Journal of
Cybersecurity and Privacy

MDPI

Article

Water-Tight IoT–Just Add Security

Guillaume Bour [1,*], Camillo Bosco [2], Rita Ugarelli [2] and Martin Gilje Jaatun [1]

[1] SINTEF Digital, Strindvegen 4, 7034 Trondheim, Norway
[2] SINTEF Community, Børrestuveien 3B, 0314 Oslo, Norway
* Correspondence: guillaume.bour@sintef.no; Tel.: +47-40-00-51-00

Abstract: The security of IoT-based digital solutions is a critical concern in the adoption of Industry 4.0 technologies. These solutions are increasingly being used to support the interoperability of critical infrastructure, such as in the water and energy sectors, and their security is essential to ensure the continued reliability and integrity of these systems. However, as our research demonstrates, many digital solutions still lack basic security mechanisms and are vulnerable to attacks that can compromise their functionality. In this paper, we examine the security risks associated with IoT-based digital solutions for critical infrastructure in the water sector, and refer to a set of good practices for ensuring their security. In particular, we analyze the risks associated with digital solutions not directly connected with the IT system of a water utility. We show that they can still be leveraged by attackers to trick operators into making wrong operational decisions.

Keywords: security; water; IoT; digitalisation

Citation: Bour, G.; Bosco, C.; Ugarelli, R.; Jaatun, M.G. Water-Tight IoT–Just Add Security. *J. Cybersecur. Priv.* **2023**, *3*, 76–94. https://doi.org/10.3390/jcp3010006

Academic Editor: Danda B. Rawat

Received: 3 January 2023
Revised: 7 February 2023
Accepted: 15 February 2023
Published: 1 March 2023

1. Introduction

The ongoing digitalization across all industries will revolutionize the way critical infrastructures operate. The water sector is no exception, as water utilities in Europe are working on integrating new digital solutions to both help them optimize and monitor their processes, but also to make operational decisions and facilitate remote operations. A typical example of such a solution can be a set of Internet of Things (IoT) sensors deployed in water bodies to monitor the level of a specific bacteria, such as *E. coli*, to help decide whether or not to open bathing sites.

Water critical infrastructures have strict cyber security requirements such as the Supervisory Control And Data Acquisition (SCADA) system being separated from the Internet, and a series of firewalls preventing access to the Operational Technology (OT) system. One of the reasons for this separation is that SCADA systems are not developed with cyber security in mind. This model has proved to be effective in securing the infrastructure, but it also limits the overall productivity and efficiency. When the SCADA system is isolated, utilities cannot automate decisions based on data collected by environmental sensors for instance. The introduction of digital solutions to the system, while solving these issues, also introduces new risks that must be identified and mitigated to maintain or improve water utilities' security to the level they are at today. Even if attacking digital solutions has little value in itself, being able to leverage such an access to perform a supply chain attack on a water utility becomes valuable for malicious actors.

To this day, research has been focusing on protecting water infrastructures against cyber-physical attacks and threats [1]. While it is vital to protect water infrastructures, to best of our knowledge, no-one has looked at the (technical and operational) risks of integrating digital solutions with water utilities. This is partially because such solutions are usually not connected to the water utilities directly, but also because there is a race to market, and security is not a priority.

We have analyzed the risks of the digital solutions developed as part of the European project Digital Water City (DWC) and derived a high level classification of attacks against

them. As the IoT-related risks were a blind spot during our conversations with water utilities, we performed a security assessment on a typical IoT-based solution in order to raise awareness about these risks. We show that while the solutions might not be directly connected with the water utilities' systems, they pose a risk for supply chain attacks and/or can be misused to lead to incorrect decisions being made.

In this paper, we first cover known security breaches in water critical infrastructures, followed by the work that was performed in the STOP-IT project on the same topic (Section 2). We then introduce the Digital Water City project and the different kind of digital solutions that will be integrated as part of it. A threat landscape for these solutions is then given in Section 3. Before generalizing the vulnerabilities found in IoT-based digital solutions, we present the case study on which we base our results in Section 4, along with the methodology that was used. We discuss the results in Section 6, and conclude in Section 7.

2. Background

2.1. Related Work

The H2020 STOP-IT project [1] presented a number of approaches for assessing and treating risk on the strategic and tactical level, as well as specific tools and technologies for cyber and physical protection of water infrastructures at the operational level. New methods and tools are embedded in the so-called STOP-IT Platform.

The STOP-IT platform consists of different "building blocks" that can be used standalone or in combination with each other [2]. The platform allows users to choose technologies that are relevant to the specific challenges they face on a daily basis, while also having the opportunity to expand by adding more components at a later date. This facilitates improved protection against combined cyber–physical threats and analysis of cascading effects of physical and cyber incidents. The platform was validated in an operational environment, and all solutions have been demonstrated in real environments. The STOP-IT platform is structured into nine modules that bring together technological solutions and analysis tools:

- Strategic and tactical tools are analytical tools designed to support managers and decision-makers in their efforts to increase preparedness against the impact of cyber–physical threats to the service to be delivered. They generate custom scenarios for attacks, assess risk in terms of service disruptions and calculate the effectiveness of risk mitigation measures to increase system resilience.
- Operational tools support the real-time operation of the integrated system by providing a comprehensive list of technologies to detect anomalies of various natures, such as jamming, IT attacks, physical intrusion, abnormal activity, loss of data availability and integrity.

The overall risk management method adopted by STOP-IT is inspired by the risk management procedure from ISO 31000 which consists of five steps: "Establishing context", "Risk identification", "Risk analysis", "Risk evaluation" and "Risk treatment". Compatibility with the standard is key for the STOP-IT framework to interact with existing procedures in the water sector.

"Establishing context" is a prerequisite for a risk management plan, defining the scope of the risk management process, the main objectives of the tool and sets the criteria according to which the risk is to be assessed. "Risk identification" generates a comprehensive list of potential risk events that may affect a water supply system. In STOP-IT, this has resulted in the creation of a Risk Identification Database (RIDB) [3] which covers the identified risks at strategic, tactical and operational levels, and which is applied to the entire water system.

The STOP-IT RIDB contains risk incidents involving physical and cyber threats. For each incident, RIDB describes the type of source of risk (e.g., external attacker, external contractor, human error, interdependent critical infrastructure, internal attacker); type of threat (physical and/or digital); type of event (destruction, interruption, manipulation); the specific element (physical or digital) where the source of risk arises (e.g., control

center, control system, dosing system); in which part of the infrastructure the risk arises (e.g., catchment area, pipeline, drinking water reservoir, pumping station); the impact caused by the incident (financial, quality, quantity, reputation); and a brief description of the incident. The purpose of RIDB is not to replace the comprehensive identification of risk events for each water network operator. Instead, the examples from RIDB can allow users to start analysis and become aware of some possibilities that should be explored when local conditions develop that indicate that an event may occur. During the development of the RIDB, several meetings were held with each water network operator involved in the project. RIDB currently covers 81 incidents that have been identified as the most relevant. RIDB will be a live database that will be updated and reviewed regularly.

RIDB comprises generic risk events that can apply to the entire industry, so RIDB does not contain sensitive information. Once the risk events are selected from the RIDB, the characterization process that includes specific and sensitive information about a given water supply system can begin, detailing a potential attack scenario.

"Risk analysis and evaluation" and "Risk treatment" at the strategic and tactical level are carried out within a framework for risk assessment and treatment, comprising the following:

- A scenario planner [4] designed to help the user select the threats to investigate, based on RIDB and generic STOP-IT fault trees. It enables users to build scenarios of attack to be investigated further and simulated in the stress-testing platform (see below).
- An advanced toolkit [4] simulating the water distribution system as a cyber-physically integrated model, where system performance under scenarios of attack can be assessed. Both water quantity and water quality effects are simulated.
- A Risk Reduction Measures Database (RRMD) [5] provides advanced options to support the identification and selection of appropriate risk mitigation measures (RRMs). RRMD is connected to RIDB. It is implemented to aid in selection and assessing the effectiveness of RRMs to increase system performance under a given attack scenario.
- A stress-testing platform [6] that can simulate both physical and cyber systems (e.g., from SCADA to PLC and monitoring). It is possible to implement network protection solutions and see how they respond to cyber attacks. The platform makes it possible to analyze, for example, the effect of introducing malware to the monitoring system and tracing these effects to key indicators.

