Exposed and Vulnerable Critical Infrastructure:

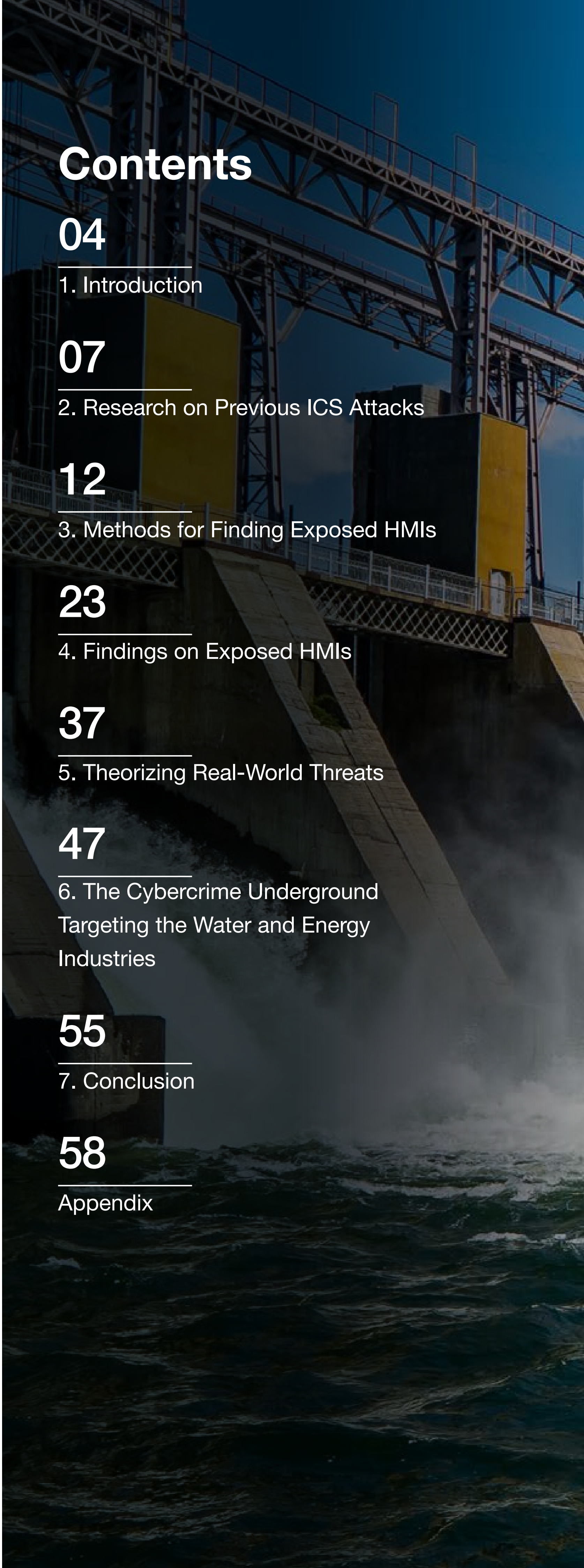
Water and Energy Industries

Stephen Hilt, Numaan Huq, Vladimir Kropotov,
Robert McArdle, Cedric Pernet, and Roel Reyes

A TrendLabs[SM] Research Paper

Cover image: Maxim Burkovskiy/Shutterstock.com

For Raimund Genes (1963-2017)



Contents

The water and energy (W&E) sectors are critical to the economy of every nation, in fact to human life, and need to be secured. Water is a natural extension of the energy sector, with hydroelectric plants operating in most countries around the world. Water is also a key component in geothermal plants, which generate heat and electricity. With news on cyberattacks dominating daily headlines, it is important to study the cyber risks faced by these industries.

The primary goal of this research was to demonstrate just how easy it is to discover and exploit cyberassets in the water and energy sectors using basic open-source intelligence (OSINT) techniques. In this paper, we present the techniques we used to find exposed cyberassets as well as data gathered from the internet of things (IoT) search engine Shodan and other open data sources. We have found a certain amount of exposed and often unprotected W&E systems online, bringing danger closer to these critical resources — and to the general population. Using a technique we call GeoStalking, we were able to find ranges of IP addresses in the immediate vicinity of the facilities we were able to locate.

After an overview of exposed devices and systems we found, we enumerate a list of likely attackers and their motives and assess their damage potential. Based on our research findings, we then pose real-life cyberattack scenarios and their impact on cities/nations. In addition, we provide a glimpse of the chatter surrounding water and energy infrastructure in the cybercriminal underground.

Finally, we provide defensive strategies for protecting the main industrial control system (ICS) equipment and the supply chain of the water and energy sectors against attacks, including those from third-party contractors/integrators and insider threats.

1. Introduction

Contrary to other sensationalized stories on the vulnerability of internet-connected critical infrastructure (CI), which focused on large organizations, our findings were mostly from small to medium organizations within these sectors. In discussions with larger organizations, we found that while they already had security firmly in mind — employing many layers of defense, dedicated information security teams and regular security assessments — most still consider an attack against their ICS infrastructure a realistic threat.

On the other hand, the exposure of more mid-tier organizations is still a concern and an important subject for research for two main reasons. First, because of CI interdependencies and the distribution network setups, failures in mid-tier providers will have cascading and far-reaching effects further up the chain. Second, and more importantly in our opinion, we limited our research to only look at fully publicly exposed systems to lower the risks of causing real-world damaging effects. A real-world attacker would have no such restrictions and could use a number of traditional approaches associated with targeted attacks to compromise larger players in this sector, which we already saw in 2015 with the power outages in Ukraine.[1] For an attacker of this caliber, more mid-tier players also act as the perfect testing ground, where they can try out the effects of their attacks in less risky settings.

The primary goal of this research is to demonstrate just how easy it is to discover and exploit cyberassets in the water and energy sectors using basic open-source intelligence (OSINT) techniques. Given the extreme importance of these two sectors, a more aggressive agenda needs to be urgently pursued to better protect and safeguard water and energy CI from cyberattacks.

According to the United Nations (UN), already 55 percent of the world's population lives in urban areas, a number that is expected to grow to 68 percent by 2050.[2] Big cities require an extensive array of utilities, goods and services to operate daily. More specifically, cities rely on sectors that include (but not limited to): utilities (power, water, gas, sanitation, etc.), financial sector, healthcare, education, government (municipal, state, and federal), retail, agriculture, transportation, manufacturing, communications, security and policing. These CI sectors[3] are the lifeblood and vital organs of modern industrial nations. When studying CI, one of the frequently asked questions is: What are the CI interdependencies? Tyson Macaulay, in his book "Critical Infrastructure – Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies," explores CI interdependencies.[4] Critical infrastructure has mutual interdependencies; the impact on one will be felt by others. Indicators of interdependencies could be either econometric or data-dependency metrics — all sectors spend and manage money; all sectors send and receive information. Using econometric analysis, the book presents an interdependency graph for critical infrastructure in the United States (see Figure 1).

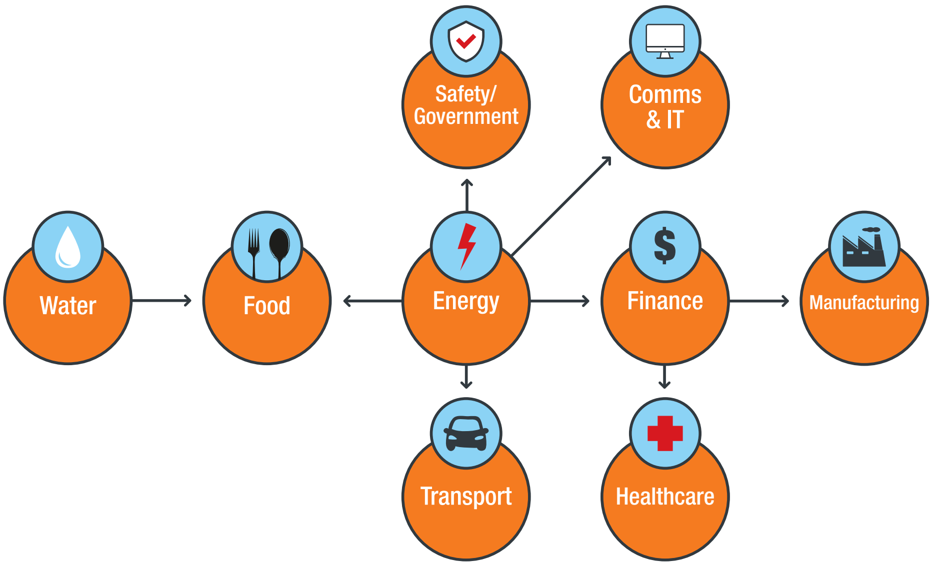


Figure 1. U.S. critical infrastructure dependency flow according to econometric analysis (adapted from Macaulay 2009)[4]

The method used for generating the U.S. CI interdependency graph can also be applied to CI of other countries, and it is expected that node dependencies and graph shape will be similar. What jumps out immediately from the graph is this: In the U.S., the energy sector is the top CI — a failure here will most likely impact at least five CI sectors directly and the remaining three CI sectors indirectly through the possibility of cascading failures. This is not difficult to imagine especially in major industrial economies where almost every aspect of the economy is directly dependent on steady energy supplies.

In this research paper, we study cybersecurity risks in the water and energy sectors. Water is a natural extension of the energy sector, with hydroelectric plants operating in most countries around the world. Water is also a key component in geothermal plants, which generate heat and electricity. With cyberattack news dominating daily headlines, it is important to study the cyber risks faced by these sectors. In this paper, we present the following:

- Using OSINT techniques, we explored the water and energy sectors to see what types of exploitable cyberassets are accessible to would-be attackers. We gathered data using the IoT search engine Shodan, as well as using other less publicized open data sources.
- We present findings from security research papers on ICS published by Trend Micro to highlight the potential threats faced by exposed cyberassets in the water and energy sectors.

- When studying cybersecurity risks, it is crucial to identify likely attackers, probe their motives, and assess damage potentials. Based on our research findings, we present real-life cyberattack scenarios that we identified and discuss how they can affect cities/nations. Furthermore, we investigate the chatter surrounding water and energy CI in the cybercriminal underground and present what criminals are discussing in forums.
- We use data collected from Trend Micro™ Smart Protection Network™ infrastructure to show what types of cyberattacks water and energy sector organizations are facing daily, and the potential implications of those cyberattacks.
- Finally, in the Appendix, we provide defensive strategies for protecting the main ICS equipment and the supply chain of the water and energy sectors. Furthermore, we also discuss other important related topics including cyberattacks against third-party contractors/integrators and insider threats.

