A Online Discoverability of Exposed Industrial Control Systems

Fabrizio d'Amore[1,2], Paolo Forte[3] and Antonio Pisano[4]

[1]Sapienza University of Rome, DIAG, Via Ariosto 25, 00185 Rome, Italy
[2]SOCINT, c/o Università della Calabria, Cubo 18-b, 7th floor, 87036 Arcavacata di Rende (CS), Italy
[3]Independent researcher, 00100 Rome, Italy
[4]Leonardo, Piazza Monte Grappa 4, 00195 Rome, Italy

Abstract

The incautious connection to the Internet of any unprotected Industrial Control System (ICS) is enormously risky, especially if those belong to critical infrastructures like the national power grid. The goals of this work are to revise a methodology for estimating the exposure of the ICSes over the Internet, which we apply to the Italian network, and to raise awareness about this subject.

In order to estimate such an exposure, our approach followed different phases. First, we studied the working principles and the technology of industrial control systems. Then, a list of the main ICS protocols was drawn up. Finally, we investigated the exposure of each ICS protocol over the Italian IP address space by querying Shodan's database for protocol-specific features (e.g., TCP/UDP ports, headers). Besides, we investigated the exposure of IT technologies commonly used for monitoring and managing ICSes (e.g., web HMI and remote desktops).

The findings we collected show that a vast amount of ICSes, belonging to different kinds of infrastructures, are currently exposed over the Internet and that anyone can freely interact with those. Moreover, this work shows how easily anyone could employ common public tools to search for ICSes exposed over the Internet.

Keywords

ICS, SCADA, HMI, Shodan, Cybersecurity

1. Introduction

With IT services representing a substantial part of any business process many actors proved themselves able to threaten the IT surface of public and private sectors, showing that it is possible to wreak havoc through world-wide cyber-attacks even against critical infrastructures; besides, attackers are hard to identify as in many cases their attacks can be carried out with low-cost technology. Among critical infrastructures such as transportation, health and communications, the most sensitive are with no doubt energy and water infrastructures. Just consider how effective could be a cyber-attack that manages to disrupt energy or water distribution inside a country, causing a domino effect that would affect all the other national infrastructures.

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, Stavropol, Krasnoyarsk, Russia, October 1, 2021

damore@diag.uniroma1.it (F. d'Amore); paoloforte.ics@gmail.com (P. Forte); antonio.pisano@leonardocompany.com (A. Pisano)
0000-0002-6518-2445 (F. d'Amore)

A typical under-estimated risk comes from the incautious connection of not adequately protected devices to the Internet. It is known that cyber-attacks are mostly directed against the IT domain, that is the ordinary corporate network made of servers, databases, endpoints and network devices. Nonetheless, the equivalent OT domain (i.e. the ensemble of software and hardware used to monitor and control all the physical processes running in an industrial environment) represents in many ways an even more critical and strategic target for cyber-attacks. That because OT systems very often do not benefit from the same cyber-protection commonly implemented into IT systems, despite their criticality. The causes are several: responsible parties' lack of knowledge, technical complexity or just pure negligence. Furthermore, considering that often OT systems are not designed to be resilient to cyber risks, it goes without saying that leaving them underprotected and accessible via the public internet makes easier for an attacker to map and exploit them. Even worse, this could pave the way for stealthy cyber-attack planning and homeland security risks.

Now more than ever this risk is real and even short disruptions of the processes running in an industrial context could cause huge economical losses. For instance, if such disruptions affected (as already occurred) national power plants and power grids, they could cause nation-wide power outages. Analogous themes about the online exposure of ICSes around the world and the connected cyber risks have been addressed in [1, 2, 3, 4]. Also, according to [5, 6] which took in account the most significant cyber threats worldwide, the number of attacks against ICSes will grow in the near future. Various threat actors will be targeting ICSes, among which state-sponsored groups will play an important role due to their interest in foreign critical infrastructure monitoring. Such an interest comes from the fact that, although being extremely sensitive targets, ICSes are inherently hard to secure.

Therefore, it is essential to adequately protect ICSes and in order to achieve that the main requirement is to maintain an updated view of ICSes exposure over a nation-wide IP address space. The main contribution of this work is to estimate such an exposure within the Italian IP address space, in order to raise awareness about this cyber risk and to inform the audience about the importance of securing ICSes.

2. Preliminaries

No matter the type, it is never appropriate to leave a device exposed over the Internet, let alone if such a device belongs to ICSes. Yet, this simple rule is not always respected and many devices widely expose their services.