The solutions offered by STOP-IT at the strategic and tactical level aim to support planning decisions and evaluation, and to increase preparedness through the assessment of system performance under one or more potential attack scenarios. The assessment of multiple scenarios helps identify the critical parts and their significance in delivering set service levels.

STOP-IT has also developed the TORC organizational-stress-testing platform [7] as a complement to the technical one described above. Through a role-playing stress test, the organization's resilience and ability to respond in crisis situations in the event of cyber/physical attacks is established. It also makes it possible to document available processes and solutions for managing stressors and improve these by identifying the gaps and possible solutions.

"Risk Identification", "Risk Analysis and Evaluation" and "Risk Treatment" at the operational level are supported by an analytical platform for real-time recording, analysis and visualization of cyber and physical security incidents affecting water infrastructure. In addition to the strategic and tactical tools, the project's innovative contribution is the ability to combine cyber and physical security incidents in addition to the ability to detect complex attack scenarios in real time.

2.2. Digitalization of the Water Sector (DWC Example)

The DWC project aims at creating digital solutions to link water management in the physical world to the digital spheres such as sensor networks, real-time monitoring, machine learning, etc. Twenty-four partners from ten countries work together to integrate

a subset of the digital solutions in the cities of Berlin, Copenhagen, Milan, Paris and Sofia. The objective is also to support water utilities and municipalities in improving water quality, returns on investment and public information about water-related issues [8].

Water supply belongs to critical infrastructures and, as such, must follow industry-specific standards and/or regulations. When integrating digital solutions, the utilities communicate those requirements to the technology providers, which have to meet these regulations.

The data from the DWC solutions are fully processed outside the utility systems and fed into internal databases and/or numerical models. However, because internal IT security standards might have prevented the use of cloud solutions, standalone applications and on-premise servers were sometimes requested. The project provides devices, typically sets of specific sensors, mobile applications or web platforms which, to a large extent, build on top of existing solutions. Sensors themselves are mostly off-the-shelf, proprietary or open-source. Within DWC, new sensor assemblies are tested, they are applied to new setups within the water and wastewater infrastructures, and new ways of data transfer and processing and visualization tools are developed. For any sensor implementation, it is important to distinguish between sensors that are directly connected to the SCADA system to monitor and regulate operational conditions, and independent installations in online or offline mode with data transfer into the databases and reporting systems connected to the office world. Data transformation and processing is accordingly performed either fully automated within the SCADA system or manually to semi-automated when reading, recording and processing the office world data. OT and IT systems are usually not directly connected, but data are pushed from the operational systems to central databases, where they are stored and accessed for decision making.

A major challenge for urban bathing water management is to ensure the safety of users and comply with regulations. The European Bathing Water Directive (BWD) [9] uses the concentration of fecal bacteria to assess the water quality. Currently, bathing water surveillance in Europe is usually based on monthly grab samples analyzed in approved laboratories. This means pollution events are only detected by chance, as most of them will happen between sampling times. The ALERT System, developed as part of DWC, is a sensor for real-time bacterial measurements. The device is fully autonomous, remotely controllable, installed in-situ and allows rapid quantification of E.coli or enterococci concentrations [10]. This eases the job of operators who can rely on more accurate and up-to-date data to decide whether or not to open bathing sites for instance. Another challenge for water utilities is the management of drinking water wells. Well rehabilitation represents a major element of annual investments and expenses to maintain service quality. This maintenance is based on the condition and capacity of the well, obtained by performing pumping tests and CCTV inspections. The corresponding solution developed in DWC is a mobile application allowing the collection of data from sensors deployed in the wells. Having these data readily available will greatly reduce operating expenditure by accelerating maintenance procedures and enable focus to be shifted onto the wells with the highest needs. It is the perfect example of data being used to improve decision-making [11].

Digital solutions developed as part of the DWC project are built using a wide range of technologies, making it difficult to generalize anything. However, based on discussion with technology providers and water utilities, we have classified solutions in three subsets, based on their level of integration with the water utilities:

Standalone solutions: These are solutions which are not interacting with any sensors or utilities. They can be web or mobile applications, publicly available or requiring authentication.

Solution with "external" sensors: These are the solutions that are gathering data from sensors "in the wild", using some long-range wireless technology (mobile networks, LoRa or Sigfox for instance) or manually gathered using most likely shorter-range wireless protocols, such as Bluetooth (low energy).

Solution with "internal" sensors: These are the solutions that are gathering data from sensors that are placed in the water utilities (but not necessarily connected to their systems).

While none of the solutions are directly connected to the water utilities in DWC, there will still be interactions, especially by operators accessing the application in order to make decisions. As such, we identified two major risks for water utilities when integrating/using digital solutions:

Supply-chain attacks: As already mentioned, water utilities, being critical infrastructures, must comply with strict regulations. It is safe to assume that they undergo regular audits and are supposed to be a difficult target for attackers to find entry points. This is the case for many industries and companies. To counter this, attackers might identify actors evolving around the main target and attack these companies instead, to later on leverage the trust in these companies as a means to attack the real target. This is called a supply chain attack and has been used successfully by attackers in the past. The most damaging one in recent years is the SolarWinds Supply Chain Attack discovered in December 2020. The network management system used by hundreds of thousands of companies was shipped with a malware, successfully hitting many high-value targets such as the US Federal government [12]. In January 2021, for instance, vulnerabilities in the Microsoft Exchange server were used to compromise hundreds of thousands of servers all around the world, including the European Banking Authority and the Norwegian Parliament [13,14]. More recently, there have been several cases of malicious node packages being uploaded to npm (npm is a package manager for the JavaScript programming language) as an attempt to target companies such as Azure, Uber or Airbnb [15].

Being led to take wrong operational decisions: Most of the digital solutions, while not interacting with the water utilities, provide crucial information to the operators of a water utility and are used as a decision support tool. The interoperable decision support system and real-time control algorithms for stormwater management for instance, can be used by operators to predict the best maintenance window, thus optimizing the process. If the information is erroneous, though, it can lead to a release of untreated water in the environment as a direct result of the wrong planning. Similarly, if the early warning system for bathing water quality reports an incorrect value, so that bathing is authorized despite the quality being below the threshold, this can have disastrous consequences (both from a public health perspective, but also from a public relations one).

Digital solutions vary a lot when it comes to the technologies used and to the services they provide, but it is possible to derive a high-level diagram of their architecture. Figure 1 presents such a diagram for DWC's solutions. Most solutions are only composed of a subset of the components presented here. The main components include

Data sources: Digital solutions usually rely on external data, which are then analyzed and/or transformed to provide added value. These data can take various shapes: some solutions collect environmental data using IoT sensors deployed in the wild (water sources, sewer network, etc.), others use data from third-party services (weather or terrain information for instance) or even drones. The applications developed by a solution can themselves be considered as a data source, for instance when collecting data from an off-line sensor using Bluetooth.

Solution infrastructure: Most solutions rely on a backend infrastructure to operate their service. Infrastructure here refers to anything that supports services run by a digital solution and can consist of on-premises servers, cloud ones but also third-party services used as part of the data collection (Sigfox's network for instance). Network providers used for data collection are here considered as part of the solution infrastructure, contrary to the other external services described in the next point.

Third-party services: These are the third-party services used by a solution to provide their own service, such as services providing SMS or email-sending capabilities.