2. Research on Previous ICS Attacks

In this report, we will discuss several examples of exposed and vulnerable systems on the internet related to the energy and water sectors. However, is a vulnerable system as much of a concern if there are no attackers actively targeting them? Saying that a system is vulnerable simply means that a weakness is present, or that there is a protection gap due to its exposure. It is important however to always factor in the risk that an attacker would make use of this vulnerability to exploit the system and gain access to it.

In the case of exposed ICS or supervisory control and data acquisition (SCADA) systems, we can reliably say, based on past research Trend Micro has carried out, that such systems are indeed of interest to attackers — and have been for quite some time now. In 2013, the Trend Micro Forward-Looking Threat Research (FTR) team released two reports on research that were carried out to explore exactly this. In the first research,[5] we set up a global network of 12 high-interaction honeypots that mimicked water plants using a combination of real-world SCADA equipment and custom machines designed to look exactly like the network of real facilities we had examined in the past. In the experiment, every single system was attacked, with 15 percent of those attacks considered critical, i.e., would have caused catastrophic failure in the equivalent real-world environment. Our second research in the same year[6] contained a more in-depth analysis of ICS and SCADA threat actors.

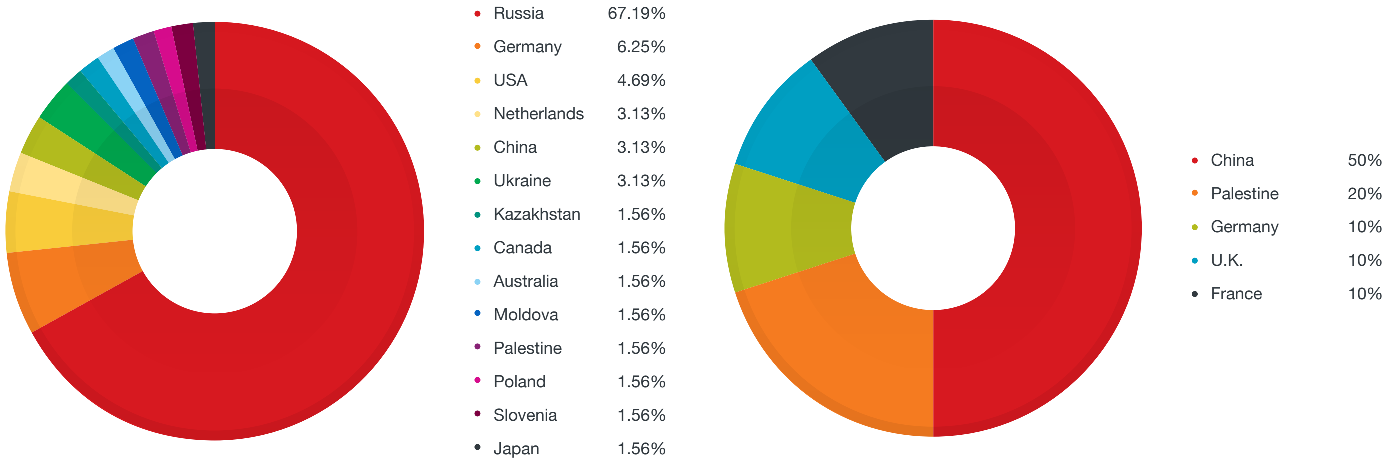


Figure 2. Breakdown of origin countries for non-critical and critical attacks from our SCADA honeypot research[6]

In 2015, these two research works were followed by a look at attacks on a different type of ICS, namely pumps at gas stations.[7] This time, we created realistic representations of systems that are used to manage such stations, which we called Gaspot, and once again we observed a number of attacks on all our global setups. In that research, we noticed that some of the top attacking origin countries differed from those that we observed in the 2013 researches. There were a number of factors that could have led to this as one system was a simulation of an ICS system that had multiple components, and Gaspot was a simulation of a single system. Gas stations would also have been on the radar of attackers due to another research published around that time.[8] Unlike our 2013 researches, the changes to these systems could not cause physical issues to any equipment, so the attacks that were seen were more in line with web defacement campaigns from hacktivism groups. In fact, we saw evidence that suggested links to either the Iranian Dark Coders (IDC) Team or the Syrian Electronic Army hacking groups. What this shows is a continued interest from attackers in such platforms, and even a lowering sophistication of the groups from which such attacks can originate.

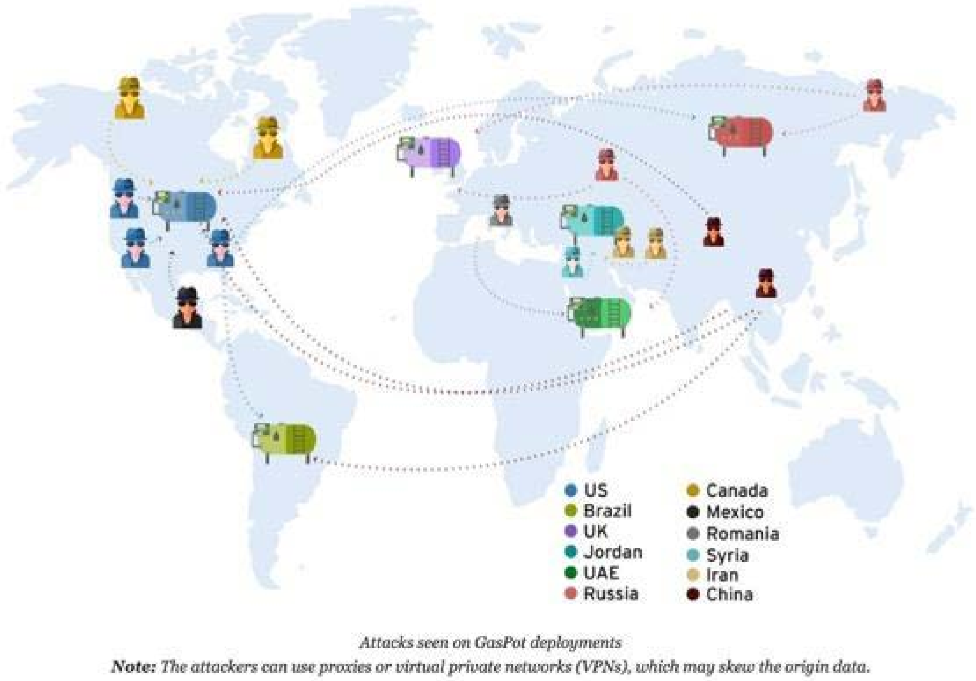


Figure 3. Attacks on our Gaspot deployments[7]

In addition to these researches, which focused on categories of vulnerable devices themselves, and those who would attack them, we have also seen a number of attacks on SCADA/ICS systems in previous years from well-known attack groups and campaigns. This is not an exhaustive list, but it clearly shows that such devices are being targeted by some of the more targeted campaigns out there.

- In 2014, the Havex[9] attack campaign (a malware associated with the Energetic Bear / Dragonfly group) was one of the first malware families that included the ability to find other ICS environments on the victim's network by, for example, performing a scan on process control (OPC) servers. This technique helped the malware to laterally move around and compromise such systems in isolated ICS environments, where a connection back to its command-and-control (C&C) server would not have been possible.
- The Sandworm campaign was also quite active in 2014.[10] During that period, it was found to be using a zero-day vulnerability to target SCADA that made use of GE's CIMPLICITY HMI (human machine interface).[11] This is not the only example of such a vulnerability being used by attackers. Trend Micro released a report in 2017 detailing a range of other vulnerabilities our Zero Day Initiative (ZDI) labs have seen for SCADA HMI over the years.[12]
- As previously mentioned, in December 2015, we saw an even more brazen attack on a real-world target, one that successfully took the Ukrainian Power grid offline.[13] This attack was tied to a wiper malware called Killdisk, which is associated with the Black Energy and Sandworm campaigns.[14] Not long after this, in 2016, there were reports that an Iranian hacking group had been targeting water dams in the United States.[15] The dams in question were small, but one theory behind the attack is that it was only a test for a larger operation that would have more damaging effects.
- In 2016, Verizon reported an incident affecting the water industry[16] in which attackers were able to compromise an unnamed water treatment plant in the U.S. and alter the amount of treatment chemicals being added to the water supply.
- This trend of compromises of SCADA systems continued in 2016 and 2017, with another power outage in the Ukraine[17] tied to a malware attack known as "Industroyer."[18] After that, the TRITON[19] group raised the stakes by going after the safety systems that control how such systems can shut down — and ultimately protect human life — during an emergency. While best practices specify that the safety systems and the main ICS system should be isolated and kept on separate networks by design and implementation, this is sometimes an overlooked security design issue from a networking stance.
- While all the above-mentioned attacks focused on the equipment controlling ICS devices, we have also seen multiple instances of sophisticated attack groups deploying highly targeted phishing attacks as an initial infection vector in the water and energy industries. In 2016,[20] we wrote about how the Pawn Storm espionage group had targeted the energy sector; and in 2017,[21] U.S. government officials spoke about targeted phishing attempts on the energy sector in the U.S., Turkey and Ireland.
- Such attacks continued into 2018, with the U.S. DHS and Federal Bureau of Investigation (FBI) issuing a **warning**[22] of cyberattacks targeting energy and other critical industrial sectors, which they tied to Russian-speaking espionage groups.

Almost all of the attacks detailed above were focused on attacking the actual network-connected SCADA systems, but of course that is not the only sort of attack that a company in the energy and water industries will face. Like every other organization today, there will also be attacks against their more traditional office environments. In some cases, these “traditional” attacks will act as a beachhead for attackers to then move laterally to the actual SCADA device targets, especially when the targets are not directly accessible from the internet. Traditional malware like ransomware can also be leveraged as a distraction by attackers to occupy the organization’s InfoSec teams while the main attack is carried out. As an example, here is a table containing statistics on the top 20 malware families we have observed trying to attack organizations in the water and energy industries from October 2017 to February 2018, arranged from highest to lowest number of instances. As can be seen, this list is not particularly different from malware we see hitting other industries and includes everything from downloaders to cryptominers. The top two entries are widespread file infectors or viruses — which again is similar to other industries. The more targeted attacks, as mentioned in the earlier list of past incidents, are rarer but are much more damaging.

