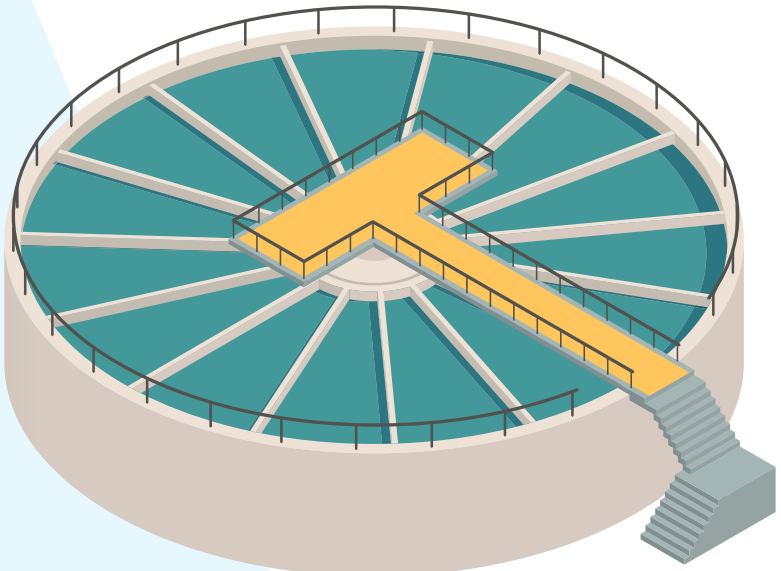
STORMSHIELD

Cybersecurity
in sensitive environments:

# Immersion in the water industry

White paper



# Three days...

## That's the life expectancy of a human being deprived of water. Hence the vital importance of this resource.



**But water is also necessary for agricultural and industrial activities and for the comfort of households. How long could companies continue to operate normally after the tap has been turned off, especially in a world affected by global warming?**

It is the job of players in the water sector – communities and private companies in delegated public service – to ensure we never have to find out. They hold a twofold responsibility towards people and the environment. Firstly, they must deliver continuity in the production and distribution of drinking water, while guaranteeing health security. Secondly, it is their responsibility to treat wastewater, in order to avoid pollution when it is discharged into the natural environment or reused.

In France, for example, the sector is sensitive enough to be coordinated by the Ministry responsible for Ecology and monitored on a daily basis by a sector coordinator from the ANSSI cybersecurity agency.

However, this dense industrial ecosystem, made up of drinking water production plants or wastewater treatment plants – some of which are classified as "operators of essential services" at European level – relies on ageing infrastructures and technologies which make it vulnerable. In addition, these operating systems are now much more exposed to cyber risk because, as a result of the digitisation of the sector and the arrival of new technologies, they increasingly find themselves connected to computer networks.

This phenomenon of IT/OT convergence is illustrated by the implementation of Ethernet IP even in factories, and also the development of Cloud solutions for industrial monitoring. This is an attractive attack surface for cyberattackers, who are often more proficient in traditional IT technologies than in specific industrial protocols.

In addition, whether in the United States or in Israel, cases of cyberattacks against water companies have multiplied in recent years. And around the world, companies and public institutions linked to the water sector are gradually becoming aware of the need to ensure the digital security of their critical infrastructures, sensitive data and

operational environments.

This increased cyber risk also highlights the fragility of a sector that has suffered from underinvestment. In Europe, as in the United States, water infrastructures are mostly managed by small organisations and generate low margins. Their industrial systems depreciate much less quickly than an office network, and they are often equipped with old-generation PLCs, increasing their vulnerability. And since an investment in cyber equipment has a direct impact on the price of a litre of water, these organisations must also address the need to control costs, in order to maintain general public access.

As a result of insufficient resources and immaturity in this area, water network managers have long prioritised the protection of public health over the protection of their information systems.—

**The objective of this white paper is therefore to enable IT managers, and the entire ecosystem of subcontractors (integrators and manufacturers) in the sector, to immerse themselves in an examination of the issue of cybersecurity in the water industry.**



In the following pages, we will offer explanations of issues in this sector and provide you with an operational inventory of possible solutions.

# Contents


**Figures to remember**

- **Infographic —** Mapping the water world

**PART I.**
**Why should the water industry take cyber issues seriously?**

**PART II.**
**A future of (cyber) water wars?**

- **Customer interview # 1 —** Point of view: cybersecurity, a habit the water industry is learning to acquire

**PART III.**
**What are the issues facing cybersecurity in the water industry?**

- **Infographic —** The sector's main vulnerabilities

**PART IV.**
**What cyber regulations exist in the water industry?**

**PART V.**
**What about tomorrow?**

- **Customer interview # 2 —** Securing a distributed network

# Figures
## to remember

**33,200**

**water abstraction structures** surveyed in France (FP2E, 2019). To prevent them from pollution, the water laws of 1992 and 2006 provide for three catchment protection perimeters (immediate, nearby, distant) and a mechanism to prevent diffuse pollution in the supply areas of these catchments. No mention of cybersecurity at that time.

**40 to 45%**

This is the **leakage rate** in water distribution networks in the cities of New York, London and Rome (compared to 20 to 25% on average elsewhere, according to Les Échos Investir, 2021). The aim is to plug these breaches using remote management and predictive maintenance.