Solution's services: Solutions provide a service to water utilities/their users. This can be, for instance, an alert if the level of the *E. coli* bacteria is too high in a water basin. A service can be exposed to the users in various forms, such as a web or mobile application, but also simply via an Application Programming Interface (API).

Users of the solution's services:

- Regular users: Users of the service are, for instance, operators in a water utility who need to take operational decisions based on the information they receive from the digital solution's service. A good example could be operators visualizing on their application that the level of *E. coli* bacteria is higher than a given threshold in a water basin and deciding to forbid swimming there.
- Machines: If the service is exposed via an API, it might be used by another solution to develop something novel, or directly by a water utility to integrate it within their own system.

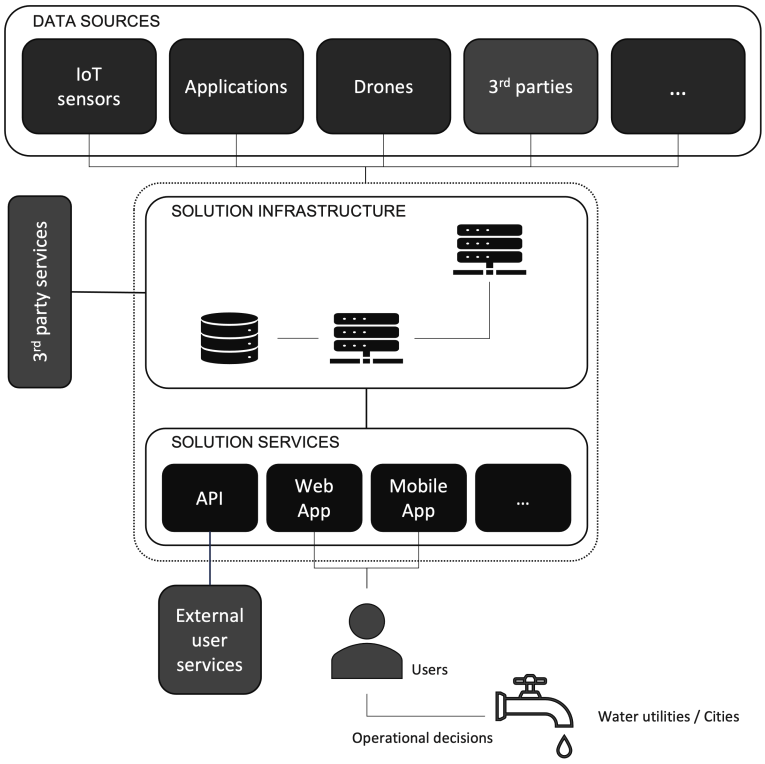


Figure 1. Generic architecture diagram for a digital solution in DWC.

3. Threat Landscape

Motivations for attackers to attack digital solutions exist, independently of their level of integration with water utilities, and this justifies the need to ensure they are secure as well [16,17].

As presented in the previous section, digital solutions can be complex and might interact with several external actors to collect data, access services or to simply provide their own service to their users. Attackers thus have a wide choice of attack vectors when targeting a digital solution, such as IoT devices, applications, third-party services, etc.

Building on the Risk Identification Database (RIDB) which gathers the generic risk events associated with the implementation of the digital solution of DWC by the cities, one can derive a classification of the attacks to the digital solutions in DWC. This classification is presented in Figure 2, and groups the attacks in six different classes which sum up the different types of attacks that can relate to a digital solution:

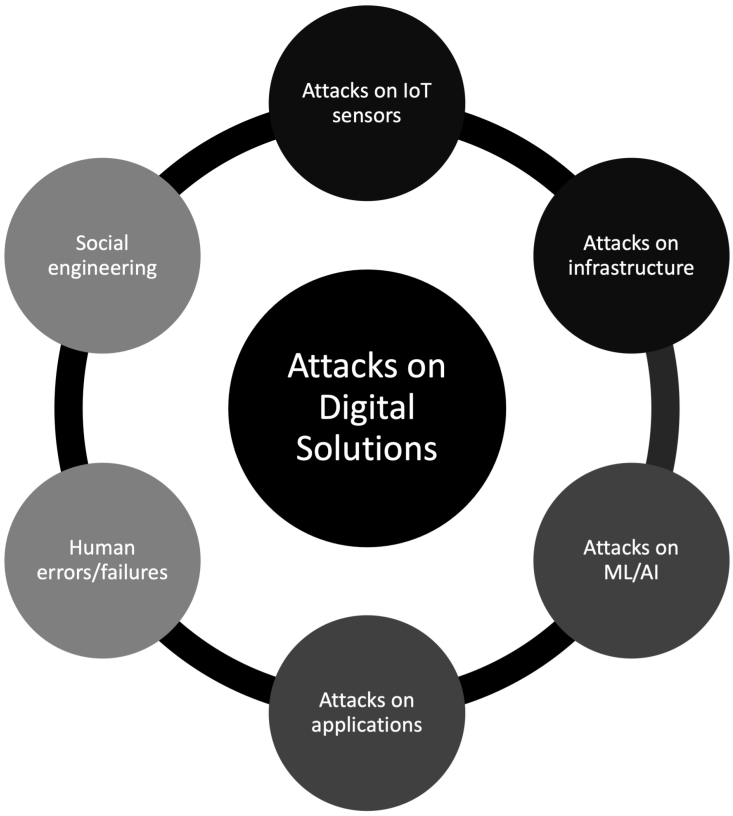


Figure 2. Classification of the attacks against DWC digital solutions.

Attacks on IoT sensors: As already explained above, IoT sensors are for many solutions a keystone as they constitute the source of data. Sensors are particularly vulnerable since they are often deployed in the wild (i.e., accessible by almost anyone), and are difficult and costly to secure (and thus have historically had poor security). While the data of the sensors themselves might not be very valuable to an attacker, being able to manipulate these data to trigger incorrect outputs by the services could have severe consequences. In addition, IoT sensors have in the past already been (and continue to be) compromised at scale to be integrated in botnets [18].

Attacks on infrastructure: Attacking the infrastructure is a way for the attackers to either disrupt the services (by, for instance, launching Denial of Services (DoS) attacks on it) or to gain unauthorized access to resources. This could also be a way for attackers to later use their access to a service to attack a water utility using and trusting this service.

Attacks on ML/AI: Compared to the other types of attack in this classification, attacks against machine learning (ML) and artificial intelligence (AI) are less known and appear to be fairly new. Attackers can for instance use specially crafted inputs to mislead the algorithms. Famous examples of such attacks include, for instance, cars being tricked into speeding by placing tape on speed signs. Other attacks consist of an attacker feeding incorrect data to the classifier (also known as data poisoning), polluting the model in such way that its own data are later classified as good data or, on the contrary, so that good data are in fact classified as incorrect. Finally, models have an intrinsic value, and an attacker might want to steal them.

Attacks on applications: Applications (web, mobile, API, etc.) are usually exposed and, if compromised, can lead to data leaks, unauthorized access to resources and actions or allow for data manipulation and denial of service.

Human errors/failures: While not being an attack per se, human error can lead to the same consequences. If a user is given access to data or actions he/she should not have access

to, he/she could misuse it (intentionally or not) and effectively create a situation similar to an attack (for instance, a user could be given access to an alert system and trigger an alarm, leading operators to take decisions based on misleading data).

Social engineering: Like human errors, a user could be tricked by a malicious person into performing harmful actions, potentially leading to dangerous consequences as well.

When securing a digital solution, it is important to take into consideration who and what one is defending against. Defending against a high-school student, running automated tools he found on the Internet, is not the same as defending against a state-sponsored threat actor that has unlimited resources. As presented by Weingart [19], we can classify attackers into three different classes based on their capabilities. While his classification is intended for the physical security of embedded devices, it can be slightly adjusted to the context of DWC. Our adapted classification is as follows:

Class I A clever outsider, who has limited knowledge about the system and a low budget and equipment. This could be a curious attacker that is targeting the system mostly for prestige and as a hobby, but also a "script kiddie" (a script kiddie is person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own) dumbly following scripts and tutorials found on the Internet.