Trend Micro Detection	
Name	**Instances**
PE_SALITY.RL	872,308
VBS_RAMNIT.SMC	382,230
TROJ_STARTER.SM	124,668
Ransom_WCRY.SM2	73,548
TROJ_DOWNADJOB.A	46,655
PE_RAMNIT.H	28,612
JS_NIMDA.A-1	26,638
TROJ_EQUATED.J	25,622
PE_RAMNIT.DEN	24.821
PACP_CORRUPTPE.STD	20,467
PUA_Dexon	19,955
PE_SALITY.ER	12,141
PE_NESHTA.A	10,827
WORM_COINMINER.RT	9,614
LNK_BONDAT.SMA	9,110
WORM_COINMINER.SMG	8,238
WORM_COINMINER.QA	7,546
TROJ_EQUATED.G	7,433
WORM_MESSEN.SMF	6,133
PE_Chir.B	5,853

Table 1. Top 20 malware families used in attacks against organizations in the water and energy industries (October 2017 to February 2018)

These previous researches by Trend Micro and others in the cybersecurity industry all point to a clear reality. Not only are critical systems from the water, energy and similar industries exposed and vulnerable on the internet today — they are also an active target for attack. To date these attackers have largely been well-resourced and sophisticated groups, more associated with espionage rather than financial gain. However, as also evidenced by some of the attacks in our "Gaspot Experiment," the barrier for entry to be able to carry out these attacks is dropping all the time.

3. Methods for Finding Exposed HMIs

In our research for this paper, we focused on looking at cyberassets within the water and energy industries that are publicly exposed on the internet. In discussing with large organizations in this industry, all had some of their equipment remotely accessible, but the protection level varied, from simple login to virtual private network (VPN) solutions. The types of exposed data depend on the device – for example, it could be a web interface/HMI, exposed ICS protocols, or remote desktop in the form of Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC). Regardless of the type of device exposed however, two important questions come to mind:

1. **Why are cyberassets exposed on the internet?**

These are common reasons behind the exposure of devices and systems online:

- Remote access was enabled on the system and connected devices to allow remote operations and troubleshooting.
- Remote access was enabled to serve a particular function. However, it was not disabled later when the purpose was fulfilled, and the device or system was possibly left in its enabled state.
- Remote access was enabled by a third-party integrator without communicating the action to the operator.
- Network settings were incorrectly configured, allowing direct device and system access.
- Connection to the internet is necessary for the devices and systems to function correctly.

2. **What are the potential risks associated with exposed cyberassets?**

Some of the possible risks presented by exposed cyberassets include the following:

- Exposed cyberassets could be compromised by hackers who steal sensitive data, for example, personally identifiable information (PII), intellectual property, financial data, and corporate data.
- Sensitive data could be leaked online without the owner's knowledge, for example, open directories on web servers, unauthenticated webcam feeds, and exposed ICS HMIs.

- Through various lateral movement techniques and by compromising just a single exposed cyberasset, hackers could gain entry into the corporate network or an ICS network and subsequently perform sabotage, espionage, or fraud.
- Compromised cyberassets could be used to run illegal operations such as executing distributed denial-of-service (DDoS) attacks, deploying botnets, cryptomining, hosting illegal data, committing fraud, etc.
- Compromised cyberassets could be held hostage for ransom payments. This is damaging especially if they are critical to an organization or individual's operations.
- Cyberassets that operate CI can jeopardize public safety if compromised.

We have already stated previously that there is a big difference between exposed and "at risk," and we will address this in succeeding sections. For our research, we did not aim to carry out a completely exhaustive indexing of every at-risk system in our industries of interest as there is no way of getting complete figures that would tie to the true exposed attack surface. In our research, we were careful to only look at truly publicly exposed devices — ones with no authentication in place, and ones where simple scans would not potentially cause adverse effects. A determined attacker has no such restrictions, and there will be far more systems at risk when considering those with weak/default authentication or out-of-date patching for known vulnerabilities.

To identify these exposed systems, we combined two methods:

- Scanning the internet through well-established techniques
- Mapping water and energy facilities from the real world to IP netblocks using an approach we call "GeoStalking"

Method 1: Finding exposed devices via internet scanning techniques

There are a number of services available today that routinely scan the internet and allow researchers to carry out detailed searches within the results. By far, the most commonly used is Shodan.[23] Shodan scans the majority of exposed ports on internet-connected devices and gathers a significant amount of highly informative metadata. This includes banners describing the services running on the device, their versions, the operating system (OS) of the device, and the geographic location of the device (based on its IP address). The vast majority of devices scanned by Shodan will be what you would expect to find on the public internet, for example, web servers. In our case, we limited our search using Shodan to ICS devices related to the water and energy industries.

Another very useful feature of Shodan is that it takes screenshots of any of the more graphical exposed protocols[24] and allows a researcher to search historical results from these scans. These results also include systems with remote desktop (e.g., RDP/VNC) enabled but have no form of authentication in place — which is very useful for any researcher or attacker looking to find accessible HMIs. In this research, we used Shodan's IP history to download all historical data for a given IP address and then extracted the HMI screenshots from the data. This enabled us to view different page windows from the same HMIs as they changed over time (Shodan captured repeated screenshots) *without having to directly interact with the devices ourselves*.

Once a device of interest has been discovered, an attacker could expand the profiling of the device through a full port scan with a tool like Nmap. Shodan already scans these ports, though, for the majority of well-known ICS protocols. (See Figure 4 for a list of ICS ports.) An attacker could also port scan an entire netblock that has been discovered as belonging to the target organization through a WhoIs records search. In this research, we avoided using Nmap as, in some cases, even a simple port scan can actually have negative effects on the device being scanned.

Protocol	Ports
BACnet/IP	UDP/47808
DNP3	TCP/20000, UDP/20000
EtherCAT	UDP/34980
Ethernet/IP	TCP/44818, UDP/2222, UDP/44818
FL-net	UDP/55000 to 55003
Foundation Fieldbus HSE	TCP/1089 to 1091, UDP/1089 to 1091
ICCP	TCP/102
Modbus TCP	TCP/502
OPC UA Binary	Vendor Application Specific
OPC UA Discovery Server	TCP/4840
OPC UA XML	TCP/80, TCP/443
PROFINET	TCP/34962 to 34964, UDP/34962 to 34964
ROC PLus	TCP/UDP 4000
Red lion	TCP/789
Niagra Fox	TCP/1911, TCP/4911
IEC-104	TCP/2404

Vendor	Product or Protocol	Ports
ABB	Ranger 2003	TCP/10307, TCP/10311, TCP/10364 to 10365, TCP/10407, TCP/10409 to 10410, TCP/10412, TCP/10414 to 10415, TCP/10428, TCP/10431 to 10432, TCP/10447, TCP/10449 to 10450, TCP/12316, TCP/12645, TCP/12647 to 12648, TCP/13722, TCP/13724, TCP/13782 to 13783, TCP/38589, TCP/38593, TCP/38600, TCP/38971, TCP/39129, TCP/39278
Emerson / Fisher	ROC Plus	TCP/UDP/4000
Foxboro/Invensys	Foxboro DCS FoxApi	TCP/UDP/55555
Foxboro/Invensys	Foxboro DCS AIMAPI	TCP/UDP/45678
Foxboro/Invensys	Foxboro DCS Informix	TCP/UDP/1541
Iconics	Genesis32 GenBroker (TCP)	TCP/18000
Johnson Controls	Metasys N1	TCP/UDP/11001
Johnson Controls	Metasys BACNet	UDP/47808
OSIsoft	PI Server	TCP/5450
Siemens	Spectrum Power TG	TCP/50001 to 50016, TCP/50018 to 50020, UDP/50020 to 50021, TCP/50025 to 50028, TCP/50110 to 50111
SNC	GENe	TCP/38000 to 38001, TCP/38011 to 38012, TCP/38014 to 38015, TCP/38200, TCP/38210, TCP/38301, TCP/38400, TCP/38700, TCP/62900, TCP/62911, TCP/62924, TCP/62930, TCP/62938, TCP/62956 to 62957, TCP/62963, TCP/62981 to 62982, TCP/62985, TCP/62992, TCP/63012, TCP/63027 to 63036, TCP/63041, TCP/63075, TCP/63079, TCP/63082, TCP/63088, TCP/63094, TCP/65443
Telvent	OASyS DNA	UDP/5050 to 5051, TCP/5052, TCP/5065, TCP/12135 to 12137, TCP/56001 to 56099

Figure 4. List of several ICS ports[25]

There are other methods of scanning for exposed ICS devices on the internet, but we mostly used Shodan due to its reliability and the depth of its available data. However it is worth noting that in some cases Google® Search has been useful to discover certain classes of devices using customized searches (Google Dorking[26]), but these results lead to a lot of false positives and need to be filtered and validated manually to find those results related to the water and energy industries.

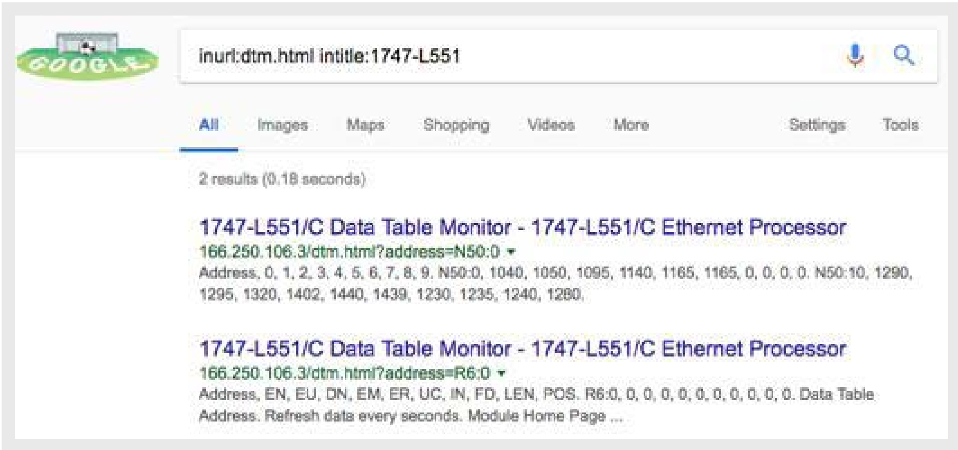


Figure 5. Example of a Google search leading to Rockwell Automation SLC-5 devices

Method 2: Mapping physical locations to IP addresses using "GeoStalking"

A second major approach we used was to first identify the physical location of a water or energy facility, and then proceeding to map it to the IP address of its corresponding internet networks. While the approach is not possible in every case, it has proved to be achievable in enough instances to be beneficial to our research. We call this approach "GeoStalking." This approach consists of two straightforward stages.