Right now, a large number of ICSes is exposed online and it is very easy to find them by using search engines freely available online, whether generic like Google or specific like Shodan [7]. The activity just described is known as *Reconnaissance* and it is the first step that an attacker makes when trying to carry out an attack, regardless of the nature of the attacker (e.g. state-sponsored groups, criminals or hacktivists). Reconnaissance enables the attacker to estimate the attack surface of the target, therefore it is extremely important to minimize and protect the attack surface of any ICS.

Just to further prove our point we mention a noteworthy and quite recent episode that was also reported by numerous publications and newspapers. As stated by the American "Department of

Justice", in 2016 a grand jury indicted seven Iranian individuals that performed work on behalf of the Iranian Government on computer hacking charges related to their involvement in an extensive DDoS campaign of over 176 days, among which one was charged with obtaining unauthorized access into the SCADA systems of the Bowman Dam, a small dam located in Rye, New York, United States, in 2013. Specifically, we read in the Press Release:

> "Between Aug. 28, 2013, and Sept. 18, 2013, *[the hacker - Ed.] repeatedly obtained unauthorized access to the SCADA systems of the Bowman Dam, and is charged with one substantive count of obtaining and aiding and abetting computer hacking. This unauthorized access allowed him to repeatedly obtain information regarding the status and operation of the dam, including information about the water levels, temperature and status of the sluice gate, which is responsible for controlling water levels and flow rates. Although that access would normally have permitted [the hacker - Ed.] to remotely operate and manipulate the Bowman Dam's sluice gate, [the hacker - Ed.] did not have that capability because the sluice gate had been manually disconnected for maintenance at the time of the intrusion. Remediation for the Bowman Dam intrusion cost over $30,000." [8]*

As reported in [9], the hacker broke into the control system of the dam in 2013 through a cellular modem. That could mean that the Bowman Dam's operators likely used a mobile subscription line to expose the control system of the dam over the Internet in order to be able to perform remote management. We believe this episode proves without a doubt that the interest of the threat actors in compromising even small ICSes is absolutely real.

The goal of this work is to estimate as precisely as possible the exposure of ICSes all over the case of the Italian IP address space, in full compliance with the Italian law.

According to the Italian mechanism, we notified the exposures to CSIRT (Computer Security Incident Response Team - Italia), following what is published in its web page.[1] CSIRT belongs to the Italian national security and notifies interested actors without revealing the source.

3. Approach and methodology

The approach of our work followed five phases. In the first phase, we studied the technological background, the peculiarities and the typical problems behind the ICSes and the OT network architectures. In the second phase, we identified the most used ICS communication protocols (or devices that run very identifiable network services) and studied their working principles: Automatic Tank Gauges (ATG), BACnet [10], Codesys [11], Red Lion's Crimson [12], DNP3 [13], Ethernet/IP [14], Omron's Fins [15], Tridium's Niagara Fox, General Electric's SRTP (GE-SRTP), IEC 60870-5-104 (IEC 104) [16], KNXnet/IP (KNX) [17], Mitsubishi Melsec-Q's proprietary protocol (Melsec-Q), Modbus [18], NPort Moxa serial device servers, OPC Unified Architecture (UA) [19], Phoenix Contact's PCWorx proprietary protocol, KW Software's ProConOS runtime system, Siemens' S7comm, XPort Lantronix serial device servers.

In the third phase, we set up everything we needed to discover the exposed ICSes: we choose the search engine Shodan as the most appropriate tool to discover the ICSes exposed over the

[1] https://csirt.gov.it/segnalazione, in Italian.

Italian IP address space, we selected a list of features to fingerprint each ICS protocol, and we developed the software to automate the data gathering and the surveying. Specifically, we built the queries to interrogate Shodan's database in order to identify the most commonly used ICS protocols. Each query was made of filters and keywords: the filters guided the search scope, while the keywords were the features that Shodan sought inside the content of the banners. A wise use of both filters and keywords enabled us to unequivocally identify the occurrences of the ICS protocols under analysis, to restrict the search scope to the Italian IP address space only, to remove any known honeypot and to limit the number of false positives. Precisely, in order to remove as many false positives as possible, the search was carried out only over the standard ports that pertain to the ICS protocols under analysis. Even though this constraint could have caused a possible failure to seize some findings, we ascertained this case to be a very low chance event. Table 1 collects the core parts of all the queries we used to interrogate Shodan's database. To automate the process, we coded appropriate Python scripts for querying Shodan's API. When queried, Shodan returns a JSON object containing all the matching services found online along with elements such as the IP address, the estimated location, the service banner, the last-seen timestamp and lots of other information related to any distinct service that matched the query. We further analyzed each IP address in order to discover the exposure of other services running on the same IP address (e.g., web server, remote desktop and so on).