Class II A knowledgeable insider, who has advanced knowledge and/or specialized education and experience in the area. This category has access to sophisticated tools. Typically, this class corresponds to researchers.

Class III A funded organization categorized by its high budget and its ability to recruit class II attackers to attack the system. This corresponds to organized crime or to a government.

Attackers have incentives to target digital solutions to disrupt or gain access to water utilities, it is thus expected that solutions should consider attackers from all three classes. However, for many solutions, defending effectively against state-sponsored actors is simply not feasible, as it would drastically increase the cost of their product, making it too expensive for any water utility to adopt. This is especially true for IoT-based solutions, which rely on low-cost environmental sensors to collect data. Securing these devices while keeping the cost low is a challenge given today's state of the art in the area: the devices being deployed in the wild most of the time can be accessed by a malicious person and analyzed not only from a software, but also from a hardware perspective. Microsoft's third immutable law of security states that "if a bad guy has unrestricted physical access to your computer, it's not your computer anymore" [20], and this holds even more true in the context of IoT devices. This, however, does not mean the solutions should give up on security, as they can still protect against class I and class II attackers by, for instance, tackling the low-hanging fruits in their product.

To secure a product against all classes of attackers, a change of paradigm is required: one must work with the assumption that parts of the solution will be broken/accessed by attackers (typically an IoT sensor) and ensure that the impact of this breach has no operational or financial consequences. There is no "one size fits all" scenario, and solutions must assess on their own where they stand and how much effort is needed to secure their product. A solution owner might be concerned by the intellectual property (IP) that an attacker could get his hands on if he were to compromise an IoT device (models, algorithms, etc.) and thus choose to invest in more hardware security than for another solution that only measures environmental data to send them back to a backend infrastructure for processing.

Another way to think about the problem is through cost: attackers, no matter which class they belong to, will go for the easiest and cheapest path that has the most impact. As such, ensuring that the low-hanging fruits are tackled will increase the cost and difficulty of an attack. Reducing the impact (for instance by ensuring proper segmentation) also contributes to attackers looking elsewhere.

4. Case Study of a Typical IoT Solution

This section presents the case study of a digital solution. The solution was chosen because it constitutes a typical IoT solution, i.e., based on environmental sensors deployed in the wild. While we have collaborated with the technology provider to (1) perform the security assessment, and (2) ensure the identified weaknesses are mitigated, we will not provide details on the solution itself, but rather abstract its use case in a generic manner.

4.1. Typical Solution Description

The solution that was tested as part of the DWC project is a "typical" IoT-based solution. Its architecture is presented in Figure 3. It is based on a set of sensors deployed "in the wild", i.e., in a location where they can be physically accessed by anyone (some water facilities that are not watched 24/7 are included too in this definition). In the water sector, this can be a river, sewers, lakes, etc. The sensors collect a set of environmental data, and might perform some manipulations on it before uploading it to a backend server. In order to obtain connectivity, the sensors rely on the mobile network or any other communication technology (LoRa for instance). To access the aggregated data, the users access an application (web or mobile) which usually features dashboards presenting them with the relevant information for them to make decisions. In the case of the tested solution, alerts could be raised if certain conditions on the measured environmental values were met.

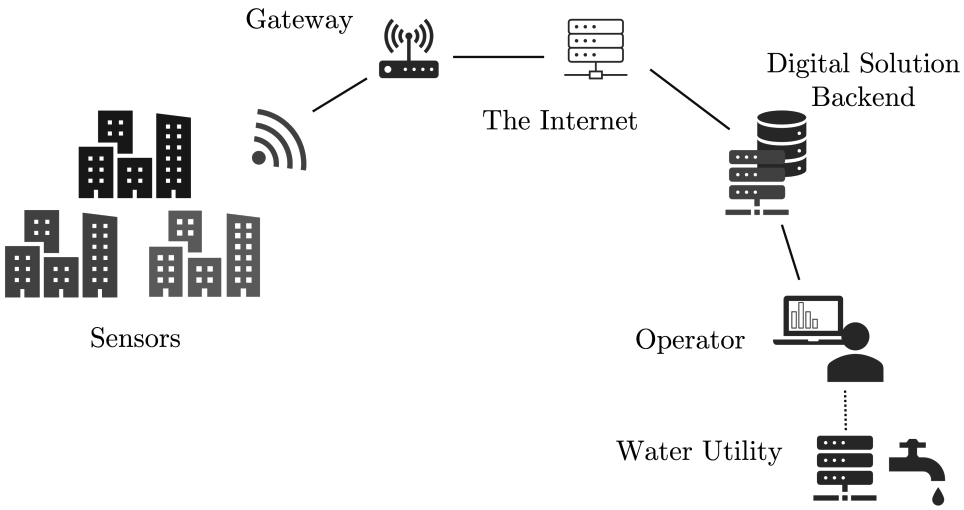


Figure 3. Typical architecture of an IoT solution (here, in the water sector).

4.2. Black-Box Testing Methodology

In a black-box testing scenario, the security expert has very little or no previous knowledge of the targeted system or device. At a high level, the methodology consists of sending inputs to the system, the "black box", and analyzing the obtained outputs to deduce the internals of the target. Having made some guesses, the attacker can adjust her inputs to confirm her thoughts or to exploit the target. This is presented in Figure 4.

Figure 4. High-level diagram of the black-box testing methodology.

The black-box testing methodology has several advantages over the white and grey ones. Its primary objective is to test a system under real conditions to emulate a real attack scenario. This means that such a test might catch errors made during the deployment of the system, such as default passwords, misconfigurations in general or even the lack of security training for operators (weak passwords). This methodology also presents a low false-positive ratio as the security expert can assess the risks associated with a vulnerability directly, i.e., if the vulnerability can be exploited or not. While black-box testing can miss some vulnerabilities and should likely not be the first test performed, it is an excellent way to assess how a system stands against attacks and to get an idea of the path an attacker would take to compromise the solution, and thus gives indications on how to tackle those potential low-hanging fruits. It can later be completed by a deeper assessment following a grey- or white-box approach.

Hardware Security Testing Methodology for IoT

Our process can be split into five different tasks (see Figure 5). The very first one is the hardware analysis. Once the device is acquired, we started analyzing its components to know what the exposed interfaces and debug interfaces are, but also the chips that are on the board. To know this, we had to open the device to access the Printed Circuit Board (PCB) to analyze it (see example in Figure 6a). Knowing the components and available interfaces, we then started looking for documentation such as datasheets, Request for Comments (RFC) or any other relevant information about the device. The goal of that second step is to understand the overall system and come up with some first hypotheses about it.