Stage 1: Finding real-world locations of energy and water facilities

In this first stage, there are a number of approaches, the most basic of which would be to simply know the location of a target facility in advance. There are a number of sites that allow a researcher to discover facilities from water, energy and other critical industries in a certain geographical area.

- ***Electrical Japan Power Plant Database***[27]

From their website, Electrical Japan Power Plant Database describes itself as "*a site to think about Japan's power problems after the Great East Japan Earthquake through "Visualization" and simulation* *of power supply (power station map) and power consumption.*" Looking at its website, however, showed that someone could easily use it to obtain data from the different power plants in Japan. One can list all hydro, wind, solar and nuclear power plants using specific location on Google Maps. This is valuable actionable information for a threat actor — an easy way to search for a vetted list of possible water and energy industry targets.

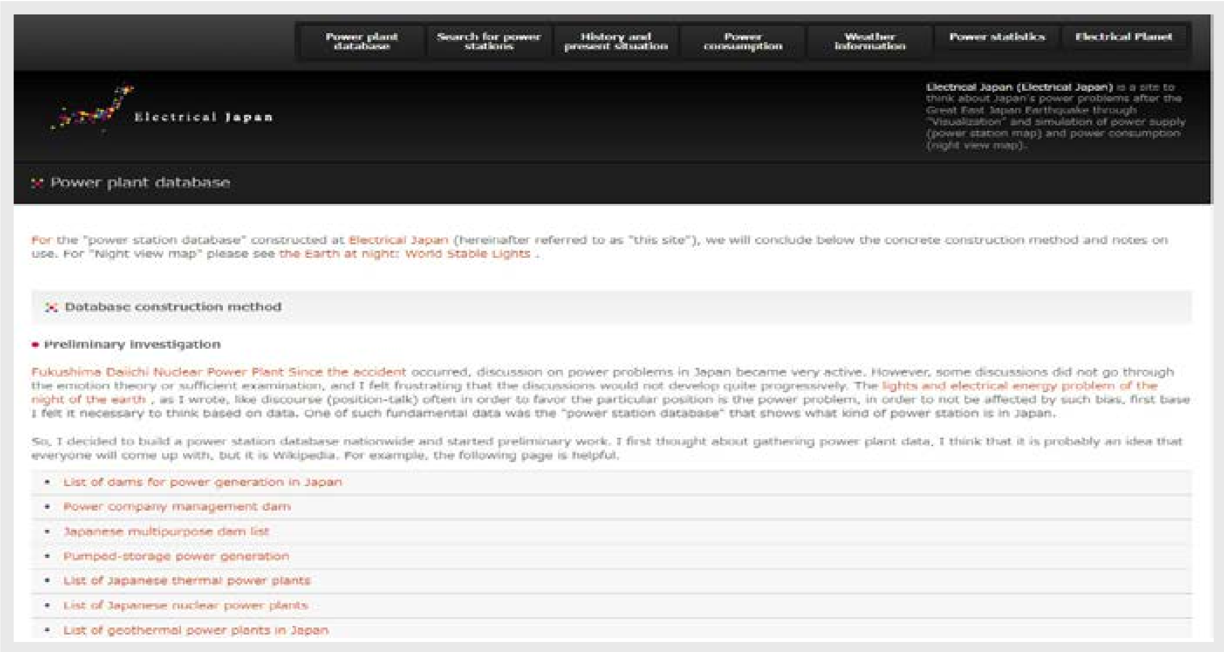


Figure 6. Electrical Japan Power Plant's main page

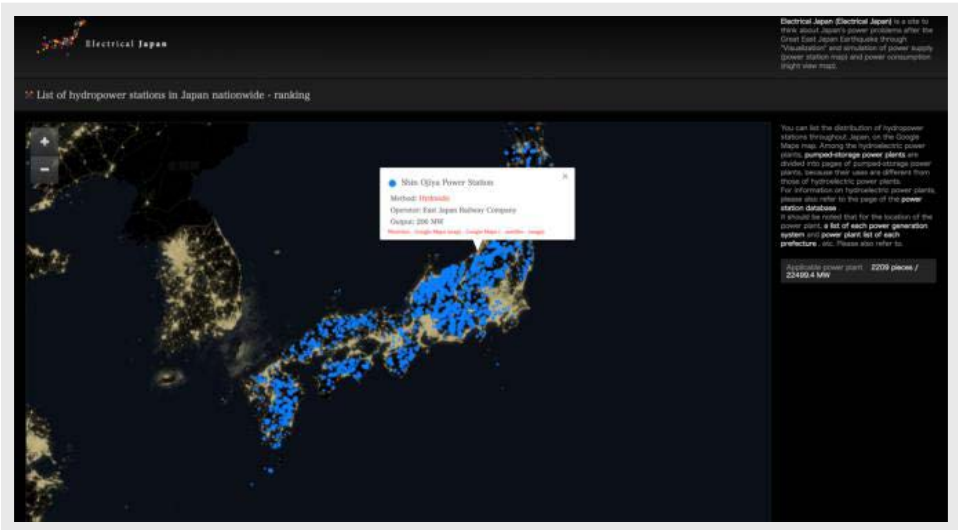


Figure 7. List of hydro power stations in Japan
(including information on the organization, output and type)

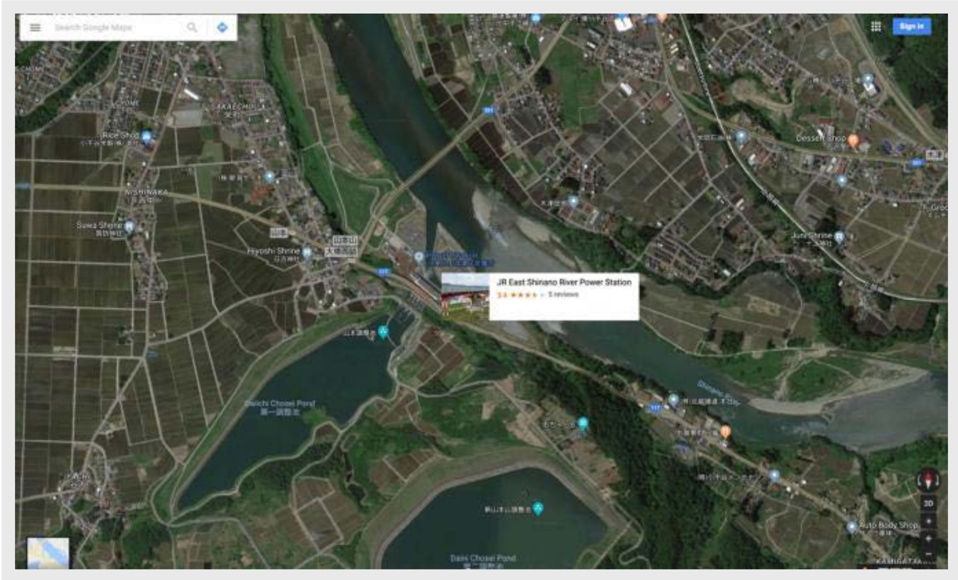


Figure 8. Geolocation of highlighted power station on Google Maps (Map data © 2018 Google)

Figure 9. Wind farms in Choshi, Japan (Map data © 2018 Google)

- ***Descartes Labs***[28]

The Descartes Labs website enables users to carry out image-based searches of physical locations. For example, once an attacker has identified the physical location of a target wind farm, the service can then be used to find other areas of the world that look similar in appearance. The website provides a global map at 15 meter resolution and a more detailed U.S. map at 1 meter resolution. The image scan for the website is at an early stage of development, so not all possible locations can be detected. But as the search algorithm becomes more mature, it will be able to locate all relevant images searched globally and reveal their physical locations. The site also contains a number of saved searches so people can start using it.

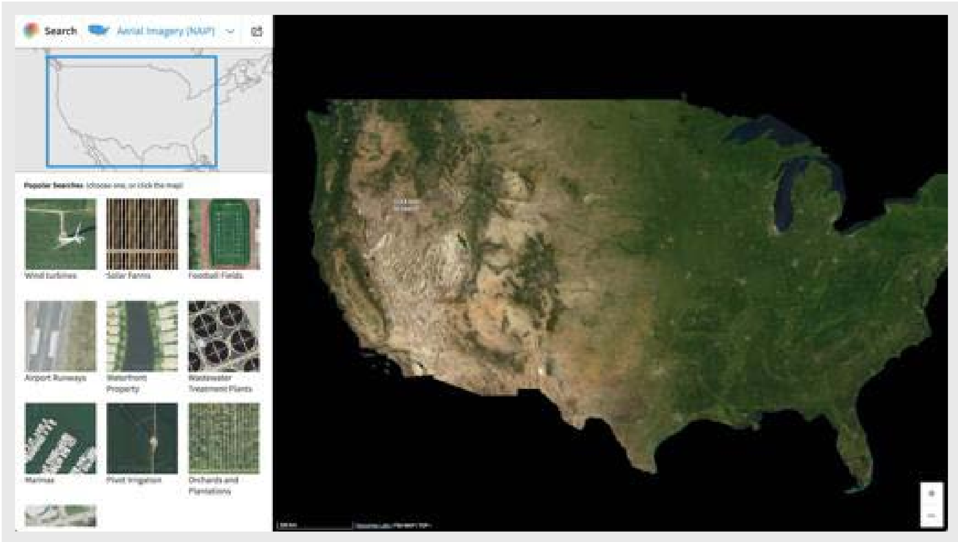


Figure 10. Screenshot of Descartes Labs website search (© 2018 Descartes Labs)