**400**

**The number of inhabitants** of Chatsworth (North Georgia, USA) who were unable to use tap water for several days in 2013. The reason: an intrusion into the monitoring system for a drinking water installation in the city and changes to the settings of the fluorine and chlorine levels.

**46**

**The number of unsuccessful attempts** to penetrate the information systems of a wastewater treatment plant in Australia in 2000. Unfortunately, at the 47th attempt, the former technical service provider of the factory succeeded in taking control of it, dumping wastewater into the seabed.

**3**

**The number of cyber crises** related to water suffered by Israel alone in the year 2020. Between April and December, cyberattacks affected pumping and water treatment stations, water pumps and a recycled water tank.

**More than 3 in 5 vulnerabilities**

in industrial information systems can result in the total unavailability of the production tool if they are effectively exploited. And 72% of them can be delivered remotely. *(Claroty, 2020).*

**52%**

of the world's population will be living under conditions of water stress by 2050 (United Nations, 2019) – further emphasising the already strategic issues related to this resource.

**x2**

The water industry's operational systems have more than twice as many vulnerabilities as the health sector, yet particularly exposed during the health crisis.*(Claroty, 2020).*

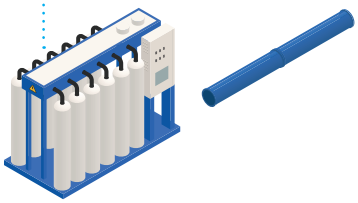
Infographic

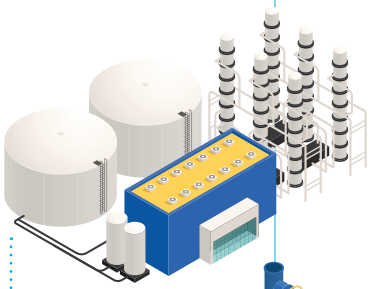
# Mapping the world of water

**From its abstraction to its use, including its treatment and transport, the course of the water cycle never does run smooth.** We dive into a non-exhaustive list of players in the water industry.

## The drinking water network

**Raw water abstraction**
(groundwater, bodies of water, rivers and streams)

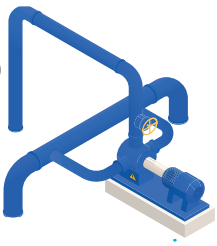




**Drinking water treatment**
(drinking water production plants, desalination plants)

**Drinking water storage**
(mainly water towers)

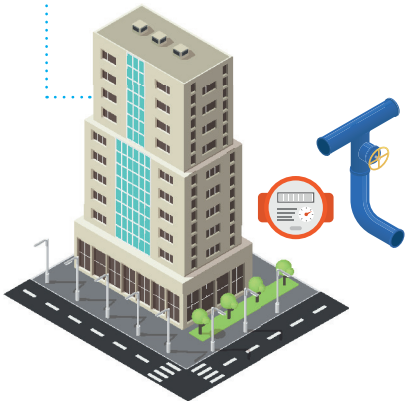




**Distribution**
via a network of pipelines

## Places of consumption or use

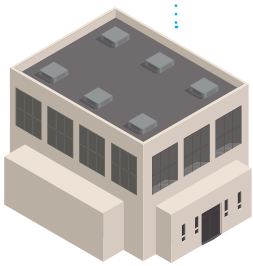
**Housing, shops and businesses**





**Crop and cattle farms**

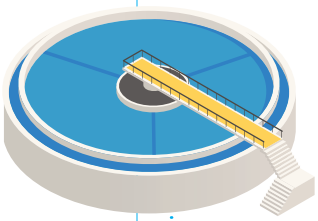
**Industries**



# The wastewater purification network

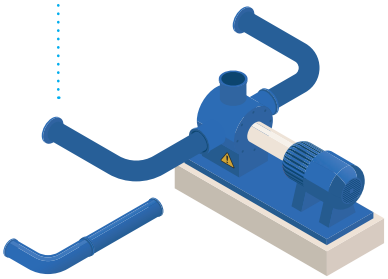


**Collection:**
sewer system for domestic wastewater



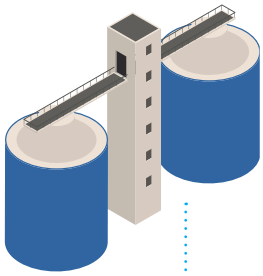
**Treatment:**
water reprocessing plants

Wastewater treatment plant or urban water treatment plants with treatment basins



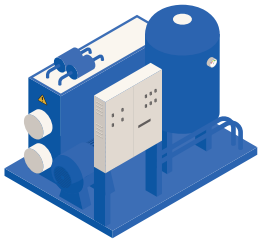
**Discharge:**
purified water evacuation systems

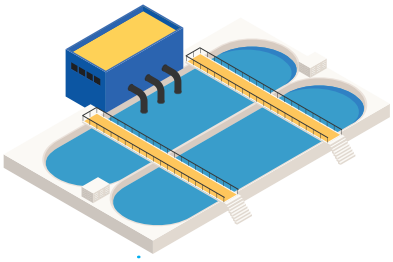
# The rainwater network



**Flood defence pumping stations**

**Municipal water pumping stations**



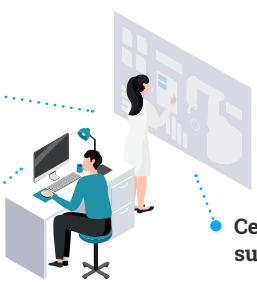


**Holding ponds**

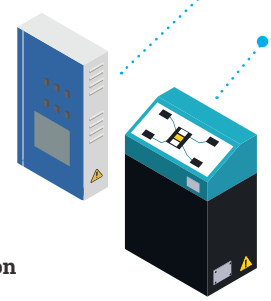
## Information systems within different infrastructures are often a mixture of many diverse elements. And all these elements constitute a significant cyberattack surface.