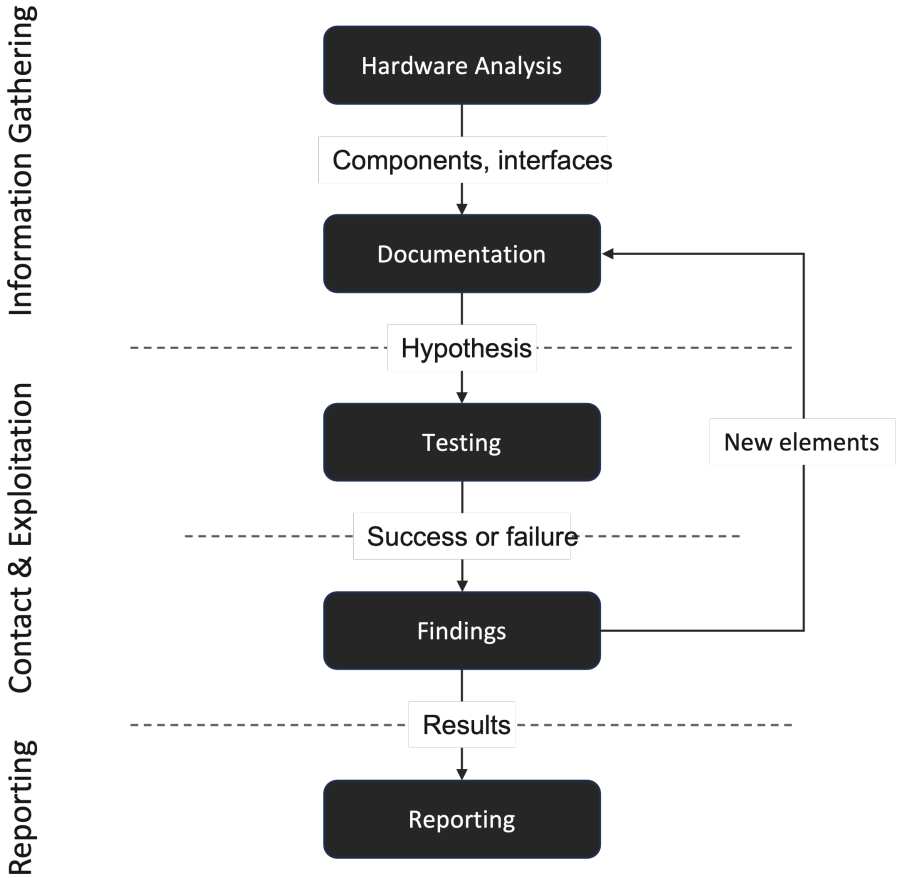
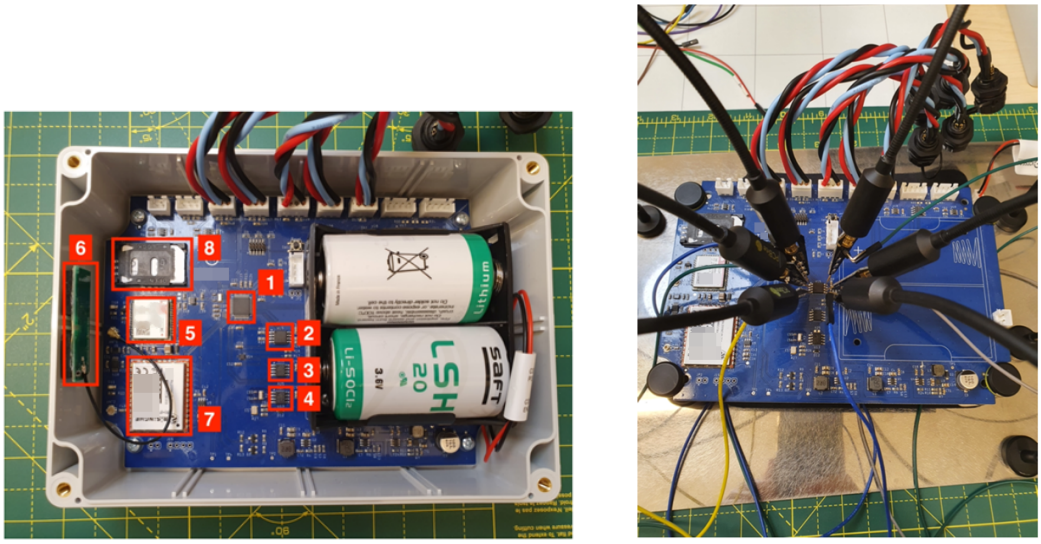


Figure 5. Hardware black-box testing methodology iterative cycles.



(**a**) (**b**)

Figure 6. Hardware testing of an IoT device. (**a**) Example of an IoT device with identified components, (**b**) Dumping the content of an external flash.

From those hypotheses, we then came up with testing scenarios to be performed on the device. Those scenarios have two possible outcomes: either a success or a failure. However, the success or the failure of a testing scenario is determined by the expected result, which in reality means that even failure brings us new information about the system.

The results of a specific scenario need to be interpreted. This interpretation is called a finding. Those findings are then used to look for new documentation and/or infer new hypotheses about the device. For example, if the hypothesis is "the device has debug ports exposed on the Universal Asynchronous Receiver-Transmitter (UART) pins and is providing the attacker with a shell when connected to it", then the testing of that particular scenario will lead to either a confirmation or a rejection of the hypothesis. The interpretation here is quite easy as it is the hypothesis itself. This finding can then be reinjected in the documentation phase to infer new testing hypotheses such as "the attacker is given a root shell when connecting to the UART console" or "the attacker can access the filesystem when connecting to the UART console".

Those findings are finally gathered to be reported. The reporting step is the one where the device is considered back in its whole ecosystem. That means the findings are interpreted again, but this time with regards to different metrics. In the case of the above example, one can wonder what is the impact of the attacker having access to the filesystem on an IoT device? Linked to other findings such as "The data is stored in cleartext on the device" or "The data is not stored on the device" the impact and thus the interpretation can be very different.

Those steps can be mapped with the Open-Source Security Testing Methodology Manual (OSSTMM) [21] which is widely used to assess the security of IT systems. The first two steps (hardware analysis and documentation) correspond to the information-gathering (or approach) phase in the OSSTMM. The contact phase is then used followed by the exploitation phase, which are here mapped with the testing and findings phases. In the OSSTMM, the information gathered during the first phase along with that gathered directly by the contact phase is then used to exploit the system and gain access. In our process, the information required to exploit and gain access comes from previous testing. Finally comes the reporting phase. In the OSSTMM, one more phase is sometimes used depending on the engagement: the persistence one. In our case, persistence is studied as a hypothesis which is then tested and reported as any other findings.

The testing stage is supported by several tools (hardware or software). As a rule of thumb, we try to use Commercial-off-the-shelf (COTS) equipment whenever it is possible.

This helps in putting a cost on an attack and deriving the risk: if an attack requires a piece of equipment that costs USD 100,000, one can assume that attackers, even if they are in the state actor category, might first look for another attack vector. On the contrary, if an attack cost is only a few dollars, more attackers can perform it, from the state actor to the high school students who wants to prove to their friends they can do it.

From a hardware perspective, we used a Raspberry Pi Zero for most of the attacks: it costs around USD 20 and can be configured as a JTAG adapter which allowed us in this case to dump the firmware using OpenOCD. Figure 6b illustrates how one can use the same tools to dump the content of an external Flash. In the context of this project, we also developed a tool called `comet` (Available at https://github.com/guillaumebour/comet, accessed on 16 February 2023) (serial Communication Eavesdropping Tool) aiming at intercepting serial communications between a microcontroller and a modem. The tool offers specific functionalities, such as multiplexing of two different sources (aimed at Tx and Rx), automatic decoding of the received data and logging in JSON format (for easy processing afterwards).

Once the data acquired, we adapted previously developed scripts to decrypt the data. Those scripts are not published as part of a tool yet, but they are based on previous work performed on the pacemaker ecosystem [22].

4.3. Identified Vulnerabilities

Following the assessment, the following weaknesses were identified and reported to the manufacturer:

- Hardware level
  - Debug interfaces easily identifiable and not disabled, allowing an attacker to dump the firmware of the device and perform dynamic analysis if required.
- Firmware level
  - The contents of the external flash and EEPROM are not encrypted and can be dumped easily.
  - The communication with the backend infrastructure uses an insecure proprietary protocol over UDP.
- Infrastructure level
  - The connection to the backend server is not protected (no Virtual Private Network (VPN) is required, for instance.)
  - No protection against replay attacks.
  - No protection against device impersonation.

While an attacker can successfully impersonate a device, he needs to have had physical access to the device to do so. The manufacturer also used individual keys for its devices, making it resource-consuming for attackers to perform an attack at scale.

