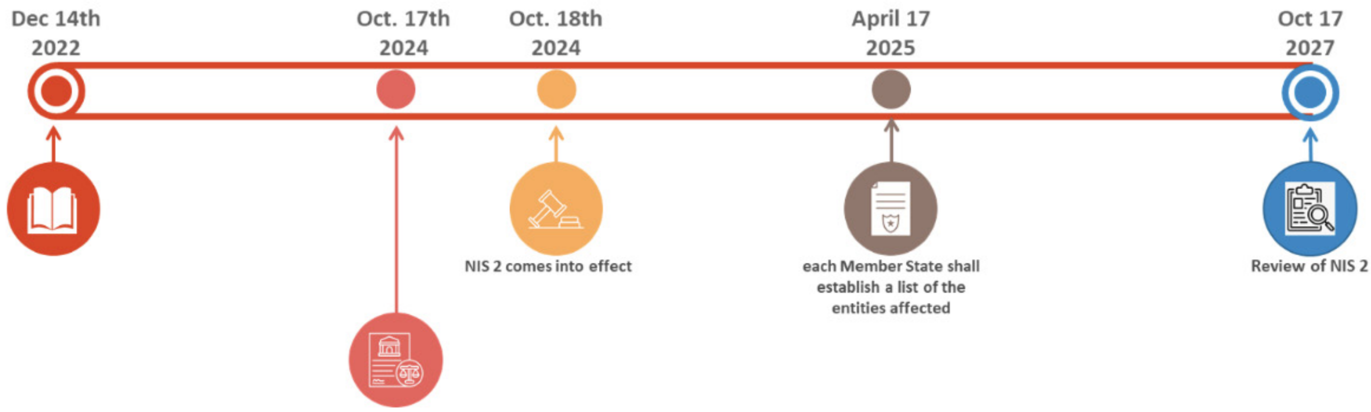
While the NIS Directive from 2016 made significant progress in enhancing the EU's cyber resilience and awareness, a review was necessary to ensure coordinated and innovative responses across all member states. The new NIS 2 Directive establishes minimum rules for a harmonized regulatory framework, aiming to align understanding and reduce inconsistencies between states. Given the interconnected nature of our world, it is crucial to have a unified level of cybersecurity across all states. The Directive will foster increased cooperation among member states, facilitating the sharing of information on cyber threats and incidents.

NIS 2 introduces mechanisms that promote effective cooperation among the responsible authorities in each member state. These mechanisms offer essential remedies and enforcement measures to ensure the successful fulfillment of obligations.

The Water & Wastewater Industry encounters distinct challenges, including legacy systems, physical security risks, resource limitations, insider threats, third-party risks, and attacks on control systems. To address these challenges, the NIS 2 Directive mandates that water utilities enhance their cybersecurity measures by allocating a larger budget, fostering coordination with other sectors, adopting risk management processes for Operational Technology (OT) systems, and potentially adjusting procurement practices to meet cybersecurity requirements. These steps aim to ensure a comprehensive and robust cybersecurity approach in the water industry.

Under NIS 2, operators will need to implement proactive risk management practices to prevent and minimize the impact of incidents. This involves adopting appropriate and proportionate technical and organizational measures to address security risks to network and information systems.