**Fixed assets (workstations, servers, etc.)**

**Mobile workstations**



**Central supervision**



**Remote control devices**

**IIoT (Industrial Internet of Things) communicating sensors**

**Cloud environments**



# Why should the water industry take cyber issues seriously?

**Part I.**

**The combination of public health, pollution and geopolitics makes cybersecurity issues in the water sector particularly critical.** However, despite the multiplicity of risks, caused in particular by the dilapidated nature of its networks, the industry is struggling to acquire the necessary digital security habits.



**Two main types of players operate water infrastructure: local authorities and private companies. This makes it difficult to draw up a uniform portrait of how these issues are handled, particularly with regard to cybersecurity investments.** The issue is a central one, however, given that more than 3 out of 5 vulnerabilities in the industrial information system can result in the total unavailability of the production tool if they are effectively exploited (source: 2020 Claroty report).

The ageing and infrequently updated operational systems of the water industry have more than twice as many vulnerabilities as the health sector (according to the same report by Claroty).

**But few companies in the water sector openly publicise the cyberattacks they foil, or to which they fall victim.** Unlike other industries, such as transport or energy, players in the water sector are only just starting to unite to discuss these cybersecurity issues. It is, however, worth mentioning the monitoring work of the Water ISAC network, which has been active since 2002 in the United States, and France's Association Scientifique et Technique pour l'Eau et l'Environnement (ASTEE), which initiated a cybersecurity working group in 2021.

**However, the sector has not been spared, as the case of a Florida water reserve in February 2021 demonstrated.** The highly-publicised (and thwarted) cyberattack in the small town of Oldsmar demonstrates the lack of security of a certain number of water infrastructures: the cyber-criminal was able to exploit a remote control software (TeamViewer) and change the setting for sodium hydroxide, used to regulate the pH in the water treatment network. Fortunately for the 15,000 residents of Oldsmar, a station agent quickly detected the anomaly (11,100 parts per million instead of 100), and corrected the concentration. It is true that the devices

> ***In a world that is increasingly connected and forced by the Covid-19 epidemic to make rapid changes, a cybersecurity problem can quickly generate a safety problem, or even raise the question of national security in certain extreme cases"***

**Khobeib Ben Boubaker**
Head of Industrial Security Business Line, Stormshield

embedded in these environments for operational safety can act as safeguards, yet the history of cyberattacks against the water world shows us that cybercriminals are able to bypass them.

Although, historically and culturally, **personal safety has always taken precedence over computer security** in the water sector, the two subjects tend nowadays to be merging into one. **The specific nature of cyber threats in the water industry** arises from the motivations of cyberattackers. This sensitive sector is not very lucrative, and consequently rarely targeted for profit. It can, however, be targeted for media stunts, as was the case in January 2021 in California: a cybercriminal was able to erase some programs used by a factory in the San Francisco Bay area in drinking water treatment processes.

**But most of all, an attack on a region's water infrastructure remains a potent tool for genuine destabilisation that can be used for political ends, as we will see in the next section.**—

# A future of (cyber) water wars?

**Part II.**

**As a vital resource, water has always occupied a strategic place in international relations.** This geopolitical dimension is reinforced by climate change at work, which is transforming the "blue gold" into an increasingly precious resource.



**At a time when water supply and treatment systems are generally connected to other networks (in this case, computer networks), their vulnerability is increasing. In Europe, this explains why some infrastructure in this sector bears "Operator of Essential Services" (OES) status, and must comply with regulatory requirements.** In France, for example, this statute is supplemented with another designating "operators of vital importance", accompanied in this case by strict regulatory obligations.

Cybersecurity in the water sector is therefore particularly critical, since it contributes to the security of an activity necessary for public survival and health. Control in this area is also a sign of a country's sovereignty.—

## The example of Israel and the 3 waves of attacks in one year

**Israel's geopolitical and geographical situation exacerbates water-related issues. This situation has caused it – along with the Gulf countries – to rely on technology. For example, 80% of the drinking water consumed in Israel is from desalination plants.**

In March 2020, Israel thwarted a series of cyberattacks aimed at gaining control over the industrial control systems of several of its water facilities. The aim of these attacks was apparently to increase the levels of chlorine in the water (in order to make it dangerous for consumption) and to cause pumps to shut down automatically. This would have deprived several thousand inhabitants of access to water during a period of intense heat. The Israeli government held Iran responsible, and appears to have carried out a retaliatory cyberattack on the Iranian port of Shahid Rajaee in response.

Two months later, agricultural water pumps were targeted by a second wave of attacks, but not damaged. Lastly, in December 2020, cyber-attackers broke into a water reservoir by exploiting a poorly secured Human-Machine Interface (HMI).