4.4. Possible Attack Scenarios

The weaknesses presented in the previous section can be chained to create an attack. We describe here two possible attack scenarios.

4.4.1. Data Manipulation

Using the vulnerabilities described in the previous section, an attacker can successfully impersonate a device. By obtaining physical access to a device, one can abuse the fact the debug port is not disabled to dump the firmware of the device and access the cryptographic material stored there. Following this step, no more physical access is needed, and the attacker can send data to the backend on behalf of the IoT sensor.

The cryptographic material is unique per device, so the attack is not particularly useful if applied to only one device. The devices are however placed in public spaces and can thus be accessed. The ease of replication of the attack makes it possible to compromise devices at scale (for instance, in a city) in order to fake all the data for the solution in a

geographic area. This can further be used to trick the human operator using this solution into taking potentially harmful decisions (remember that the digital solution is not used to take automatic decisions, yet).

4.4.2. Denial of Service

Another potential attack that can be mounted against this solution is a Denial of Service (DoS) attack. An attacker can exploit the fact that there is no protection against replay attacks and device impersonation (without the actual device being needed) to flood the server with replaying a legit capture exchange. This could potentially fill the databases and would render the solution useless. Depending on how the backend is configured, this could also lead to additional expenses (for instance, if using databases from a cloud provider, then the database might scale up but so will the cost).

However, when discussing with the manufacturer, they explained that this attack would not be feasible because of some checks being made on the data.

4.5. The Operational Impact of Those Attacks on This Solution

From a water engineering point of view, the impact of the described hack on the discussed IoT device can result in severe environmental consequences. The considered device has been developed within the DWC project as a solution to remotely inform water utilities about Combined Sewer Overflows (CSOs), which should be limited over time to preserve the surrounding environment because of the potential releases of polluted discharge.

Combined sewer systems are designed to overflow occasionally during heavy rainfalls leading to untreated wastewater discharge into nearby receiving water bodies, eventually resulting in significant public health concerns, stress on aquatic organisms, and water quality concerns [23]. Several studies [24–28] have largely shown that frequent CSOs can lead to environmental severe issues such as high concentrations of solids, microbial pathogens and toxic pollutants in receiving water bodies.

The hydraulic devices which are designed to handle CSOs should meet specific criteria, which often depend on national or international regulations. Usually, CSOs devices must discharge the wastewater flow while being compliant to specific restrictions, such as limited yearly frequencies and sufficient dilution between wastewater and rainwater [29].

Having control of the several CSO devices over time has usually been an issue for water utilities because of the significant high costs of the installation and maintenance of flow and water level meters that are installed remotely at the location of the CSO devices along the whole combined sewer networks. Moreover, climate change is nowadays eventually worsening the level of compliance of existing CSO devices around our planet, in terms of frequency of CSO occurrences [30]. In the past, CSO chambers and pipes have often been designed without considering the actual status of current and foreseen climate change, while accounting only for the historical precipitation data of the involved territory. The analyzed IoT device has been developed in the DWC project with the aim of providing the water utilities with a low-cost solution which allows them to monitor the frequency of CSOs by adopting real-time surrogate temperature sensors, among the cheapest sensors on the market.

When the water level is sufficient enough to overflow from a CSO device, an alarm is registered by the IoT device because of a significant difference in temperature between the external environment and the discharged wastewater. If anomalies of temperature are detected by the analyzed IoT device, a message is remotely sent to the operators of the water utility to inform them about the critical situation of a given CSO device. When this digital solution is properly installed on a significant number of CSO chambers or pipes in a given sewer network, the interested water utility can benefit from the transmitted information to improve CSOs management. Specifically, sensors are coupled to wireless communication and cloud data transmission through state-of-the-art data-shared platforms to allow online visualization and data processing. Artificial intelligence and predictive analytics techniques have been developed to extract accurate real-time knowledge from

the raw temperature measurements and define user-friendly set rules for optimal CSO prevention. Additionally, the interested water utility can rely on the obtained overview of CSOs devices concerning the identification task of the most critical areas which should be revamped accordingly with data-driven master plans aimed at network rehabilitation.

Overall, the rapid growth of IoT devices in the water industry is allowing an outstanding improvement of process effectiveness in existing water systems. On the other hand, water utilities increasingly rely on a variety of digital solutions which are normally susceptible to different types of hacking, hence the related IT protection from malicious attackers is paramount to avoid environmental and/or social disasters.

5. Results

5.1. Common IoT Vulnerabilities

We collected the insights from using IoT in the water industry and combined them with our findings from similar use cases in other critical infrastructures. From this list, we derived a security checklist [31] which aims to cover the most common vulnerabilities and low-hanging fruits in the IoT.

The IoT Security checklist is a questionnaire-like document to be used for a self or guided assessment of an IoT device. The objective is to raise awareness of specific weaknesses. It aims to be domain-agnostic. The questions come from both our experience working with IoT devices and guidelines such as the "Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures" from ENISA [32].

Following the example of the OWASP Application Security Verification Standard [33], three levels are defined [31]:

- **Level 1** is the bare minimum security IoT devices should strive for. Complying with this level should counter attackers who are using simple and low-effort techniques to identify easy-to-find and easy-to-exploit vulnerabilities. In the case that the IoT device is processing data that are sensitive or critical for operation, you probably do not want to stop at this level.
- **Level 2** aims to defend against the most common risks associated with IoT devices today. It is appropriate for devices processing healthcare data or other sensitive assets. Threats to level 2 are typically skilled and motivated attackers focusing on specific tools and techniques that are effective to discover and exploit weaknesses within applications. Aiming at this level should be enough for most devices.
- **Level 3** is typically reserved for devices requiring a significant level of security verification, such as in the military, health and safety or critical infrastructure domains. If you think your device must comply with level 3, then this checklist likely will not be enough in itself and you probably want to also look at IoT certification schemes such as Common Criteria, FIPS-140 or PSA Certified.

The IoT security checklist [31] is a dynamic document which is evolving as we gather more use cases. The latest version will always be available from our website (https://www.sintef.no/en/projects/2022/ragnarok/outcomes/) accessed on 16 February 2023.

5.2. Associated Attack Scenarios

This section presents example scenarios that make use of the different IoT vulnerabilities exposed in the checklist and which could potentially lead to the theft of sensitive information, disruption of essential services, potential harm to users or even physical damage to infrastructure.

5.2.1. Data Manipulation

Data manipulation refers to the act of intentionally altering or manipulating data collected from IoT devices in order to gain unauthorized access to sensitive information or disrupt the normal functioning of the device. This can include tactics such as injecting false data into the system, modifying existing data to change its meaning or deleting important

data to prevent the system from functioning properly. Data manipulation attacks can be particularly dangerous because they can be difficult to detect and can have serious consequences for the security and integrity of IoT systems. If such systems are being used in critical infrastructures, the consequences can be disastrous. For instance, if such a system, used to measure water quality, is manipulated in such a way that contamination of the water is undetected, citizens' safety is at stake.

Data manipulation can impact digital solutions which interact directly with a critical system (e.g., a given action being executed if a threshold value is reached), those who feed an AI model (e.g., the data are manipulated in such a way that the AI is giving a wrong prediction) or even those who are fully disconnected from a critical systems but which are used by operators to take decisions.

When it comes to motivation to perform such attacks, there are many. Just to name a few, one might want to perform an attack on a country by infecting the water system. Another might be a company who wants to hide some of its activities to the authorities to avoid taxes or fines.

5.2.2. Privacy and Confidentiality Issues

IoT devices can be compromised, leading the attacker to gain access to potentially sensitive information. Additionally, the vast amounts of data collected by IoT devices in critical infrastructure can raise concerns about the protection of personal privacy, as well as the potential for these data to be used for malicious purposes. Some devices might acquire data at the user level (e.g., smart meters) and can reveal patterns in individuals' lives. These data could be misused for surveillance purposes for instance. While this scenario might sound hypothetical, law enforcement already uses such sensor network to detect illegal drug workshops, for instance in the Netherlands by monitoring the sewers.