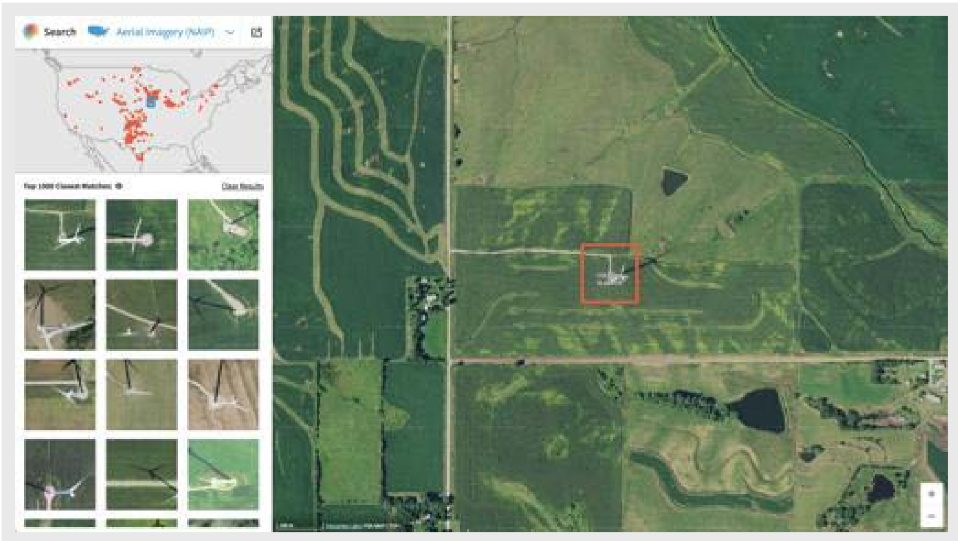


Figure 11. Screenshot of a Descartes Labs search result showing the physical location of a wind turbine in the U.S. (© 2018 Descartes Labs)

Figure 11 shows an example of results for wind farms found across the U.S. The red indicator on the upper left column is the actual physical location of each wind turbine, which is similar to the image selected on the main section. Using such a tool, a potential attacker could determine the physical location of other wind and solar farms.

Figure 12. Screenshot of a Descartes Labs search result showing a
hydro power plant in Japan (Map data © 2018 Google)

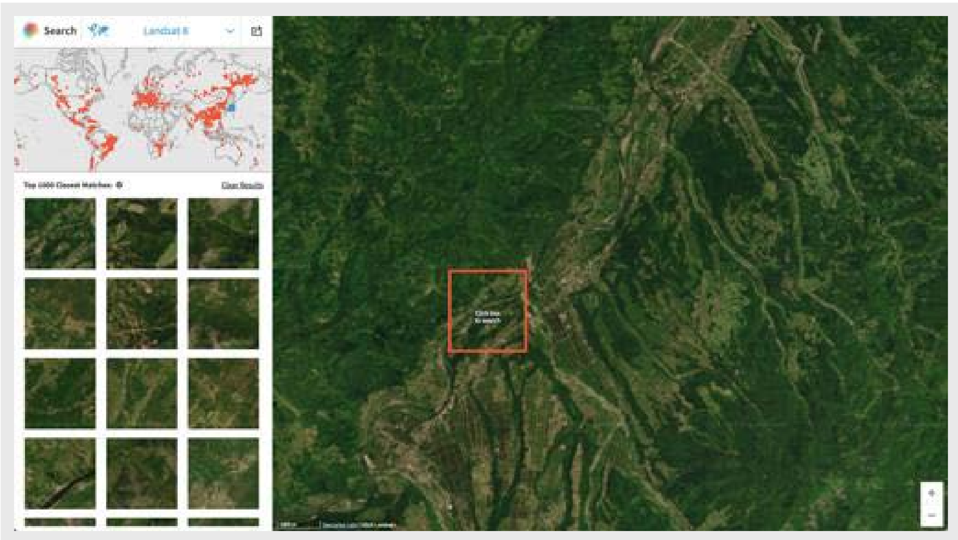


Figure 13. Screenshot of a Descartes Labs search result showing possible locations of
hydro power plants across the world (© 2017 Descartes Labs)

Figure 12 shows a hydro power plant in Japan (found using the Electrical Japan database), and Figure 13 shows similar locations in other places in the world. An attacker would of course need to first filter the list for non-relevant results.

- ***Other systems***

As with the Descartes Labs and Electrical Japan, numerous other charts exist for Europe and other specific countries. The Energy Charts website by the Fraunhofer Institute for Solar Energy Systems has a map of power plants in Europe that can be filtered by country, power source and capacity.[29] Another website, Picbleu.fr, has a map of the nuclear power plants in France.[30]

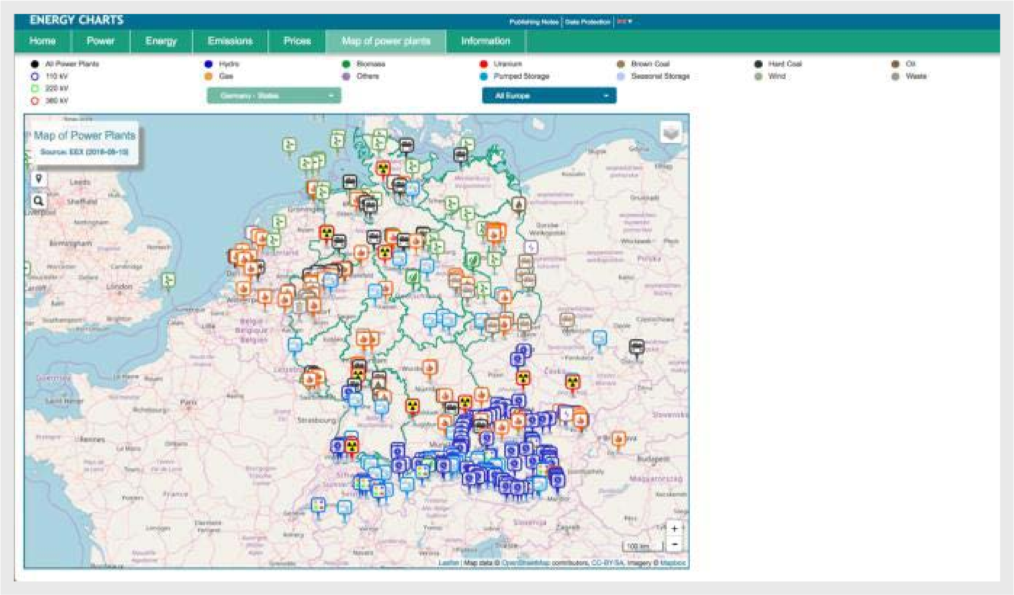


Figure 14. Energy charts of Europe

Stage 2: Mapping real-world locations to IP addresses

Once an attacker has found the physical location of a target, the next step is to attempt to find corresponding internet locations. To do this they can access available data from a geolocation service such as Maxmind[31] (which allows the mapping of location data to IP address data, and vice versa), along with results from Shodan, Nmap and other scanners previously mentioned.

For example, if an attacker first locates the physical location of a target wind turbine, he/she can then use IP geolocation to return a list of all IP networks within a certain radius. However, IP geolocation is rarely precise, so the attacker then validates these possible IP addresses by using a port scan or Shodan. The list is then narrowed down to the IP addresses whose profile matches the sort of ICS devices one would expect to find in a wind farm. The attacker can then perform a vulnerability assessment on these IP addresses to see if it is possible to can gain control of or disrupt the equipment. Lastly, if the attacker is able to obtain successful targets, he/she can now work in reverse: starting with the one device found using the GeoStalking process detailed earlier and then scanning nearby IP ranges (even the entire internet) for all similar devices, as it is likely an organization has a similar setup for many of its devices.

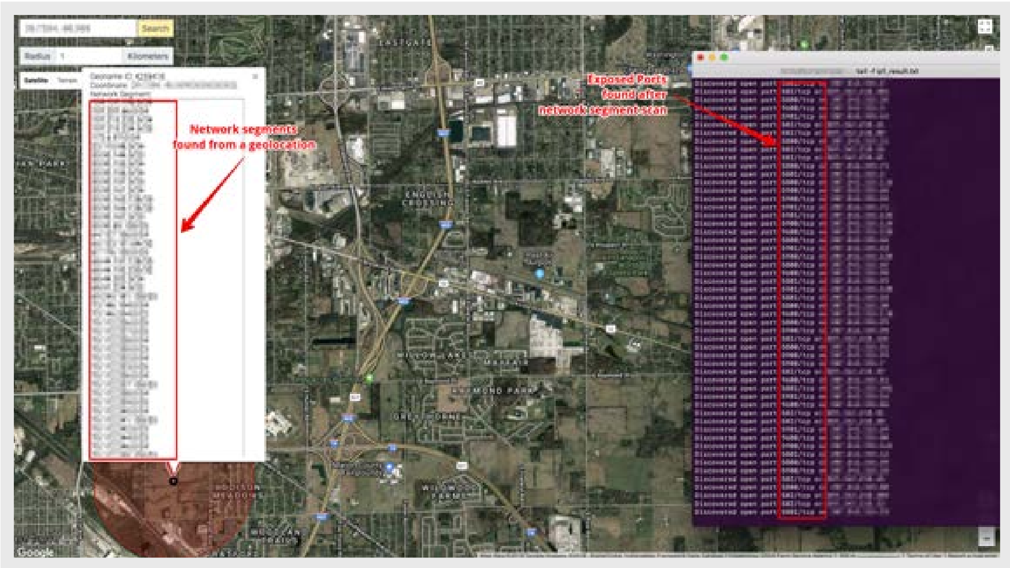


Figure 15. ICS/SCADA-related IP found using GeoStalking

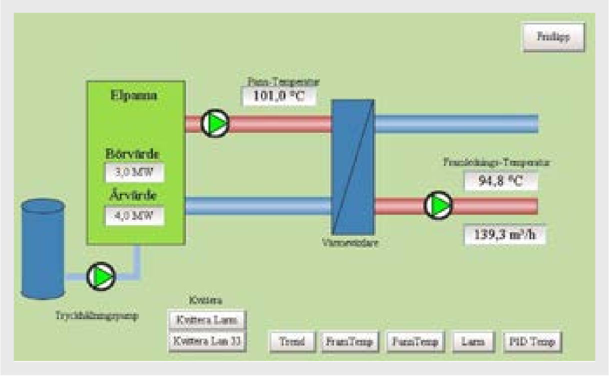
4. Findings on Exposed HMIs

Using Shodan and Shodan IP histories, we collected data on internet-exposed HMIs for the energy and water industries. In this section, we present a selection of the exposed HMIs we found. As previously stated, this is not meant to be an exhaustive search of all exposed HMIs as attackers would not be operating under the same constraints as researchers.