Key dates



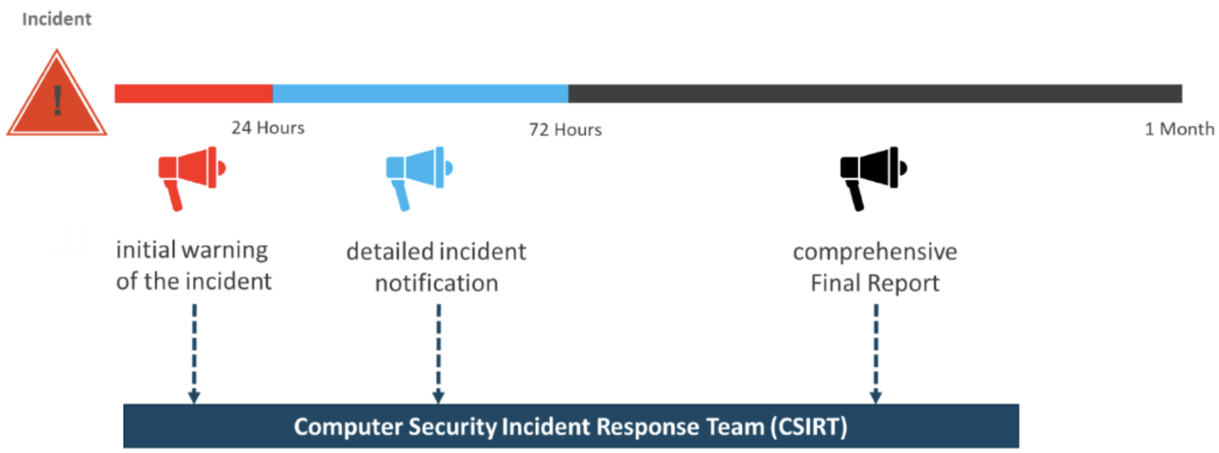
Sectors of High Criticality

- Suppliers and distributors of Drinking water intended for human consumption.[7]
- Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water.[8]

NIS 2 introduces the classification of entities into two distinct categories: Essential and Important. Here are the key distinctions between these two categories:

	Essential	Important
More than 250 persons and annual turnover > EUR 50 million and/or annual balance sheet > EUR 43 million	Yes	No
Less than 250 persons and annual turnover < EUR 50 million and/or annual balance sheet < EUR 43 million	No	Yes
Supervisory tasks by the competent authorities		
On-site inspections and off-site supervision	Yes, with random checks	Yes, ex-post
Targeted security audits	Yes, regularly	Yes
Ad hoc audits	Yes	No
Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned	Yes	Yes
Requests to access data, documents and information necessary to carry out supervisory tasks	Yes	Yes, ex-post
Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned	Yes	Yes
Requests for evidence of implementation of cybersecurity policies	Yes	Yes
Administrative Fines	**Essential**	**Important**
Maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover, whichever is higher	Yes	No
Maximum of at least EUR 7 000 000or of a maximum of at least 1,4 % of the total worldwide annual, whichever is higher	No	Yes

Mandatory Incident Reporting



Accountability

Management responsibilities with NIS 2 include:

- Approve the adequacy of cybersecurity risk management
- Supervise the implementation of risk management measures
- Keep up with training to identify risks and assess cybersecurity risk management practices and their impact
- Provide regular training to employees.
- Taking accountability for non-compliance

How to start

The NIS 2 Directive is a significant step in reinforcing the cybersecurity posture of essential sectors like water and wastewater, demanding a proactive, thorough, and coordinated approach to managing and mitigating cyber risks. The NIS 2 Directive, specifically under **Article 21**, mandates a comprehensive set of cybersecurity risk-management measures to enhance the security of network and information systems used by essential and important entities, including those in the water and wastewater industries. These measures are multifaceted and aim to address both technical and organizational aspects to manage and mitigate risks effectively.

Key requirements, with a direct reference to “Article 21”, include the following:

(a) Policies on risk analysis and information system

- **Start with a Risk assessment.** Risks to network and information systems should be analyzed and managed, considering factors such as exposure, size, likelihood of incidents, and impact.
- **Implement a risk management framework,** with appropriate and proportionate measures, that best fits specific needs and priorities.
- Different priorities in IT vs OT call for specific frameworks- ISO27001 for IT and ISA/IEC 62443 for OT.
- These frameworks prioritize **safety and availability in their approach to risk management.** This may be more suited for operational environments in OT.

(b) Incident handling

.

- Prepared routines and response plans are essential for effective management of incidents.

- Use established frameworks to develop robust response strategies.

- Implement advanced technologies for threat detection and monitor activity using intrusion detection systems (IDS), intrusion prevention systems (IPS), and Security information and event management SIEM, to identify breaches or ongoing attacks.

- Implementing a secure network perimeter, such as industrial firewalls, is critical to prevent malware and adversaries.

(c) Business continuity

- Apply a mindset that a breach will happen, it's just a matter of when.

- Create an Asset Inventory: maintain a list or database of all IACS and SCADA hardware (both physical and virtual) and software.