In the fourth phase, we eventually performed the actual data gathering operations, querying Shodan's database and collecting all the matches. In addition, we also performed some additional searches in order to detect any HMI exposed online over typical IT protocols like HTTP and VNC. The data collected and presented in this work was gathered during the first week of March 2020.

Lastly, in the fifth phase we analyzed the data just obtained, we ascertained that the dataset was clear of any remaining inconsistent information, duplicates and honeypots, we extracted some statistics and we identified several noteworthy findings such as some management interfaces of devices belonging to ICSes used for the electric power generation.

4. Results and discussion

4.1. ICS Services

As shown in Table 2, we detected 6038 ICS services exposed online over 5936 IP addresses belonging to the Italian IPv4 address space. It is important to highlight that the number of matching addresses varies and grows over time, therefore our results are to be intended as a reference value and a potential lower bound of the actual number of ICS services currently exposed over the Internet.

It is hard to understand the actual purpose of the services we found given that most of those can be employed in many different fields. As shown in Figure 1, without a doubt most of the findings are related to building automation systems belonging to industrial, commercial or domestic entities; examples of this are the high number of KNX gateways, widely used in home automation systems, or the high number of Fox and Bacnet interfaces, both employed in BASs and HVAC systems. The second most observed services are belonging to those industrial entities that make extensive use of automation systems (e.g., manufacturing but also energy industry), as

Table 1
Queries for Detecting Online Exposed ICSes

ICS Services	Shodan Queries
ATG	port:10001 I20100
BACnet	port:47808 Instance
Codesys	port:1200,2455 operating system
Crimson	port:789 product:'Red Lion Controls'
DNP3	port:20000 source address
Ethernet/IP	port:44818 Product name
Fins	port:9600 response code
Fox	port:1911,4911 fox hello
GE-SRTP	port:18245,18246 product:'general electric'
IEC 104	port:2404 asdu address
KNX	DIB_DEV_INFO
Melsec-Q	port:5006,5007 product:mitsubishi
Modbus	port:502,503 Unit
NPort Moxa	port:4800 Moxa Nport Device
OPC UA	port:4840 DisplayName
PCWorx	port:1962 PLC
ProConOS	port:20547 PLC
S7comm	port:102 Basic Module
XPort Lantronix	port:30718 Lantronix

evidenced by the high number of services like Modbus, Codesys, PCWorx, S7comm, Ethernet/IP, Fins, OPC UA, GE-SRTP, ProConOS, Crimson and Melsec-Q. About DNP3 and IEC-104, it is known that these protocols are employed almost exclusively in the power distribution field, therefore it goes without saying that their online exposure is highly risky. Finally, we can even pinpoint the online exposure of some gas stations, as shown by the ATG devices that are purposely designed to monitor fuel tanks. All 6038 services are to be considered vulnerable and at-risk simply because exposed online.

Table 3 shows the first 10 ISPs that serve the 82.61% of the 5936 total IP addresses found. First, it can be noticed that the 52.28% of the IP addresses refer to mobile customers (i.e. Telecom Italia Mobile, Vodafone Italia and Wind Tre); these kinds of subscription are typically more expensive and less performing than wired ones, suggesting that those systems are likely placed in areas that cannot be cabled and the only option for the owners was a mobile subscription line. Second, without a doubt at least 13.64% of the IP addresses belong to business entities due to the fact they are served by Telecom Italia Business. All remaining 1032 IP addresses belong to smaller ISPs or to other entities, among which we identified 109 IP addresses assigned to universities and research institutes. The sole analysis of the IP addresses did not enable us to achieve further information about the owners of the exposed devices.