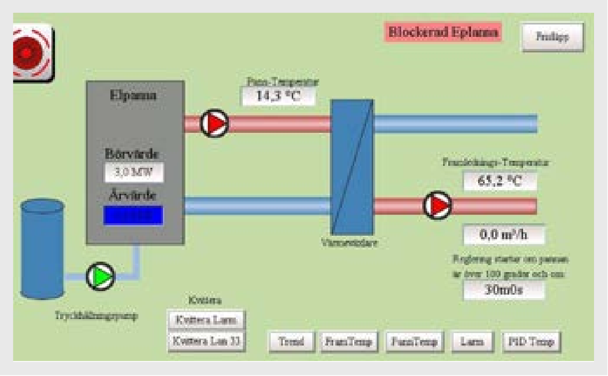
All identifiable elements in the screenshots have been deleted for privacy reasons. All screenshots were collected from Shodan data.

Exposed Water System HMIs

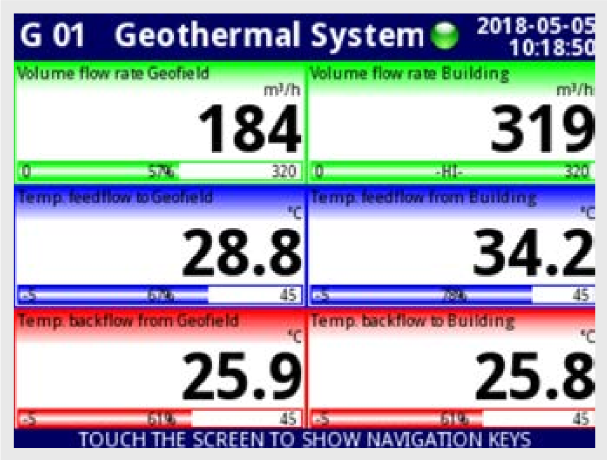
Unlike some of the other industry segments described later, the exposed water system HMIs we discovered came from all over the world.



Water heating system in an industrial facility located in Sweden. The boiler uses up to 3MW of electricity, which implies a very large volume of water is being heated and circulated. There is a "release" button at the top corner, which is likely a reset mechanism.



An alarm condition was triggered and the flow of water in and out of the boiler has stopped.



Geothermal system displaying the rates of water flow in/out of the building and the ingress and egress water temperatures.

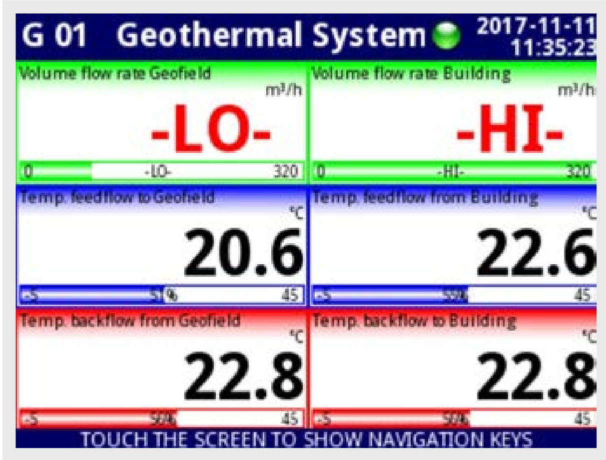
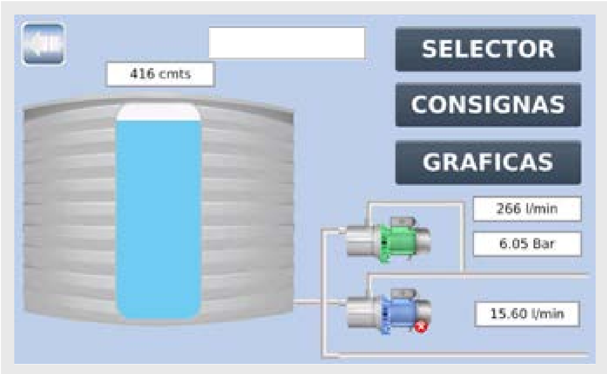
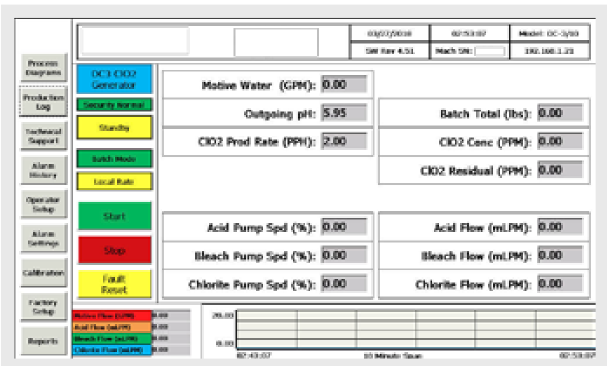


Image indicates water is not flowing properly from the geothermal well and there is a subsequent drop in water temperature, probably an error condition.

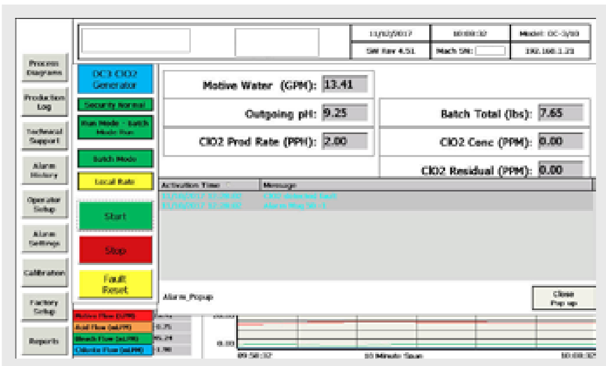


A monitor for a water pumping system. Top-level menu displays the available submenus: Selector, Readings, and Graph. This page shows one of the pumps is pumping water at 266 L/min, while the second pump is mostly inactive and pumps at 15.6L/min.

Another overview page shows both pumps are currently deactivated.



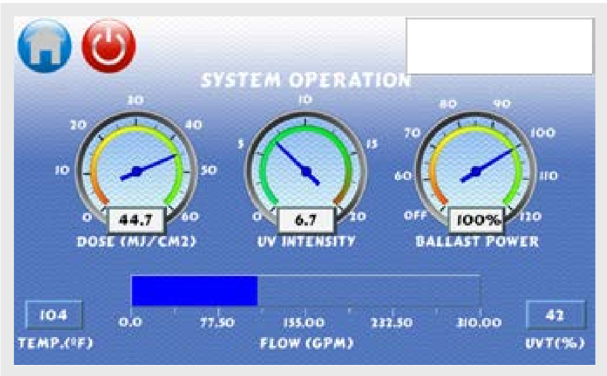
An overview menu showing readings from the different subsystems. The Start, Stop, and Fault Reset buttons are all accessible from this page.



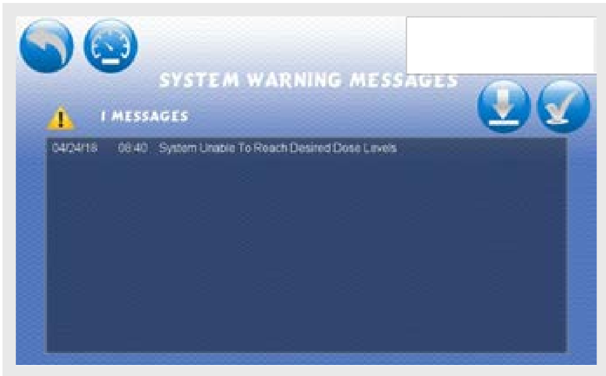
A pop-up menu displaying event information, including alarms.

Water filtration facility in Colombia. The HMI requires user authentication before full menu access.

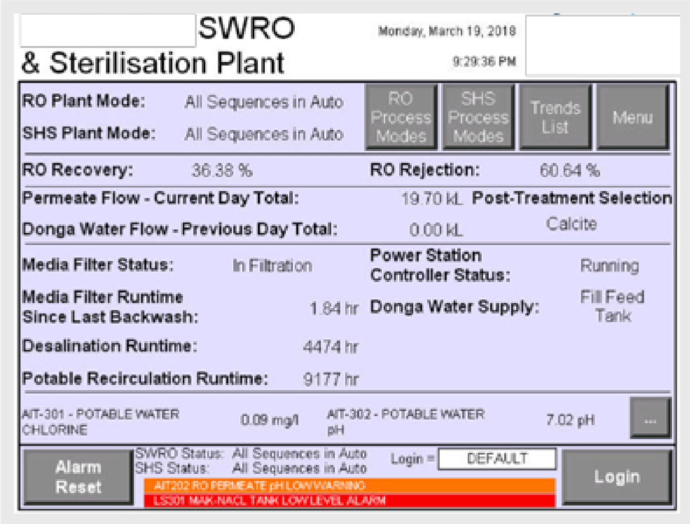
The same HMI without the user authentication pop-up window. It is unclear if the user has already authenticated, or if clicking on the menu items will bring up the user authentication window.



Water purification/disinfection plant in Canada. The page displays all subsystem status information in one screen. The HMI and/or system can likely be shut down from this screen.



System warning message displaying an alarm condition has triggered. The operator can acknowledge or further investigate the alarm from this page.



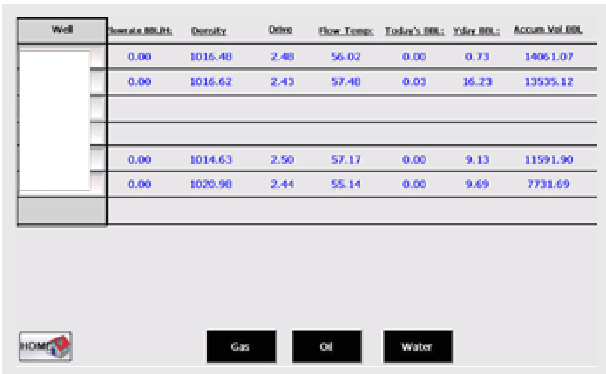
The top-level menu of a seawater reverse osmosis (SWRO) and sterilization plant in Australia. This page shows all the subsystem status information in one screen. The operator can access different submenus and the Alarm Reset menu from this page.