These Israeli examples show the extent to which cyberattacks are today an integral part of state arsenals in more or less open conflicts or intelligence efforts. In another area, Russia and China have been singled out recently following the cyberattacks against the European Medicines Agency (EMA) in 2020.—



## Is the water sector ready for cyber warfare?

**In general, levels of cyber protection in the water industry vary.** While some operators have included cybersecurity criteria in their calls for tenders for several years, the cyber risk is still undervalued at the local authority level. This partly explains how relatively basic attacks can sometimes infect industrial systems. Nevertheless, the entire water industry now seems determined to catch up with other sectors, such as energy and banking, which had been quicker to gain awareness.

"*In France, since the adoption of the Military Planning Law and the European NIS Directive, the ministries and ANSSI have done great work sensitising the relevant local authorities and companies to this issue.*, explains David Giorgis, IT and OT Regional Security Manager, France and Industrial IT Manager at Suez France. *Previously, cybersecurity received cursory mentions in the calls for tenders drafted by local authorities, with some exceptions. Today, the subject often occupies several pages, and answers are expected to include supporting evidence. It is the sign of a reassuring awareness and increasing skills for the future.*"—

Customer interview

# Point of view: cybersecurity, a habit the water industry is learning to acquire

**David Giorgis, IT and OT Security Manager and Industrial IT Manager at Suez France, has a front row seat from which to observe developments in the water industry.** We were able to ask him a few questions and take a deep dive with him below the surface of the cybersecurity industry.

**David Giorgis —** *"About 90% of cyber incidents we observe relate to management IT; that is, office automation, workstations, messaging, applications. It has to be said that our CRM contains the data of millions of direct customers, and that our IS must be accessible for consumption monitoring, among other things. These are all assets that require securing, in addition to the traditional vulnerabilities relating to messaging, for example.*

*Fortunately, on the IT projects side at Suez, the security-by-design approach is now universal. On purely industrial projects, this habit has not yet been adopted everywhere, because they are often managed locally and cybersecurity is developing to become an integral part of the culture. This means that these OT projects are increasingly secure, which is why Suez is implementing a comprehensive approach to cybersecurity in order to obtain maximum operational performance. The difficulty that we encounter, when working on the cyber-security of operational systems, is very often related to industrial protocols. Some large manufacturers have indeed made specific features to standard protocols, and security tools are improving to take account of them. Analysis is therefore limited, until the editor of cybersecurity solutions develops a specific module. It is therefore important for players in the sector to work together."*

**As part of his duties, David Giorgis regularly works with Suez France client communities. We asked him what were the most common recommendations issued in the field of industrial water cybersecurity:**

**DG —** *"A new collaboration always begins with an analysis of the existing system, to ensure that the available information matches reality. After that, we usually begin a negotiation phase aimed at renewing obsolete equipment and updating existing equipment. In reality, the goal is to be "as up to date as possible": we are sometimes forced to retain old operating systems, because business applications are not compatible with the most recent versions of these OSes.*

*The other major area for improvement involves segmenting the operational network. This represents a lot of work. It is also important to separate industrial ISs and management ISs (a key rule for Suez) or, if an exception has to be made, to ensure that the interfaces between the two are secured. This requires the deployment of a basic security foundation (antivirus, update, firewall, etc.). These are entirely standard actions in the world of management IT, but still novelties in the industrial sector in general, and water in particular."*

**The scale of the task prompts the question of how the teams on the ground are feeling: do they generally perceive cybersecurity as an impediment to their projects?**

**DG —** *"There has been a lot more talk in recent years about cybersecurity issues, so overall, industrial teams are very aware of its importance. I would add that the role of the person in charge of the security of information systems is not to impede a project, but to support it so that it takes the relevant security conditions into consideration. Our philosophy is to guide on-site industrial IT specialists towards complete, secure and national packaged solutions. Our central teams and our subsidiary Suez Smart Solutions, which specialises in industrial systems and their cybersecurity, are also available to help them in implementing these solutions."*—

> **A pragmatic and collaborative approach that ultimately seeks to establish cybersecurity as an effective support function in the daily life of operational teams.**

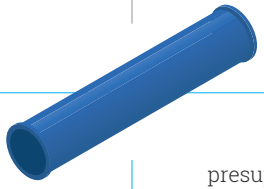
# What are the issues driving cybersecurity in the water industry?

**Part III.**

**In addition to state or criminal motives, what makes the water industry a prime target for cyberattackers?** We have listed the key cyber issues in the sector from three perspectives: human, technological and operational.



**To start with, it should be noted that in the water industry, the main aim of cybersecurity is to ensure the availability and integrity of industrial processes. The concept of confidentiality also comes into play, but within the less critical context of the customer relationship: data integrity is of very great importance in terms of telemetry to ensure accurate invoicing, but the issues are of a different order of magnitude when it comes to, say, guaranteeing the supply of drinking water.**



## Human perspective

**• Significant human risks inherent in the sector**
As we detailed in the previous section, the supply of drinking water and the treatment of wastewater are critical activities, as they are necessary for human survival and health. The consequences of a dam failure or water contamination would indeed be dramatic.

**• Risks of errors or malicious acts**
For these reasons, the human component – whether the result of an error or a deliberate malicious act – is one of the components most feared by business and industrial operators, and calls for different scenarios for optimal operating safety to be devised.

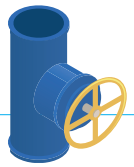
**• Occasionally complex collaborations**
From a business point of view, the coordinated management of IT and operational cybersecurity presupposes an ability to satisfy the needs of the automation engineer while reducing the risks identified by the CISO or IT security manager.