Lastly, although Shodan claimed to be able of geolocating the IP addresses, we ascertained that the coordinates found by Shodan were very often incorrect; specifically, we tested Shodan's geolocation functionality on some IP addresses of which we already knew the exact locations, leading to wide inconsistency in Shodan's results. We believe that the causes behind this

Table 2
ICS Services Found Exposed Online in Italy

ICS Services	Occurrences
KNX	1738
Fox	1210
Modbus	1167
Codesys	410
PCWorx	332
S7comm	271
NPort Moxa	270
XPort Lantronix	191
BACnet	158
Ethernet/IP	136
Fins	86
ATG	26
DNP3	13
OPC UA	12
GE-SRTP	6
ProConOS	5
IEC 104	4
Crimson	2
Melsec-Q	1
Total	**6038**

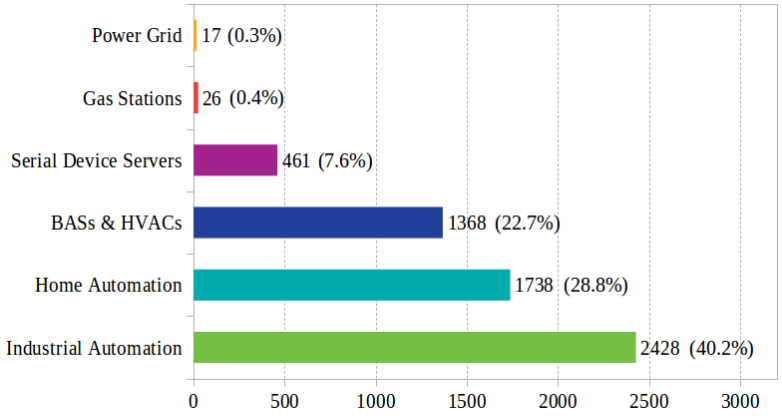

Figure 1: Distribution of the ICSes found exposed in Italy.

inconsistency might be the large number of mobile subscription lines already shown in Table 3 and the unknown identities of the assignees of the IP addresses (which are mainly assigned to the ISPs). Probably Shodan's algorithm confuses the actual location of the device with the location of the ISP's Point of Presence. It could also be that this simply represents a limit of Shodan and perhaps other paid services could better pinpoint the correct locations of the IP addresses.

Table 3
Top 10 Internet Service Providers

N°	ISP	Occurrences
1°	Telecom Italia Mobile	1257
2°	Telecom Italia	822
3°	Vodafone Italia	685
4°	Telecom Italia Business	669
5°	Wind Tre	622
6°	Vodafone Italia DSL	287
7°	Fastweb	283
8°	EOLO	235
9°	Irideos S.p.A.	44
10°	NGI SpA	44
—	**Sum**	**4904**
—	**Total**	**5936**

4.2. IT Services

As previously stated, starting from the data already collected and performing additional targeted searches, we conducted a survey about the exposure of ICS services over typical IT protocols like HTTP and VNC. Specifically, here we refer to HMIs and other management systems that were left reachable by anyone over the Internet. The variety of these systems which are often customized makes it difficult to quantify them in an automated fashion. However, they are extremely easy to find for someone who knows the right keywords. Many of such systems are protected by weak password-based authentication mechanisms, though the vast majority have no authentication at all: at the time of writing, the VNC servers in Italy that do not even ask for a password are 353.

Here we show some of the most noteworthy findings, properly anonymized and grouped by field of application. In full compliance with the Italian law, we state one more time that the services were lacking of any authentication mechanism, that we never even attempted to access any device that had any kind of authentication mechanism deployed, and that we simply browsed the services without executing any command nor modifying any setting. Despite what follows is serious, we decided to present it anyway because we believe that the reader might understand better the severity of this topic by looking at an actual graphical management interface exposed online than by simply looking at some cold cryptic banner of a random communication protocol. In any case, we want to stress that both cases are equally severe.

4.2.1. Wind Power

Thousands of web servers for managing different kinds of wind turbines and wind farms were found exposed over the Italian part of the Internet and the vast majority of those were protected by simple password-based authentication mechanisms. However, many web servers were still found totally unprotected. For instance, Figure 2 shows a web interface from where it seemed possible to alter the settings of a wind turbine belonging to a wind farm made of 11 more