Figure 16. Screenshots of exposed water system HMIs

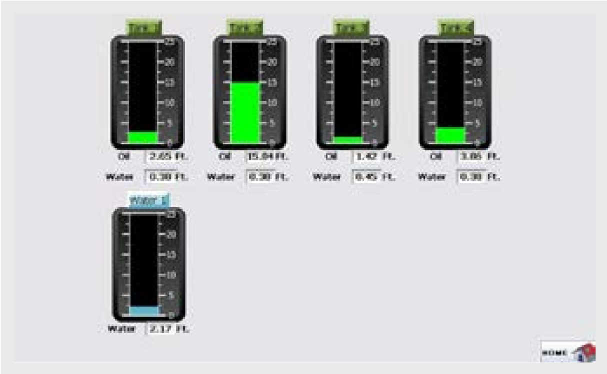
Exposed Oil and Gas HMIs

All exposed oil and gas HMIs detailed below, with one exception (a drilling rig found in the Middle East), were discovered in the U.S.

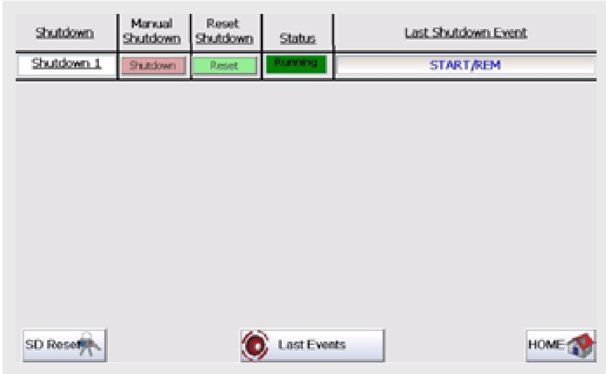
Top-level menu showing the available submenus and the name of the operator (deleted for privacy reasons).



Page displaying readings from wells currently in production.

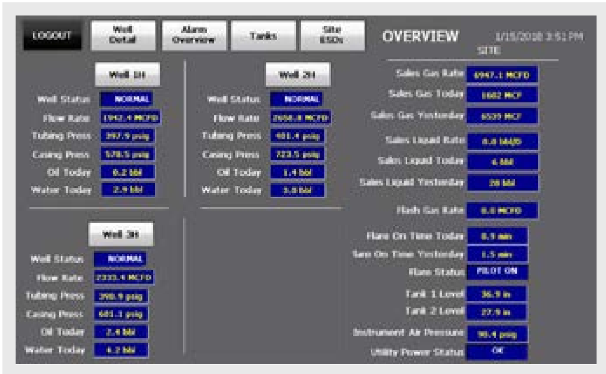


Page displaying oil and water levels in the storage tanks.

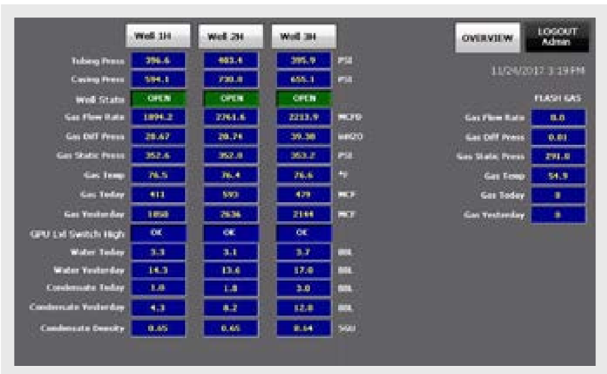


The wells can be shut down or reset from this events page.

Display of the readings from an individual well.



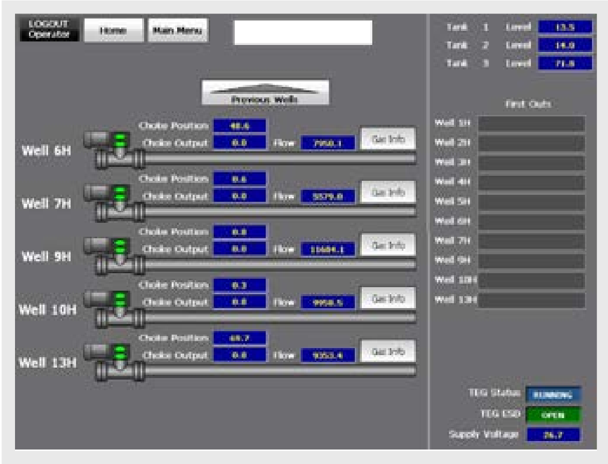
Overview page displaying readings from production wells.



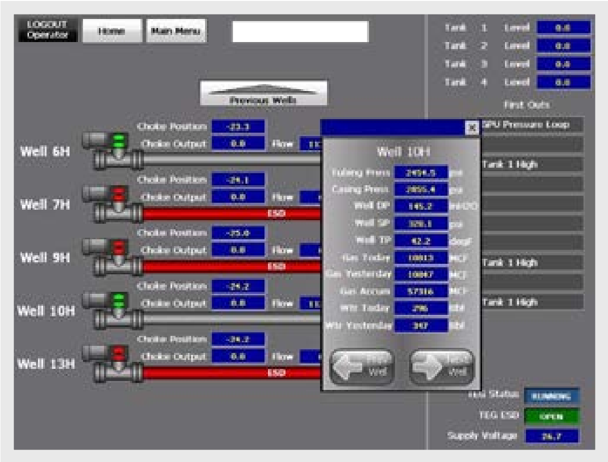
A second information page displaying well status in greater detail.

Page displaying the status of an individual well.

Page displaying oil and water levels in the storage tanks.

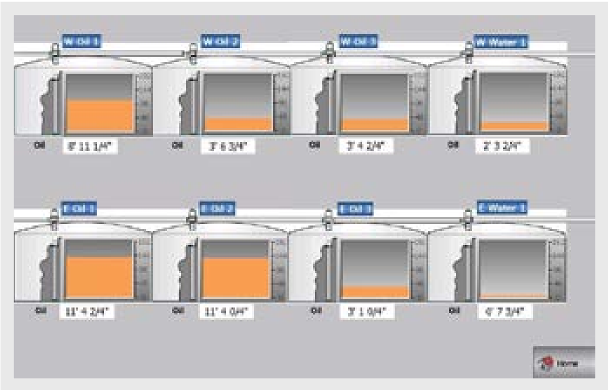


Overview page displaying readings from production wells.

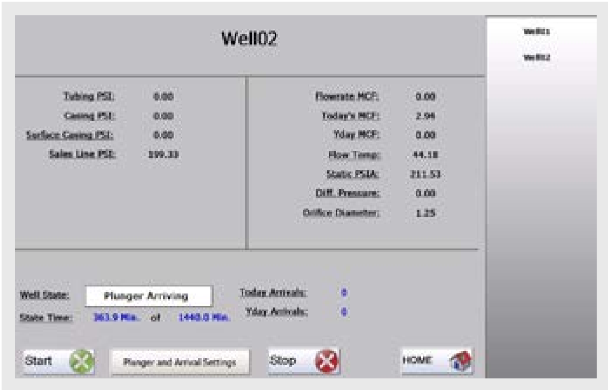


Overview page showing three out of the five wells are in Emergency Shutdown (ESD) mode. It also displays the status of an individual well in a pop-up window.

Individual well controls showing that a specific well can be either reset or “close-choked” (i.e., shut down) from this page.

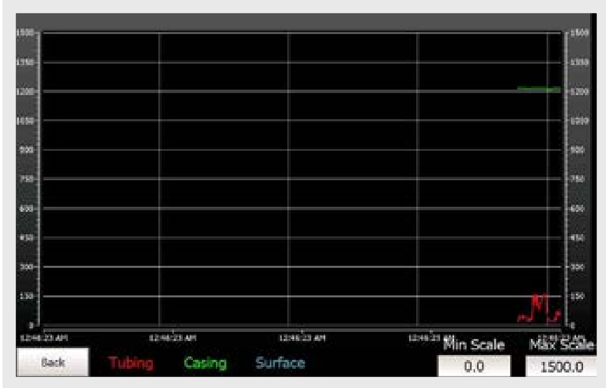


Display of storage tank oil and water levels.



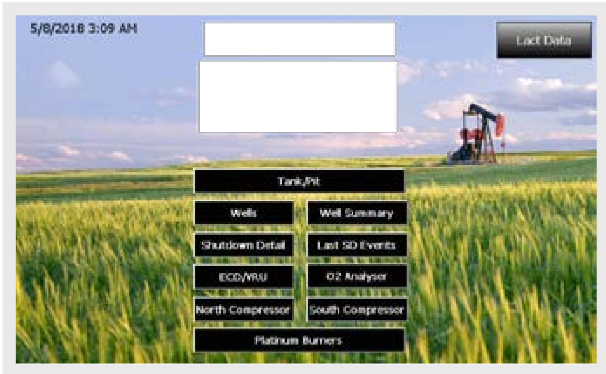
Displaying readings from a specific well. The start/stop controls and “Plunger and Arrival Settings” are accessed from this page.

A visual representation of valve pressure values.



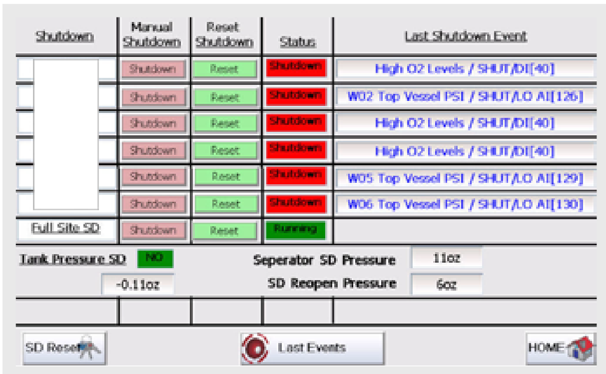
A graphical (trends) representation of valve pressure values.

Control page for the sales valve.

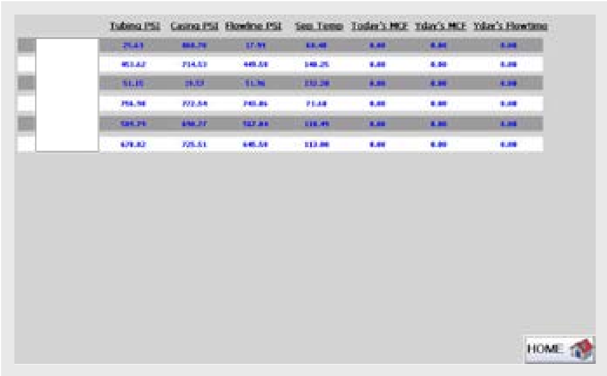


Top-level menu showing the available submenus and the name of the operator (deleted for privacy reasons).