5.2.3. Denial of Service

A DoS is a type of cyber attack that is designed to disrupt the normal functioning of a digital system by overwhelming it with traffic or requests. In the context of IoT-based digital solutions, a DoS attack can cause the system to become unresponsive or unavailable, disrupting its ability to provide the intended services. In the water sector, this could for instance be the sensors' data becoming unavailable for the AI model to perform prediction. In some cases, this can have a severe impact as operators might be forced to fall back to "manual" operations or to cancel activities for safety reasons. Overall, DoS attacks on IoT solutions can have serious consequences for critical infrastructure systems, and it is important to implement measures to prevent or mitigate these attacks. This can include implementing strong authentication and access control mechanisms, as well as monitoring systems for unusual traffic patterns that may indicate an attack.

5.2.4. Initial Access and Privilege Escalation

Vulnerabilities in IoT devices can be exploited by attackers to gain initial access to a network and then perform further exploitation. One common way this is achieved is through the use of malware that are specifically designed to target IoT devices. This malware can be delivered through various means, but it often involves exploiting vulnerabilities in the device's software or firmware, when the device is directly exposed on the Internet and not patched. Once the malware has been installed on the IoT device, it can be used to gain initial access to the device and then perform privilege escalation. This may involve using the malware to gain root access to the device, which allows the attacker to execute arbitrary code and take complete control of the device. With root access to the device, the attacker can use this access to perform a variety of malicious actions. For example, they may be able to collect sensitive information from the device, such as passwords or personal data (if any), or they may be able to use the device to launch further attacks on other systems or devices. Overall, security vulnerabilities in IoT devices can create significant risks for organizations that rely on these devices.

5.3. Evaluating the Operational Impact

On top of the decisions on mitigation action to secure water systems together with their digital devices, a Risk Management Procedure (RMP) should be undertaken, taking into account that risk is given by a combination of consequences (operational impact on the system) and probabilities (likelihood of occurrence of the identified risk). After defining the context and properly identifying the risk, according to ISO 31000:2018 standard, a risk analysis must be performed in order to evaluate the level of risk [34]. During risk analysis, understanding how to model the risk event is key, keeping in mind which data would be required in the analysis in relation to the risk criteria set a priori, and which variables are the most relevant for the identified risk event (e.g., potential critical areas, number of affected individuals, etc.). Moreover, depending on the level of data availability and resources and on the grade of attention toward the identified risk, there are three types of methods for risk analysis which can be adopted for determining the level of risk, namely qualitative, semi-quantitative and quantitative methods [35]. In the water infrastructure domain, a quantitative method to calculate the operational impact on the system has been developed in the STOP-IT project (See https://stop-it-project.eu/, accessed on 16 February 2023) through the RAET (Risk Assessment and Evaluation Toolkit), focused on risk management of cyber–physical threats in drinking water supply systems [6]. Studies about the evaluation of the impact produced by cyberattacks on water systems are emerging in the literature, for instance RAET has been tested in real environments, providing the estimation of unmet demand in water distribution systems for selected scenarios of attack [35].

6. Discussion

The security of embedded systems is still a major concern in the adoption of IoT-based solutions for critical infrastructure, and the water sector is no exception. Many Real-Time Operating System (RTOS) still fail to implement even basic security mechanisms that have been standard in the desktop world for a long time, such as Address Space Layout Randomization (ASLR). This lack of security in the design of these systems leaves them vulnerable to attacks that can compromise the integrity and reliability of the critical infrastructure they support.

One key approach to addressing this issue is to prioritize security by design. This means not only focusing on the functional requirements of a digital solution, but also bringing security experts on board the project from the start. By considering security at every stage of the design process, it is possible to identify and address potential vulnerabilities before they become a problem. This approach also allows for a more holistic view of the security risks associated with a given IoT solution, and can help to balance the trade-offs that are often faced in this field.

As part of this process, it is also important to ask the right questions when making decisions about security. For example, is it acceptable for a single device to be compromised by an attacker, or would it be better to invest in stronger security measures to protect against such an attack? Similarly, what would be the consequences of a large-scale attack that compromised a significant number of devices? These are the kinds of questions that need to be considered when designing and implementing IoT solutions for critical infrastructure.

In addition to these measures, it is also important to raise awareness among engineering teams about the importance of tackling low-hanging fruit when it comes to security. By addressing the most obvious and easily exploitable vulnerabilities, it is possible to significantly raise the cost of an attack and make it less attractive to potential attackers. This can help to create a more secure environment for critical infrastructure systems, and can help to prevent some attacks.

Finally, it is important to be prepared for the fact that even with the best security measures in place, it could still be possible for an attacker to compromise a digital solution and use it to make operators take wrong decisions. As such, it is essential to have contingency plans in place to respond to such an attack, and to be prepared to quickly recover from any disruption that may occur. By taking these steps, it is possible to mitigate the security risks

associated with IoT-based solutions for critical infrastructure, and to ensure the continued reliability and integrity of these systems.

7. Conclusions

In conclusion, our research shows that the security of IoT-based digital solutions is a critical concern in the adoption of Industry 4.0 technologies. These solutions are increasingly being used to support critical infrastructure, such as the water sector, and their security is essential to ensure the continued reliability and integrity of these systems. However, as our work demonstrates, many digital solutions still lack basic security mechanisms and are vulnerable to attacks that can compromise their functionality.

The importance of this issue cannot be overstated. The "cyber-world" is now the new battlefield, and connected critical infrastructures are valuable targets for attackers. If we do not take security seriously from the start, we will face serious problems in the future. Our contributions in this project include bringing attention to this issue and providing an IoT security checklist that can help to ensure a basic level of security for digital solutions.

Overall, our work emphasizes the need for security by design and the importance of considering security at every stage of the design process. By doing so, we can ensure that IoT-based solutions for critical infrastructure are secure and reliable and can continue to support society in the face of growing cyber threats.

Author Contributions: Conceptualization, G.B.; methodology, G.B.; investigation, G.B., C.B., R.U. and M.G.J.; resources, R.U.; writing—original draft preparation, G.B., C.B., R.U. and M.G.J.; writing—review and editing, G.B., C.B., R.U. and M.G.J.; supervision, R.U.; project administration, R.U.; funding acquisition, M.G.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the EU H2020 Research and Innovation Programme under Grant Agreement No. 820954.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful for the collaboration and support from the Digital Water City partners.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

ASLR	Address Space Layout Randomization
BWD	Bathing Water Directive
COST	Commercial off-the-shelf
CSO	Combined Sewer Overflow
DoS	Denial of Service
DWC	Digital Water City
IoT	Internet of Things
OSSTMM	Open-Source Security Testing Methodology Manual
PCB	Printed Circuit Board
RFC	Request for Comments
RIDB	Risk Identification Database
SCADA	Supervisory Control And Data Acquisition

STOP-IT	Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats
UART	Universal Asynchronous Receiver-Transmitter
VPN	Virtual Private Network
RMP	Risk Management Procedure
RTOS	Real-Time Operating System