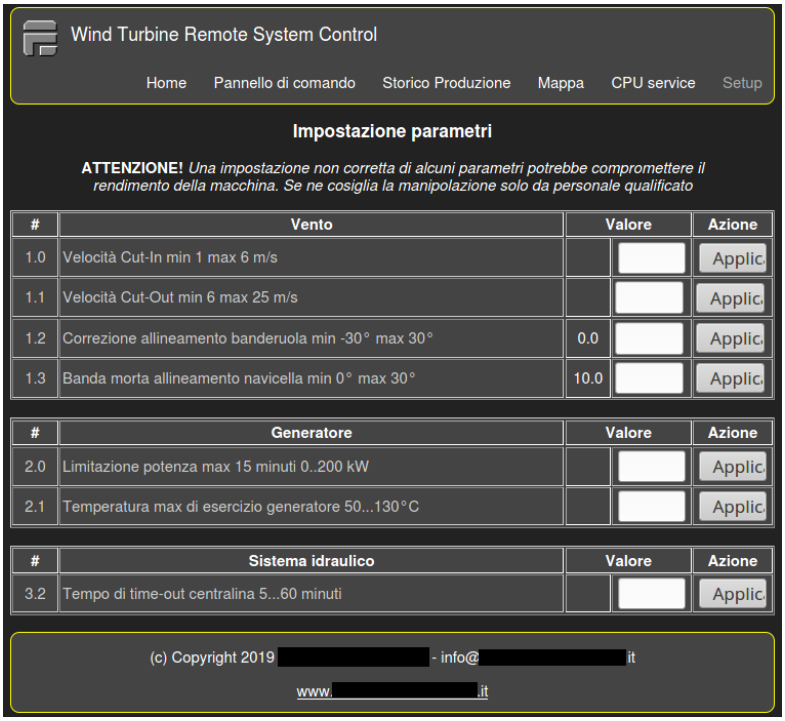

Figure 2: Web Interface of a Wind Turbine.

turbines. From the same web interface it was also possible to monitor the status of the wind

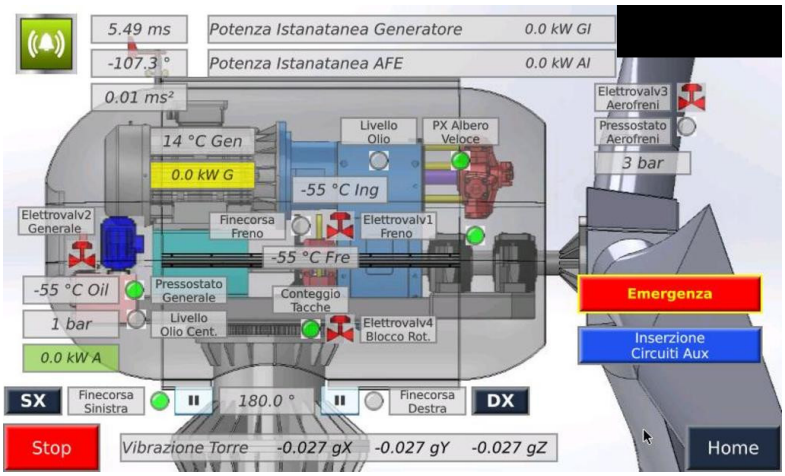

Figure 3: Remote HMI of a Wind Turbine.

turbine and apparently even to start or stop the turbine's blades. This specific management software was found exposed on other 4 IP addresses connected to wind turbines belonging to wind farms all located in different places. Figure 2 shows another case of a wind turbine

Figure 4: Remote HMI of a Solar Farm.

whose HMI was remotely controllable via VNC over the RFB protocol; apparently, it would have been possible to start or stop the turbine, or to press a baffling ”emergency” button. Further examining the services exposed by the IP address of the latter case, we also found a video stream over RTSP of the inside of the wind turbine and an SSH server. Knowing that the SSH public keys are often hardcoded in software and shared among similar devices of the same brand, we queried Shodan’s database for this specific SSH fingerprint and we found 30 more IP addresses connected to other remote management systems installed in solar and wind farms or hydro-power plants. However, this time all systems were implementing authentication via password.

4.2.2. Solar Power

As for Wind Power, over a thousand of different kinds of web platforms for managing solar farms were found exposed over the Italian IP address space and most of them were protected by simple password-based authentication mechanisms. It must be considered that, just like for the other renewable sources in Italy, the energy power generated in small solar plants contributes to a considerable extent to the fulfillment of the national energy demand, therefore a systematic cyber-attack against such infrastructures could potentially cause important impairments all over the Country. For instance, in Figure 4 we present an HMI that monitors a solar farm; this solar plant was composed of two modules that were monitored by two identical HMIs (both exposed) and each module was generating around 2000kW for an estimated total power of 4000 kW. It can be noticed that the solar plant under analysis appears to be somehow connected to the power supply grid of a well-known Italian power company, hence we should consider the

possibility that any denial of service caused to the solar plant could affect the local power grid too.