In organisational terms, for example, it is often the case that several players will work on a delegated basis for the same urban area. The urban area may itself retain part of the internal management. The result in such cases is a real water management ecosystem whose stakeholders must learn to work together.

**• Scopes that often exclude industrial cybersecurity**
As in other industries, it is common for teams in charge of operational cybersecurity to be placed under the responsibility of the plant manager, rather than within the scope of the local IT manager. In other cases, the IT manager will sometimes recommend cyber rules that the service operator is free to apply. Or not...

> ***"Industrial networks are sometimes overlooked when assessing cybersecurity risks, or when recovering from a cyberattack"***

**Tarik Zeroual**
Global Account Manager, Stormshield



# Technological perspective

**• A blurred line between IT and industrial cybersecurity**

With the end of the PSTN (switched telephone network), the water industry is gradually migrating to communication technologies such as Ethernet, 4G, and even 5G. This development is part of a global trend of convergence between IT and OT in recent years. This therefore leaves industrial networks more exposed than before, as they have entered the perimeter of a potential cyberattack via the computer network.

**• An Industrial Internet of Things (IIoT) to be secured**

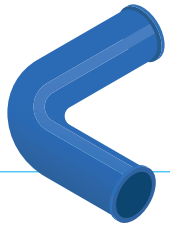
The IIoT refers to any connected object that sends information (temperature, open valve, chlorine level, etc.) to a machine. These relatively inexpensive "smart" sensors are very easy to integrate into existing systems, which explains their success in industrial settings. Unfortunately, they are also very vulnerable, because it is still all too rare for cybersecurity issues to be considered at the time of their design.

**• Protection to be extended to virtual environments**

With the adoption of the cloud – particularly when supplied with data by the IIoT – and the use of virtual machines, a whole section of water companies' information systems has been outsourced. It is therefore vital to secure these cloud links to avoid cyber-smurf attacks against the infrastructure of industrial sites. However, this requires clearly identifying whether the responsibility for this task will fall to business units or managed services.

> ***"Predictive maintenance is one of the main operational applications of the IIoT. The data fed back by the sensors are used for prediction calculations, eliminating unnecessary maintenance and reducing the probability of failure"***

**Tarik Zeroual**
Global Account Manager, Stormshield



# Operational perspective

**• Strong disparities in maturity**
In Europe, consideration of cybersecurity issues in water infrastructure varies greatly depending on the specific authority in charge's level of awareness and resources.

**• Multiple sites: a key source of cyber-complexity in the sector**
In practice, delivering cybersecurity for critical water infrastructure is not easy, because it is a very decentralised sector that is forced to operate multiple sites to supply the entire geographical area. Internet connections and remote maintenance therefore create major issues relating to the remote access methods that ensure remote sites operate correctly.

**• A difficult cyber implementation on the ground**
Due to their fragmented distribution, certain infrastructures in the water industry have specific constraints, such as humidity or temperature.

**• Sensitive production equipment**
It is not uncommon to find that an automatic device in operation in a wastewater treatment plant is already 10, 15 or even 20 years old. These ageing devices rarely have integrated cyber protection mechanisms and use insecure industrial protocols, and are therefore vulnerable.

**• A permeable network architecture**
These systems are still too often organised according to a "flat" network architecture; that is to say, without partitioning or segmentation. This poses a real risk in terms of the spread of malware.

**• A major time constraint**
The sensitivity of this equipment is also due to the constraint of real-time operation. In the water industry, it is essential to trigger each operation instantly, and therefore to minimise the time between the instruction and the action. Safety equipment must therefore generate as little latency as possible, to avoid disrupting the industrial process – which could result in a shutdown of production.

**• A variety of stakeholders, which can blur visibility**
Given the age of most industrial water systems, the current operator does not always have access to the past history of modifications. The use of numerous service providers, operators and integrators also serves to accentuate this phenomenon.

> ***"These distributed networks are also more prone to physical intrusion. It means thinking differently about cybersecurity. This safety issue adds complexity to the approach of cyber-securing a wastewater treatment plant or a water tower"***

**Vincent Nicaise**
Industrial Partnership and Ecosystem Manager, Stormshield

Infographic

# The main vulnerabilities in sector

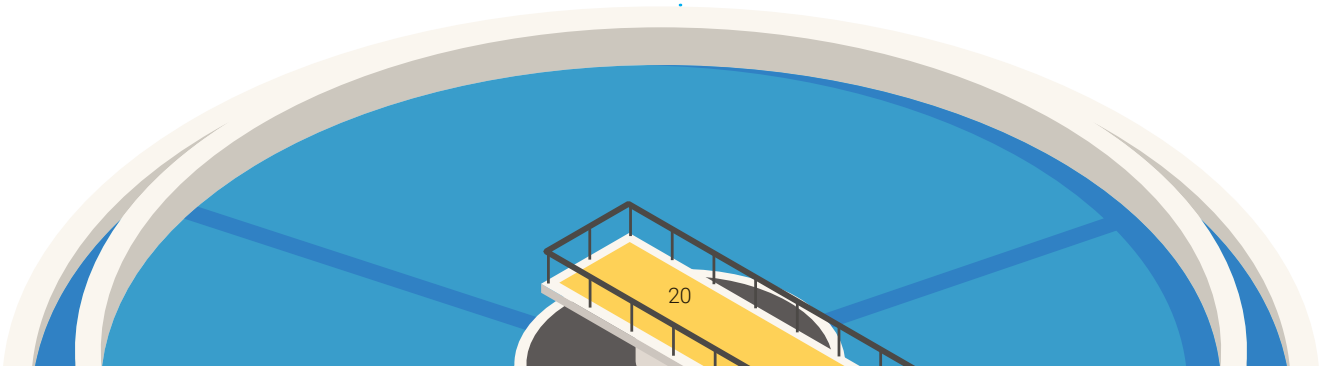
**In recent years, the concerns of cybersecurity professionals have focused in particular on the deployment of the "Industrial Internet of Things" (IIoT). However, this should not mean overlooking a certain number of structural vulnerabilities in these industrial systems.**