- Be sure to have a backup management established: Centralize your backups and automate what you can.

- Establish contingency plans ahead, patch and maintain all backup systems to the same level as the primary systems.

- Periodically verify that the fail-over systems will work properly when called upon.

- Well-documented crisis management plans are essential for success in handling breaches.

- Separate plans specific for OT are necessary, as priorities may differ from IT systems.

(d) Supply chain security

.

- Focus on securing the supply chain and relationships with direct suppliers and service providers.

- **System integrators** and **Product vendors** to address their own cybersecurity risks, with an adequately protected infrastructure, secure processes, and implement technical measures based on recognized standards such as ISO27001, IEC62443-4-1 and 4-2, and ISO9001 for quality management systems.

- Consider specific vulnerabilities and overall quality of products and cybersecurity practices.

- Use vulnerability management solutions to track vulnerabilities per vendor, product, and parts.

- Utilize software bill of material (SBOM) as input data for vulnerability management.

- Establish contractual agreements that address security compliance and advocate for secure development practices across the entire supply chain.

(e) Security in network and information systems

- Practices include security in network and information systems acquisition, development, maintenance (including patching and update), vulnerability handling, disclosure, cybersecurity training, use of cryptography/encryption where appropriate, human resources security.

(f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

.

- Organizations need to have a structured approach for cybersecurity evaluation and improvement.
- Clear objectives and metrics must be established.
- Assessment tools and techniques should be implemented.
- Regular review and reporting of policies and procedures is necessary.

(g) Basic cyber hygiene practices and cybersecurity training

- Train all relevant personnel and ensure they are aware of policies and procedures.
- Foster a culture of cybersecurity awareness among employees.
- Emphasize the importance of measures in place to protect against cyber threats.
- Enforce strong password policies.

(h) Basic cyber hygiene practices and cybersecurity training

- Ensure that there is appropriate handling of secret information like passwords and that they are transported in cyphered format.
- Use encryption for networks that are easily accessible to third parties and for remote access in any case.

(i) Human resources security, access control policies and asset management.

- Access control policies are mandated for each asset to ensure only authorized individuals have access.
- These policies can be implemented on the devices or controlled through the network.
- Use least-privilege access control policies and a Zero trust approach.

(j) Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

- Develop an access control policy that establishes appropriate logical and physical rules and rights for each user or group of users.
- Employ multifactor authentication for critical IACSs.
- Segregate data with high sensitivity and/or business consequence from other internal information.
- Establish separate IACS domains for each area.

Strategies to adopt NIS 2

Asset owners are advised to increase their security posture with 3 strategies:

Standardization

Utilize Standardized frameworks to leverage best practices on implementing better security processes, routines, and guidelines.

The first step in this is creating awareness and training for management and employees. Second is to implement a methodology to collect information about all the assets in place – a secure inventory with information on location, device types, firmware etc. Using frameworks, the asset owner can then complete a strategic risk assessment to identify where investments for protection must be made.

For IT security ISO27001 is a good base – it is also the base of the NIS directive and therefore covers some 90% of the requirements. ISO27001[9] functioning as a comprehensive rulebook, guiding organizations in safeguarding information and data against unauthorized access, use, or sharing. It establishes a structured approach to ensure the safety and security of information, particularly vital in contexts where continuous services are delivered.