4.2.3. Hydroelectric Power

For the sake of brevity, we present just a few of all the ICSes belonging to hydroelectric power plants that we discovered online. Figure 5 and Figure 6, Figure 7 and Figure 8, and Figure 9 respectively show 3 different hydroelectric power plants. Due to the fact that their HMIs were publicly exposed and lacking any kind of protection, we could have freely acted (but obviously we have not) on the water intake structures or on the turbines. Out of curiosity, we also searched the Web looking for some information about these plants and we found that they seem to be supplying energy to their respective local power grid. Moreover, we found that the realization of one of them apparently cost around 800.000€ and that it produces an estimated revenue of 100.000€ per year.

5. Future work

Understanding whether the devices found exposed online were for domestic or industrial use was a very difficult task due to the presence of several limitations typical of the approach we pursued in this work, yet the only one we could follow to the extent permissible by the Italian law. While performing the survey no active port scanning was done, instead we fully relied on Shodan's indexing in order to not fall into potential technical or legal issues: from a technical perspective,

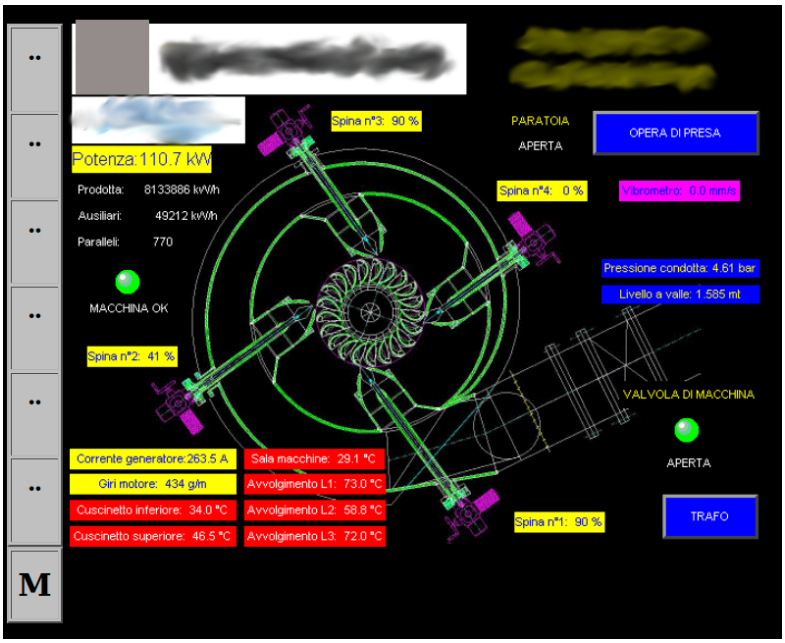

Figure 5: Remote HMI of a Hydropower Plant.

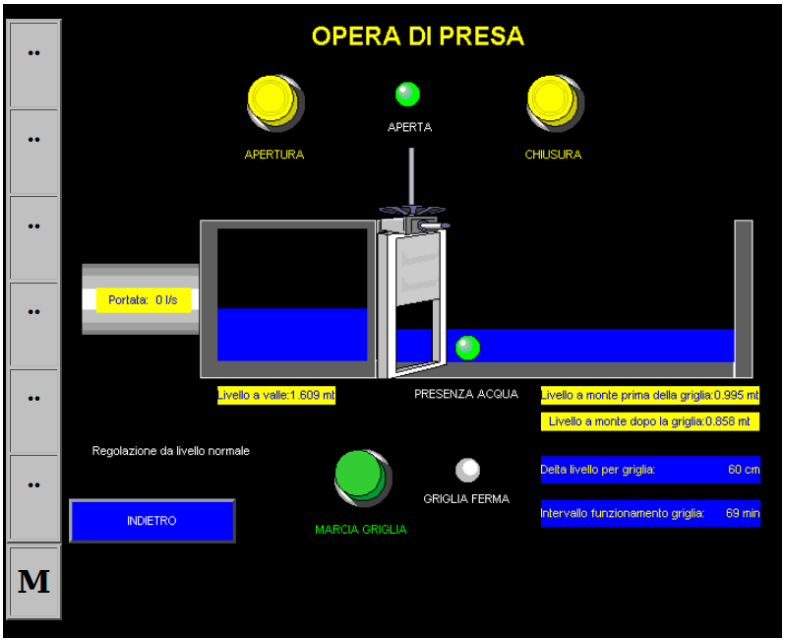

Figure 6: Remote HMI of a Hydropower Plant.