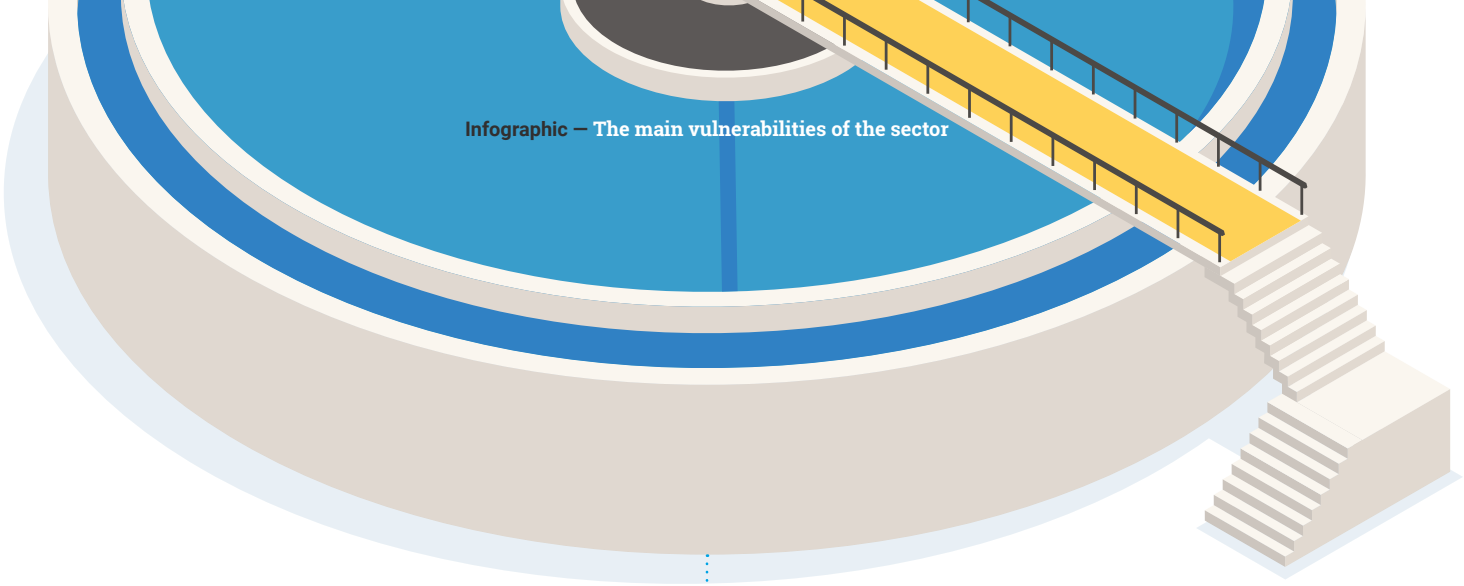
Industrial control systems (ICS) in general can present vulnerabilities at several levels:

## In operational equipment (software, hardware and firmware)

featuring disparate, ageing and/or insecure technologies. These include a jumble of the following: the DCS (for *Distributed Control System*), human-machine interfaces (HMIs), industrial programmable logic controllers (PLCs), SCADA data acquisition and control solutions and other supervision software, as well as the IIoT sensors and cloud platforms with which they communicate. Taken together, these form a considerable attack surface.

**In February 2020, a vulnerability was discovered in the C-more HMIs of the American manufacturer AutomationDirect.** These HMIs are used, among others, by operators in the water industry. By exploiting this flaw (CVE-2020-6969), cybercriminals were able to discover credentials and other sensitive information in unprotected project files.—





Infographic — The main vulnerabilities of the sector

## In the network and its peripherals

Often designed according to a "flat" architecture, industrial networks are not always isolated from each other, according to the principles of segmentation. In addition to being fertile ground for the spread of malware, network equipment has new vulnerabilities every day – because it is obsolete and infrequently updated. Such vulnerabilities can also be introduced by remote management, which is still too often performed insecurely.

## In protocols

The use of unencrypted, insecure protocols, such as Modbus, is common in industrial monitoring.

## In operating systems for monitoring or programming stations

These offline systems are rendered obsolete from a cyber point of view due to a lack of updates. But these systems are also the only ones that run some historical business applications, which are incompatible with more recent systems.

## In users

The operators and maintainers in charge of the industrial process do not yet all have a high awareness of cybersecurity issues. This means that user, password and access management policies are aspects that are too rarely used in industrial systems.–

# What cyber regulations are there in the water industry?

**Part IV.**

**In addition to its strict health and environmental oversight,** the water sector is subject to national and international cyber regulations.