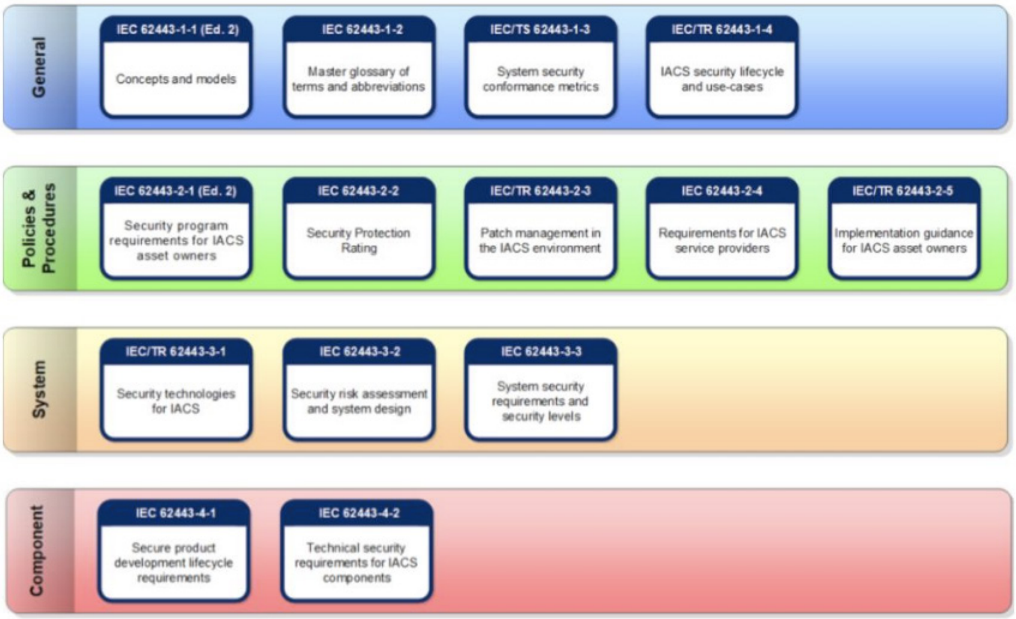
However, it focuses less on the inherent security of products themselves and has little specific OT environment requirements. OT is different than IT, the challenge lies in the misalignment of core values.

While the CISO is under scrutiny and often manages the OT security budget, it is the operational manager who bears the responsibility of ensuring uninterrupted factory production. The inherent conflict arises from differing priorities. IT professionals adhere to the CIA framework, prioritizing Confidentiality first, followed by Integrity and then Availability. On the other hand, Operational personnel, placing Safety at the forefront, prioritize Availability as the primary concern, followed by Integrity and, lastly, Confidentiality – forming the (S) AIC sequence.

This dichotomy results in conflict and friction, yet the underlying shared objective remains clear: safeguarding business continuity. Recognizing this common goal, both parties must collaborate to navigate these challenges and harmonize their approaches.

IEC/ISA 62443 is a complementary framework to ISO27001 focused specifically on Operational Technology (OT). IEC/ISA 62443[10], comprises rules and guidelines tailored for securing products used in industrial automation and control systems, offering developers and organizations insights on creating, testing, and updating software with security in mind. Its application is crucial for preventing cybersecurity threats that could compromise these critical systems. An asset owner will build their architecture – or system – with guidelines as described in 62443-3-3.

Product vendors will be required to use 62443-4-1 as a certification of their development process used when building the product. And 62443-4-2 lists specific features that a component/product must comply too. There are 4 different security levels: SL1 through SL4. Security Level 1 describes basic security and level 4 describes measures to protect against foreign power. For most operational environments level 1 will be a significant improvement – though many are expected to aim for level 2.



IEC62443 Framework[11]

Defense in Depth

Adopting Defense in Depth will ensure that Operational assets will be shielded off from IT as much as possible.

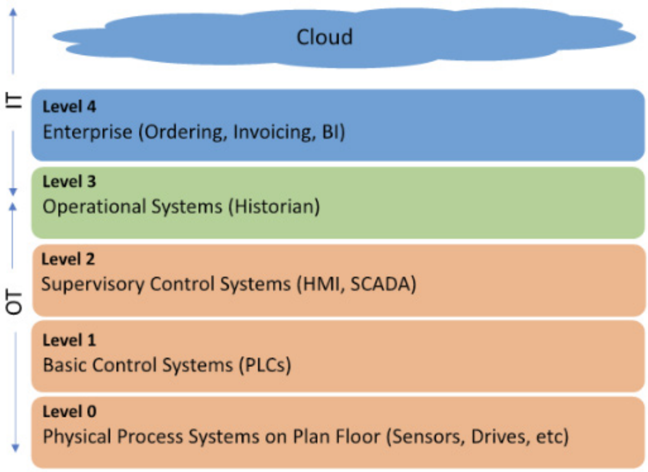
Enhancing the control of traffic within and between IT and OT requires deploying multiple layers of protection. However, it is crucial for asset owners to go beyond just implementing layers. The adoption of ISA/IEC 62443 Zones and Conduit Architecture should also be considered.