the devices under analysis are notoriously delicate and they can accidentally break even after basic network scans; from a legal perspective, the Italian penal code punishes with imprisonment who disrupts the availability of public or private services or who illegally commits unauthorized access to computer systems (especially those of public or military interest), regardless of the quality of the protective measures. [20]

For the reasons above, it was not possible to evaluate the type or the number of vulnerabilities (i.e. *CVE*) on our findings. Anyway, the very act of estimating such vulnerabilities could have been misleading: the message we want to express is not about the presence or absence of known and unknown vulnerabilities, rather the fact that ICSes should not be exposed at all. In other words, the purpose of this work is to highlight the wrong posture of many systems with regard to the proper implementation of the cybersecurity best practices.

Also, the list of protocols used to estimate the exposure surface of the Italian ICSes is not to be considered exhaustive, although it already gathers the most used ICS protocols; therefore, because this study did not cover every existing ICS protocol, the actual number of exposed devices could be higher, making the number of devices found in this work a lower bound.

Finally, the next step we plan to take is to extend our research to consider all the Internet address space, scanning the worldwide ICS landscape in a continuous monitoring approach instead of performing a single survey.

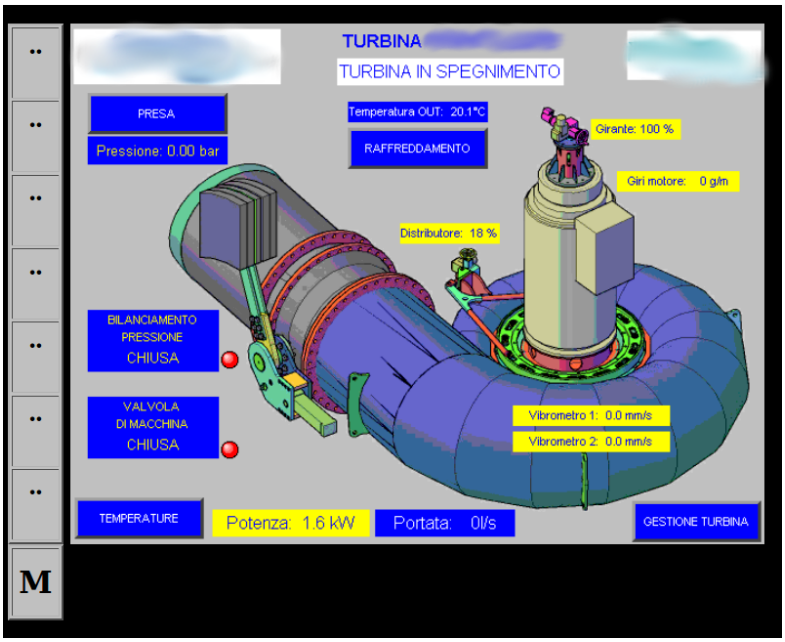

Figure 7: Remote HMI of a Hydropower Plant.

Figure 8: Remote HMI of a Hydropower Plant.

6. Conclusion

In this work we assessed the online exposure of the Italian ICSes. To this end, after having identified the most used ICS protocols, we proceeded to detect the presence of such systems over the Italian IPv4 address space. We found that more than 6.000 Italian ICSes are exposed over the

Internet. The fields of application are various: we found home automation systems, building automation systems and industrial automation systems. We also found devices belonging to power grids and to gas stations. Lastly, we found many unprotected HMIs accessible via web or via remote desktop applications, mainly related to renewable power generation plants and to HVAC systems.

These results suggest that the real number of unprotected ICSes on the Italian IP space could be even larger; it is safe to assume that a motivated and economically supported attacker, who would carry out his actions outside the law, could achieve better results than the ones presented in this work. Nonetheless, we believe that what we achieved is enough to prove that the online exposure of ICSes is a widespread problem that potentially affects all industrial sectors. The causes are without a doubt the digital illiteracy and the negligence of the operators (both technicians and executives) who, willingly or not, often left their systems unguarded.

It is important to underline that we cannot exclude that among what we found there could be something of strategic value; however, the limitations of our approach did not enable us to investigate this possibility. Also, we believe that a successful attack even against the ICSes of a small enterprise could affect bigger enterprises too and have severe impacts over the whole national context, given that the Italian industrial landscape is made of a vast amount of small and medium-sized enterprises which are often links of the national supply chain. Besides, given that smaller ICSes might share common technology with critical ICSes, we must take into account that smaller ICSes might be perfect cyber shooting ranges that the threat actors could use to validate their attack strategies before targeting actual critical systems.