***"With the implementation of the decrees in 2016, we began to see an acceleration in cyber-awareness from French operators. With the local authorities, it took a little more time and we saw initial changes in this area between 2017 and 2018"***

**Khobeib Ben Boubaker**
Head of Industrial Security Business Line, Stormshield

**In addition to its strict health and environmental oversight, the water sector is subject to national and international cyber regulations.**

In view of the public health challenges described above, it is easy to see how the activity of certain players in the sector is deemed to be critical. In France, the actors in charge of the supply and distribution of drinking water hold the status of OIVs (operators of vital importance) within the meaning of the French Military Planning Law (LPM) (2013). They must therefore comply with the 20 rules set by the LPM for the most critical ISs: IS mapping, monitoring, identification and authentication rules, incident notification, use of qualified security solutions at the highest level, etc.

At European level, they can also be identified as OESs (operators of essential services) under the NIS directive (2016). France had taken a little lead during its transposition into national law to include sanitation stakeholders: European harmonization is on its way, since this sector is expected to be included in the text of the directive during its planned revision in late 2021, just as with waste management.

Finally, some organisations – often small local authorities – are considered neither as OIVs nor as OSEs: without regulatory obligation, they therefore act according to their resources and their level of awareness of the threat. To help them, ANSSI has published several best practice guides for self-assessment and self-security. And for those who wish to go even further, many standards exist – including the IEC 62443-3-3 international industrial cybersecurity standard and the US NIST framework.—

# What about tomorrow?

**Part V.**

**Digital is a major driver in the protection of water:** taking only what is necessary, minimising the environmental footprint of factories and ensuring the delivery of quality water without leaks are all challenges that will increase in coming years.



**In its efforts to improve drilling and pump operation with machine learning, pick up weak signals warning of drought and predict future flows, the water sector is increasingly turning to technology.**

With the continued digitalisation of the sector, the boundaries between IT and OT will continue to blur, increasing the cyber risk to which the sector is already exposed. The water industry must therefore raise its cybersecurity levels and organise its cyber-resilience to enable it to cope with increasingly frequent and dangerous attacks.

## A fully educated audience and tighter regulations

Consequently, in the future, cybersecurity must be an integral part of maintaining the industrial process. This represents a significant task; almost all current infrastructure must be secured. But there are encouraging signs. In support of this process, the trend over the next few years will be to strengthen the regulatory framework for cybersecurity – according to David Giorgis, IT and OT Security Manager and Industrial IT Manager at Suez France. He believes the forthcoming revision of the NIS directive is a first step which will be followed by numerous adjustments made to France's Military Planning Law, among others. Cross-border cooperation should be one of the main axes of these new regulations, the ambition of which – according to the ANSSI cybersecurity agency – is to "*improve the cyber-resilience of the European Union and its members*".

> ***"Automation integrators are increasingly addressing the challenges of industrial systems. It is also encouraging to see the number of tenders for the design or renovation of systems that now include a cyber component"***
>
> **Vincent Nicaise**
> Industrial Partnership and Ecosystem Manager, Stormshield

So it is worth gaining an early advantage by following the advice of Tarik Zeroual, Global Account Manager at Stormshield, who is now recommending "*going beyond minimum compliance*".

## Tried and tested technological solutions

The future of the water industry will inevitably be tinged with cyber threats, but publishers and cybersecurity researchers are hard at work to offer solutions that address both recurring and emerging issues.

**• Protecting networks through segmentation**
Network segmentation is essential because it helps to prevent the spread of a cyberattack by isolating the subsystems. Firewalls such as those in the Stormshield Network Security (SNS) range can be used for this purpose.

**• Approving traffic**
It is also important to have solutions capable of verifying the legitimacy of commands issued by the PLCs. "*Not only to guard against man-in-the-*

*middle attacks, but also to verify the integrity of the data by inspection*", says Stéphane Prévost, Product Marketing Manager at Stormshield.

**• Managing remote access**

In a sector with infrastructures that can sometimes be very distant from one other, it is imperative to set up systems to manage and secure remote access (remote maintenance, alarm management, etc.). To ensure secure communications between the various sites and machines, the SNS solution handles data encryption through the creation of VPN tunnels and user authentication.

**• Obtaining an overview**

To facilitate the management of multiple distributed SNS solutions, Stormshield has developed a centralised management platform entitled Stormshield Management Center (SMC). Stormshield also offers a log management solution – Stormshield Log Supervisor (SLS) – which offers improved visibility on the status and logs of computer networks. These solutions also take into account the increase in traffic between the IT and the OT, thanks to a unified security policy between the two environments.

**• Protecting endpoints**

Endpoint protection is essential, whether engineering workstations or supervisory workstations, because of their key role in handling the parameters of the operational process and providing a real-time view of the state of the systems. For example, a cyberattack on monitoring stations would leave operational teams completely "blind" and prevent industrial processes from running properly. This is why the Stormshield Endpoint Security (SES) solution combines a behavioural analysis engine, a device control engine and the ability to perform application whitelisting, disabling any software that is not strictly necessary in order to provide better protection.

**• Adapting equipment to the constraints of the water industry**

The water industry has a number of specific physical constraints (high humidity, wide temperature ranges, isolation of certain sites, etc.), in addition to operational constraints for business continuity. This industry therefore requires equipment capable of meeting these environmental constraints. The functionality of SNS firewalls and their bypass functionality (safety mode) are also powerful assets for the water industry, because they ensure the availability of the operational process.