This approach involves segmenting assets based on their risk profiles and implementing conduits to isolate each zone. By doing so, lateral movement is prevented, breaches are contained, and the overall impact is minimized.

Following the best practices outline in the 62443-3-3 requirements for systems will greatly increase the security posture for the operational environment. To achieve this, asset owners are encouraged to create a Defense in Depth architecture starting with following the Purdue Model.

The Purdue Model[12] (The Purdue Enterprise Reference Architecture) is a reference model for enterprise architectures from the 90-ties still frequently used. In short it introduces layers to separate Manufacturing Systems from Control Systems from Business Logic Systems. Or simply separate IT from OT, with as many layers as possible creating a defense in depth architecture, making it more difficult for the attacker to reach the critical production systems.

Purdue Model



While the Purdue model has shown effectiveness, it may be considered simplistic when applied to the W&WW applications with a diverse range of processes and systems, each with varying levels of hazardness, and often located remotely and relying on public networks for communication. For instance, within a wastewater plant, the criticality of the disinfection process can differ significantly from that of pumping.

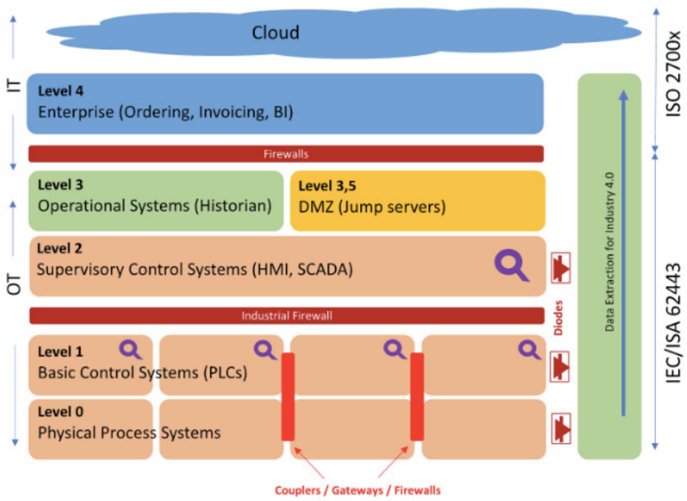
This is where the IEC/ISA 62443 standards come into play, providing guidance on how to structure the OT environment to accommodate these variations. The standards recommend the creation of zones, with each zone housing specific machines separated by conduits, enabling robust network segmentation.

This segmentation effectively isolates assets without hindering core processes. Conduits incorporate devices that tightly control communication between zones, allowing only necessary exchanges. By taking this approach, additional columns are introduced within the lower layers of the Purdue model.

Zoning is frequently implemented to isolate older assets that are difficult to upgrade promptly or are non-upgradable. Assets that fail to meet the minimum-security requirements for a zone require individualized protection, adding complexity to the architecture and making the management of the OT network more challenging.

The evolved Purdue model takes zoning into account, implementing segmentation within the lower layers. To enable unrestricted communication between machines where necessary, protocol gateways or couplers can be utilized. These devices allow industrial protocols between machines to communicate, while blocking all other IT and OT traffic from transferring between the zones. This way, PLCs can freely signal requests to their neighboring machines, while unauthorized traffic from hackers will be dropped.

Evolved Purdue Model



Device Hardening

In addition to ensuring a secure architecture, asset owners are strongly advised to prioritize the security of each individual asset or IoT device within their operations. These devices should be fortified with configurations such as secure passwords, multi-factor authentication, and audit logging. It is also crucial to consider the use of secure protocols, particularly when operating over publicly accessible networks. In cases where device hardening measures are insufficient, complementary products should be implemented to strengthen the perimeter around the specific asset.

Furthermore, to safeguard these devices, it is important that they adhere to a recognized security standard themselves. While the IEC/ISA 62443-4-2 standard provides specific guidelines on device hardening, it is important to note that this specification has not yet been widely adopted for device certification. The EU Cyber Resilience Act[13] however is one of the newest legislations and while not formally enacted yet, it aims to impose requirements on software and connected devices, necessitating minimum-security hardening and continuous updates throughout their lifecycle. This will enforce compliance, like the CE product safety standard, before a product can be sold on the European market. Anticipated to be adopted in early 2024 and enforced 36 months thereafter, it will prohibit the sale of non-compliant hardware and software in the EU.