References

1. Ugarelli, R.; Koti, J.; Bonet, E.; Makropoulos, C.; Caubet, J.; Camarinopoulos, S.; Bimpas, M.; Ahmadi, M.; Zimmermann, L.; Jaatun, M. STOP-IT-Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats. *Phys. Cyber Saf. Crit. Water Infrastruct.* **2019**, *56*, 130.
2. Ugarelli, R. Cybersecurity Importance in the Water Sector and the Contribution of the STOP-IT Project. In *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry*; Soldatos, J.; Praça, I.; Jovanović, A., Eds.; Now Publishers: Boston, MA, USA, 2021; pp. 145–158.
3. Ostfeld, A.; Salomons, E.; Smeets, P.; Makropolous, C.; Bonet, E.; Meseguer, J.; Mälzer, H.J.; Vollmer, F.; Ugarelli, R. *STOP-IT D3.2 Risk Identification Database (RIDB)*; Zenodo: Genève, Switzerland, 2018. [CrossRef]
4. Makropolous, C.; Moraitis, G.; Nikolopoulos, D.; Karavokiros, G.; Lykou, A.; Tsoukalas, I.; Morley, M.; Castro Gama, M.; Okstad, E.; Vatn, J. *STOP-IT D4.2: Risk Analysis and Evaluation Toolkit (RAET)*; Zenodo: Genève, Switzerland, 2019,
5. Mälzer, H.; Vollmer, F.; Corchero, A. *STOP-IT D4.3 Risk Remediation Measures Database (RRMD)*; Zenodo: Genève, Switzerland, 2019. [CrossRef]
6. Nikolopoulos, D.; Moraitis, G.; Bouziotas, D.; Lykou, A.; Karavokiros, G.; Makropoulos, C. Cyber-physical stress-testing platform for water distribution networks. *J. Environ. Eng.* **2020**, *146*, 04020061. [CrossRef]
7. Ahmadi, M.; Ugarelli, R.; Grøtan, T.O.; Raspati, G.; Selseth, I.; Makropoulos, C.; Nikolopoulos, D.; Moraitis, G.; Karavokiros, G.; Bouziotas, D.; et al. *STOP-IT D4.4: Cyber–Physical Threats Stress–Testing Platform*; Zenodo: Genève, Switzerland, 2019,
8. Schwarzmüller, H.; Vennesland, A.; Haro, P.H.; Bour, G. *D4.1: Interoperable and Secure Flow of Information—Cyber-physical Sphere and Interoperability Aspects in the Utilities Regarding the DWC Solutions*; Technical Report D4.1; Digital Water City; Zenodo: Genève, Switzerland, 2021. [CrossRef]
9. Directive 2006/7/EC of the European Parliament and of the Council of 15 February 2006 Concerning the Management of Bathing Water Quality and Repealing Directive 76/160/EEC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0007 (accessed on 6 February 2023).
10. City, DW. Sensors for Real-Time In Situ *E. coli* and Enterococci Measurements. Available online: https://www.digital-water.city/solution/sensors-for-real-time-in-situ-e-coli-and-enterococci-measurements/ (accessed on 6 February 2023).
11. City, D.W. Mobile Application for Asset Management of Drinking Water Wells. Available online: https://www.digital-water.city/solution/mobile-application-for-asset-management-of-drinking-water-wells/ (accessed on 6 February 2023).
12. What You Need To Know About the SolarWinds Supply-Chain Attack | SANS Institute. Available online: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ (accessed on 6 February 2023).
13. European Banking Authority Hit by Microsoft Exchange hack-BBC News. Available online: https://www.bbc.com/news/technology-56321567 (accessed on 6 February 2023).
14. Fouche, G. Norway's parliament hit by new hack attack. *Reuters* **2021**. Available online: https://www.reuters.com/world/europe/norways-parliament-hit-by-new-hack-attack-2021-03-10/ (accessed on 6 February 2023).
15. A Large-Scale Supply Chain Attack Distributed Over 800 Malicious NPM Packages; Section: Article. Available online: https://thehackernews.com/2022/03/a-threat-actor-dubbed-red-lili-has-been.html (accessed on 6 February 2023).
16. Governments Need to Reassess Security Infrastructures | Orange Business Services. Available online: https://www.orange-business.com/en/magazine/new-generation-critical-infrastructures-secure (accessed on 6 February 2023).
17. Clear the "Air Gap" Myth to Evade Cyber Threats—Securing Critical Infrastructure in the Digital World. Available online: https://www.nokia.com/thought-leadership/articles/critical-infrastructure-enterprise-security/ (accessed on 6 February 2023).
18. Kambourakis, G.; Kolias, C.; Stavrou, A. The Mirai botnet and the IoT Zombie Armies. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 267–272. ISSN: 2155-7586. [CrossRef]
19. Weingart, S.H. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defences. In Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems, CHES '00, Worcester, MA, USA, 17–18 August 2000; Springer: Berlin, Germany, 2000; pp. 302–317.
20. Microsoft. Ten Immutable Laws of Security (Version 2.0); The Mirai Botnet and the IoT Zombie Armies. Available online: https://learn.microsoft.com/en-us/security/compass/ten-laws-of-security (accessed on 6 February 2023).
21. ISECOM. OSSTMM.The Open Source Security Testing Methodology Manual. Available online: https://www.isecom.org/OSSTMM.3.pdf (accessed on 6 February 2023).
22. Bour, G.N. Security Analysis of the Pacemaker Home Monitoring Unit: A BlackBox Approach. Master's Thesis, NTNU (Norwegian University of Science and Technology), Trondheim, Norway, 2019.

23. Mailhot, A.; Talbot, G.; Lavallée, B. Relationships between rainfall and Combined Sewer Overflow (CSO) occurrences. *J. Hydrol.* **2015**, *523*, 602–609. [CrossRef]
24. House, M.; Ellis, J.; Herricks, E.; Hvitved-Jacobsen, T.; Seager, J.; Lijklema, L.; Aalderink, H.; Clifforde, I. Urban drainage-impacts on receiving water quality. *Water Sci. Technol.* **1993**, *27*, 117. [CrossRef]
25. Walsh, C.J.; Roy, A.H.; Feminella, J.W.; Cottingham, P.D.; Groffman, P.M.; Morgan, R.P. The urban stream syndrome: Current knowledge and the search for a cure. *J. N. Am. Benthol. Soc.* **2005**, *24*, 706–723. [CrossRef]
26. Passerat, J.; Ouattara, N.K.; Mouchel, J.M.; Rocher, V.; Servais, P. Impact of an intense combined sewer overflow event on the microbiological water quality of the Seine River. *Water Res.* **2011**, *45*, 893–903. [CrossRef] [PubMed]
27. Holeton, C.; Chambers, P.A.; Grace, L. Wastewater release and its impacts on Canadian waters. *Can. J. Fish. Aquat. Sci.* **2011**, *68*, 1836–1859. [CrossRef]
28. Madoux-Humery, A.S.; Dorner, S.; Sauvé, S.; Aboulfadl, K.; Galarneau, M.; Servais, P.; Prévost, M. Temporal variability of combined sewer overflow contaminants: Evaluation of wastewater micropollutants as tracers of fecal contamination. *Water Res.* **2013**, *47*, 4370–4382. [CrossRef] [PubMed]
29. Mannina, G.; Viviani, G. Separate and combined sewer systems: A long-term modelling approach. *Water Sci. Technol.* **2009**, *60*, 555–565. [CrossRef] [PubMed]
30. Fortier, C.; Mailhot, A. Climate change impact on combined sewer overflows. *J. Water Resour. Plan. Manag.* **2015**, *141*, 04014073. [CrossRef]
31. Bour, G. IoT Security Checklist. 2022. Available online: https://www.sintef.no/en/projects/2022/ragnarok/outcomes/ (accessed on 6 February 2023).
32. Baseline Security Recommendations for IoT. 2017. Available online: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (accessed on 6 February 2023).
33. OWASP Application Security Verification Standard | OWASP Foundation. Available online: https://owasp.org/www-project-application-security-verification-standard/ (accessed on 6 February 2023).
34. ISO 31000:2018(en), Risk Management—Guidelines. Available online: https://www.iso.org/standard/65694.html (accessed on 6 February 2023).
35. Bosco, C.; Raspati, G.S.; Tefera, K.; Rishovd, H.; Ugarelli, R. Protection of Water Distribution Networks against Cyber and Physical Threats: The STOP-IT Approach Demonstrated in a Case Study. *Water* **2022**, *14*, 3895. [CrossRef]