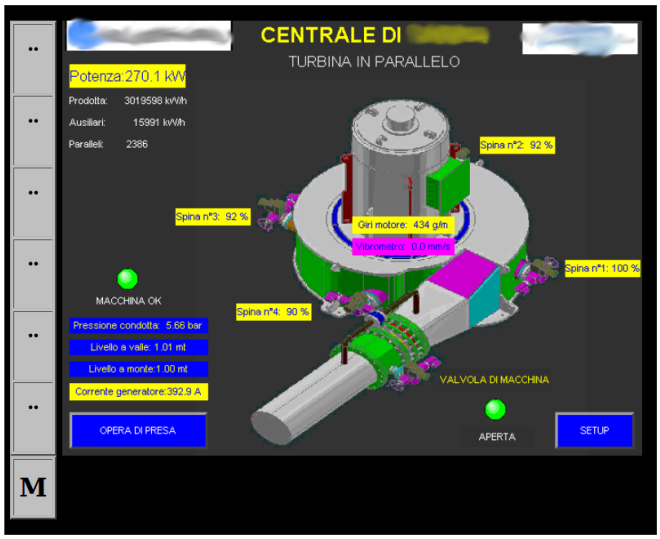

Figure 9: Remote HMI of a Hydropower Plant.

Acknowledgement

This work has been partially supported by the IoT-STYLE project RG12117A7CE68848.

References

[1] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. Sidorov, A. Timorin, Industrial control systems and their availability, 2016. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190427/KL_REPORT_ICS_Availability_Statistics.pdf.

[2] S. Hilt, N. Huq, V. Kropotov, R. McArdle, C. Pernet, R. Reyes, Exposed and vulnerable critical infrastructure: Water and energy industries, 2018. URL: https://documents.trendmicro.com/assets/white_papers/wp-exposed-and-vulnerable-critical-infrastructure-the-water-energy-industries.pdf.

[3] M. Nawrocki, T. C. Schmidt, M. Wählisch, Uncovering vulnerable industrial control systems from the internet core, in: NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, 2020, pp. 1–9. doi:10.1109/NOMS47738.2020.9110256.

[4] A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Halderman, M. Bailey, An internet-wide view of ics devices, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016, pp. 96–103. doi:10.1109/PST.2016.7906943.

[5] P. Paganini, Top cybersecurity predictions for 2020, 2019. URL: https://resources.infosecinstitute.com/topic/top-cybersecurity-predictions-for-2020/.

[6] A. Yan, Fortinet 2019 operational technology security trends report, 2019. URL: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-security-trends.pdf.

[7] Shodan, Shodan, 2020. URL: https://www.shodan.io.

[8] O. of Public Affairs, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector, Department of Justice, 2016. URL: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged, press Release Number 16-348.

[9] M. Thompson, Iranian cyber attack on new york dam reveals future of war, 2016. URL: https://time.com/4270728/iran-cyber-attack-dam-fbi/.

[10] Anonymous, Bacnet official website, 2020. URL: http://www.bacnet.org/.

[11] Anonymous, Codesys official website, 2020. URL: https://www.codesys.com/products/codesys-communication/standard-ethernet.html.

[12] Anonymous, Redlion's crimson official website, 2020. URL: https://www.redlion.net/red-lion-software/crimson.

[13] Anonymous, Dnp3 official website, 2020. URL: https://www.dnp.org/About/Overview-of-DNP3-Protocol.

[14] Anonymous, Ethernet/ip official website, 2020. URL: https://www.odva.org/technology-standards/key-technologies/ethernet-ip/.
[15] Anonymous, Omron's fins official website, 2020. URL: http://www.ia.omron.com/support/glossary/meaning/168.html.
[16] Anonymous, Iec 60870-5-104 international standard, 2020. URL: https://webstore.iec.ch/publication/25035.
[17] Anonymous, Knxnet/ip official website, 2020. URL: https://support.knx.org/hc/en-us/articles/360000040999-KNX-Specifications.
[18] Anonymous, Modbus official website, 2020. URL: https://modbus.org/.
[19] Anonymous, Opc unified architecture official website, 2020. URL: https://opcfoundation.org/about/opc-technologies/opc-ua/.
[20] Anonymous, artt. 615-ter, 635-bis, 635-ter, 635-quater, 635-quinquies, 2020. Https://www.cyberlaws.it/2019/codice-penale/.