While most products are certified through self-assessment, approximately 10% of products from manufacturers are expected to require third-party validation.

What is HMS posture in relation to Cybersecurity in Water?

HMS plays a crucial role in the water industry's supply chain, offering innovative Industrial ICT products and solutions. Our focus is on developing secure systems for system integrators and their customers. We specialize in manufacturing communication interface cards that are embedded in various industrial devices such as pumps, valve controllers, analyzers, drives etc. By leveraging our CompactCom IIoT & Secure solution, vendors can benefit from enhanced security features such as secure boot, certificate storage, and encrypted communication protocols like CIP Security, OPC-UA, MQTT, and Profinet Class 2 and 3. Our goal is to provide easy, embedded, and secure communications for a wide range of industrial applications.

Furthermore, with Anybus, we provide gateways that excel in protocol translation. These gateways are designed to ensure network security by isolating and filtering out all IT traffic. They also offer a seamless way to establish secure segmentation, enhancing overall network protection. The HMS Anybus Development organization is certified at Maturity Level 3 (62443-4-1), which signifies the implementation of secure development processes throughout the product lifecycle.

In addition, our renowned brand Ewon specializes in manufacturing secure gateways for data management and remote access. These gateways are further enhanced by Talk2M Cloud – with an ISO 27001 certification to ensure the appropriate levels of information security - providing a secure method to remotely access critical assets in the Water industry. When it comes to data management, our offering offers remarkable flexibility. For instance, it allows the collection of data using industrial protocols like Profinet or Modbus amongs others and facilitates its transmission to analytics systems through MQTT or secure connectors to platforms such as Amazon and

Azure, among others. Ewon products are compliant with IEC 62443-4-2 standards and are designed with a security chip integrated at the hardware level.

Last but not least, our Anybus Diagnostics solution plays a crucial role in detecting errors at an early stage, thereby maximizing uptime. It is capable of identifying various types of errors, including deteriorating cables, malfunctioning equipment, or suspicious network traffic.

Act now, don't wait

The NIS 2 Directive is a mandated regulation that carries heavy fines for non-compliance. However, it is ultimately the responsibility of each asset owner to take timely action and enhance their security measures. Frameworks like ISA/IEC 62443 can be invaluable in organizing the work and achieving the desired level of implementation. While the standard itself is not obligatory, asset owners must consider their desired maturity level to safeguard their operational platforms.

NIS 2 is set to come into effect in October 2024, and with local countries announcing their enforcement laws throughout that year, there will be limited time for implementation and compliance. It is strongly advised that asset owners begin the process of securing their organization and infrastructure as soon as possible, leveraging a well-established standard to guide them.

1 https://www.ghd.com/en/insights/cybersecurity-in-water

2 https://www.swr.de/swraktuell/baden-wuerttemberg/ulm/cyberangriff-donau-stadtwerke-100.html

3 https://therecord.media/italian-water-supplier-ransomware-attack-disruptions-medusa

4 https://www.siaap.fr/presse-publications/publications/detail/actualites/bulletin-cyberattaque/

5 https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-03.pdf

6 https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-03.pdf

7 excluding distributors for which distribution of water for human consumption is a non- essential

8 excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity

9 https://www.iso.org/standard/27001

10 https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

11 https://isagca.org/isa-iec-62443-standards

12 https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture

13 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

About the authors

Xavier Cardeña is the Water & Wastewater Dev Manager at HMS Networks. With 25 years of experience in the industrial automation and Internet of Things (IIoT) sector, helps companies achieve digital transformation of their operational technology (OT) operations. Working for OT Security for more than 10 years he is a Certified with ISA/IEC 62443 Cybersecurity Expert

Thomas Vasen is the Business Development Manager in Network Security at Anybus, a division of HMS networks. With over 25 years of experience in operations and security of telecommunications, military, and critical infrastructures, now focus specifically on helping companies manage risks and securing uptime in their operational technology (OT) environments.