**• Striving towards *security by design*, even for OT**

The *security by design* approach consists of addressing cybersecurity issues from the earliest

## SNi40 and SNi20: industrial firewall solutions

**Stormshield has worked with Schneider Electric to design ruggedised enclosures that address the requirements of highly constrained environments, such as the water industry.** Optimized for low induced latencies and equipped with a bypass functionality (a safety mode that enables in-service maintenance), they can be easily installed in close physical proximity to the equipment to be protected, and can withstand the environments specific to this industry. At the regulatory level, the SNi20 and SNi40 firewalls hold the Standard qualification from ANSSI – evidence of its robustness and trustworthiness.—

system design stage. This is a more relevant – and preferable – approach in the water industry, given the after-the-fact integration of cyber measures. This is because of the relatively long development times, the problems of installed user bases that are even greater than in office automation, and the numerous technical challenges of compatibility with existing assets. Integrators and experts are therefore well aware that *security by design* is the key to a better-protected industry in future.

### New profiles for delivering cybersecurity in the water industry

As we have seen, delivering cybersecurity in the water sector today means relying on more and more tools. Many different skills are therefore needed to grasp, understand and make the best use of these resources.

In order for the monitoring and intervention teams (CSIRT, SOC, etc.) to have access to the best skills, it is therefore important for automation specialists to be trained in IT cybersecurity. And conversely, for cybersecurity specialists to become familiar with the industrial side.—

> ***"It is precisely because we are keen for our teams get to know each other and work better together that we run a cyber exercise each year, featuring a scenario that includes industrial systems, and with the participation of our OT specialists"***

**David Giorgis**
IT and OT Security Manager and Industrial IT Manager at Suez France.



**IT and OT systems may be converging, but is the same process now under way among their respective human teams? Time will tell, but cybersecurity in the water industry over the coming years seems to depend on the ability of industrial and cybersecurity experts to work together in co-constructing relevant solutions.**

Do you have a complex cybersecurity issue? A security project involving specific infrastructure? Our internal experts are here to discuss it and provide you with the support you need.
**Contact us.**

Customer interview

# Securing a distributed network: how to improve the cybersecurity of a city's water authority

**The local city authority of a major French region has chosen to entrust the management of the public service for producing, transporting, storing and distributing drinking water** across most of its geographical area of responsibility to a single point of contact, after several years of working with three different operators.

**1.3** million inhabitants

**60** municipalities

**100** water towers

### Modernising its IT infrastructure and raising its level of security

This service rationalisation process also provided the city authority with an opportunity to review its IT architecture, making it more modern and more secure.

The primary operator selected by the customer turned to Stormshield for support in securing this industrial environment and implementing the key required functionalities; i.e. the control and filtering of each communication (using *Deep Packet Inspection*, DPI – and with special attention to the Modbus protocol) and the implementation of an IPSec VPN solution to protect communications.

Firewalls were set up to segment and better protect the various operational networks (IT office network, central VPN concentrators, industrial and security IT, and also remote sites).

**An industrial response tailored to the constraints of the water sector**

For example, security at the central site has been reinforced by the installation of firewalls between the office network and the business installations. These installations are spread across two separate networks (security and industrial), each protected by a cluster of firewalls designed to act as VPN hubs.

This architecture interconnects these same applications to the various water towers, which were individually fitted with two clusters of SNi40 ruggedised firewalls, securing the flows between the various sites and applications.

The customer was also highly impressed with the Stateful DPI functionality of industrial protocols, which will take security in these sensitive systems to a new level, in parallel with modernised infrastructures.

**Services designed for these complex industrial environments**

To guarantee service to users and address accessibility and sensitivity issues at certain sites, Stormshield and the selected operator have set up appropriate support mechanisms, including:

• The implementation of a procedure enabling a technical agent with no network/security skills to replace a failing firewall and restore the site to operational status with the appropriate level of security,

• the activation of the bypass functionality (a safety mode that enables in-service maintenance) at the 5% of sites that are equipped with a single firewall instead of a cluster,

• a range of professional services to support the city authority in its process of industrialising configurations at the initial pilot sites.—

## Three key factors for an effective response

- Strong involvement of the **operator / publisher partnership**, making it possible to manage the project and ensure its successful and speedy end-to-end deployment.
- A **Stormshield industrial offering that adapts** as well to managing standard sites as it does to environments with strong industrial constraints (temperature, humidity, DIN rails, industrial power supply, bypass).
– A **single unified firmware** deployed across the entire Stormshield Network Security range and a **single management console**, Stormshield Management Center, to manage all firewall assets.—

STORMSHIELD

The European cybersecurity choice




All over the world, companies, government institutions and defence organisations need to be able to rely on trusted partners to support their digital transformation and provide cybersecurity for their infrastructure, users and data. Stormshield technologies are certified at the highest European level (EU Restricted, NATO Restricted, Common Criteria EAL3+ / EAL4+, ANSSI qualifications and visas), and address IT and OT challenges to protect your business activity. **Our security solutions restore your freedom to do business with complete peace of mind.**

**www.stormshield.com**

All distribution, reproduction or representation, even in part, of this white paper, for any purposes other than private use, regardless of the medium, is prohibited, and may engage the civil and criminal liability of any person failing to comply with this prohibition.