Controls for the North Compressor.

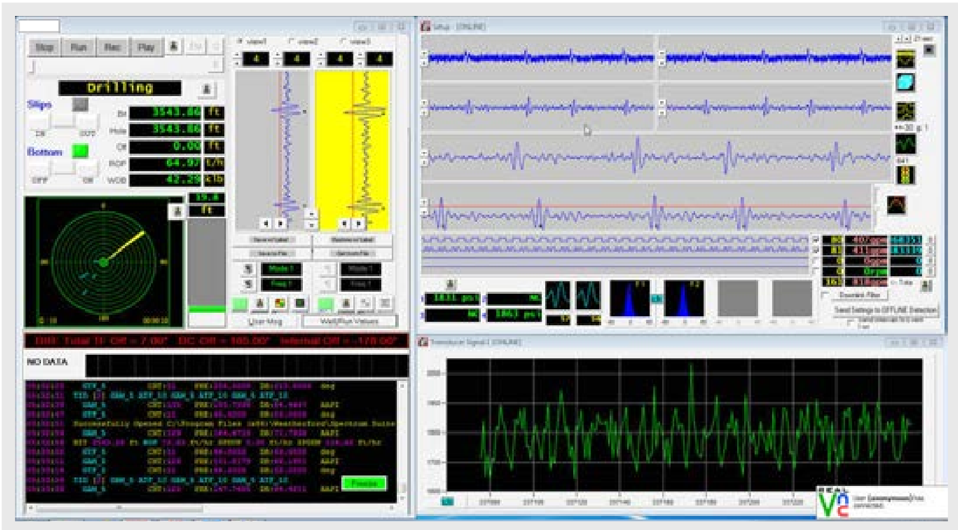


Individual wells can be shut down or reset from this events page. It also displays the current running status of the wells.



Page displaying readings from wells currently in production.

Readings from a well. The start and stop controls and plunger and arrival settings are accessed from this page.

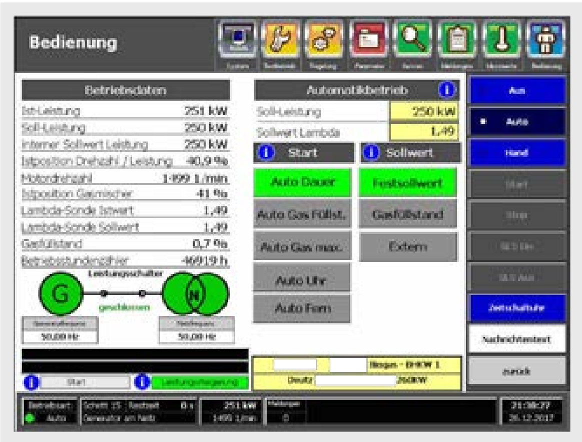


The controls for a drilling rig located in the Middle East. Drilling to depths of more than 3,500 feet strongly implies this is for an oil well. All aspects of the drill can be controlled using the application shown. In this screenshot, we observed Real VNC displaying the message “User anonymous has connected,” which in this case will be the Shodan crawler accessing the unauthenticated VNC server to capture the above screenshot.

Figure 17. Screenshots of exposed oil and gas HMIs

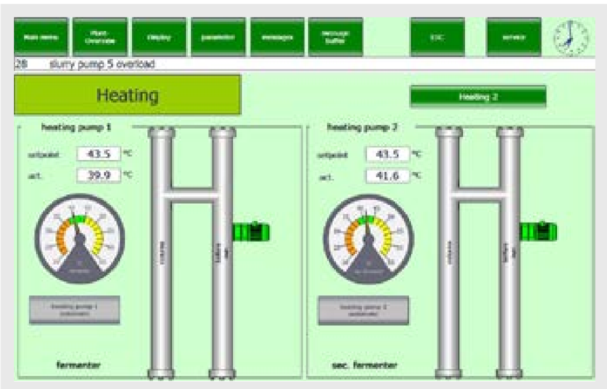
Exposed Biogas HMIs

Exposed biogas HMIs were discovered in Germany, France, Italy, and Greece, where this form of energy extraction is prevalent.



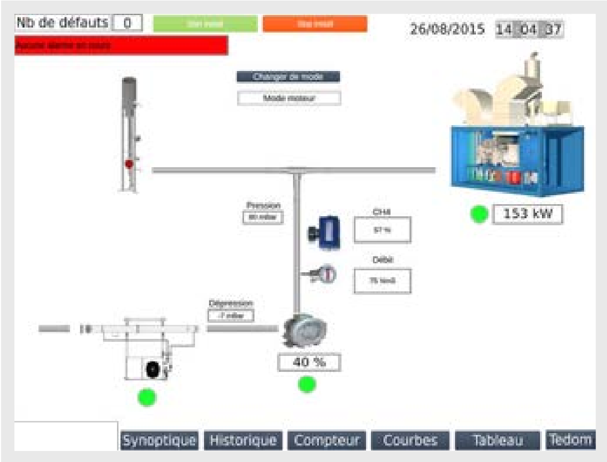
Top-level menu for a biogas facility in Germany. The main system start/stop and controls for adjusting set points, volume, timers, breakers etc.

Top-level menu displaying the available submenus, such as Slurry Pump, Mixing Tank, Fermenter, Gasanalyser, Feeding, etc.

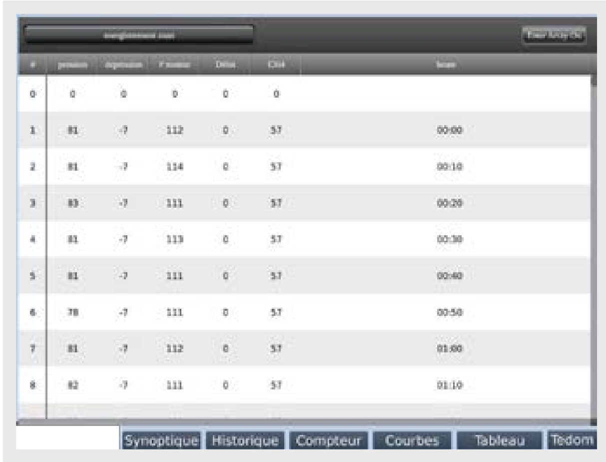


Heating controls. A “slurry pump overload” warning message is displayed at the top of the page.

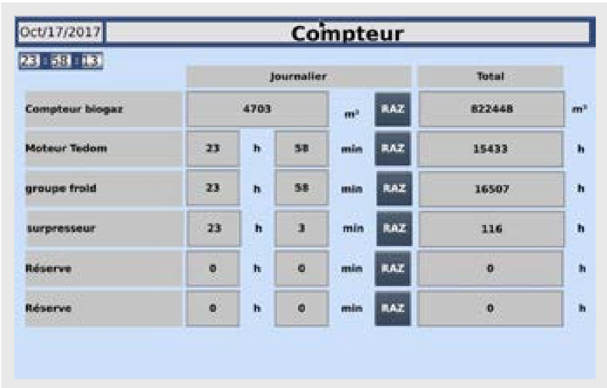
System in a German facility. The top-level menu has controls for pumps, air-gas mixers, circulation, start/stop, parameter adjustment, etc.



Top-level menu displaying the various submenus and subsystems. Start/stop controls for this plant are accessible from this page.



Overview page displaying readings from the different subsystems.



A counter menu that displays values for production volume, engine runtime, compressor runtime, etc.

Top-level menu for a biogas facility in Italy. Submenus, system reset, and alarm are all accessible from this page.

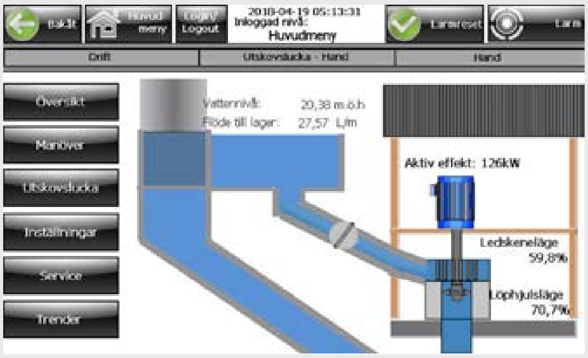
Figure 18. Screenshots of exposed biogas HMIs

Exposed Power System HMIs

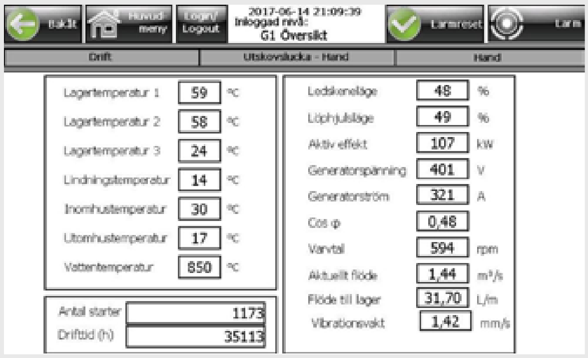
Exposed power system HMIs were discovered in Germany, Spain, Sweden, the Czech Republic, Italy, France, Austria and South Korea, and include systems from solar, wind, and hydroelectric plants. Surprisingly, no North American instances were found using our methods.

Main menu displaying energy generated by the solar cells.

System for a solar farm. The energy generated is used for agricultural processes.

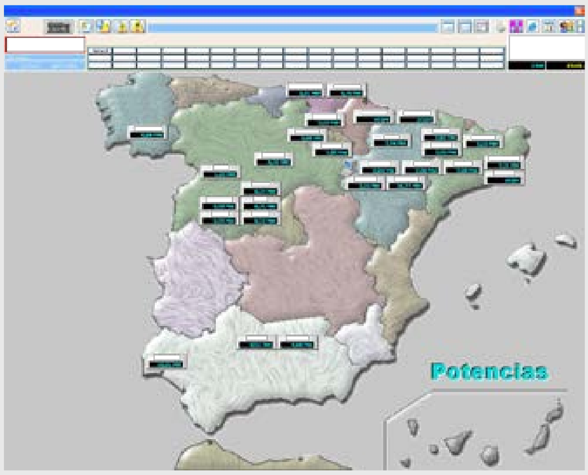


Hydroelectric plant main menu displaying the different submenus: Overview, Settings, Trend, Service, Spillover, Maneuver, etc.

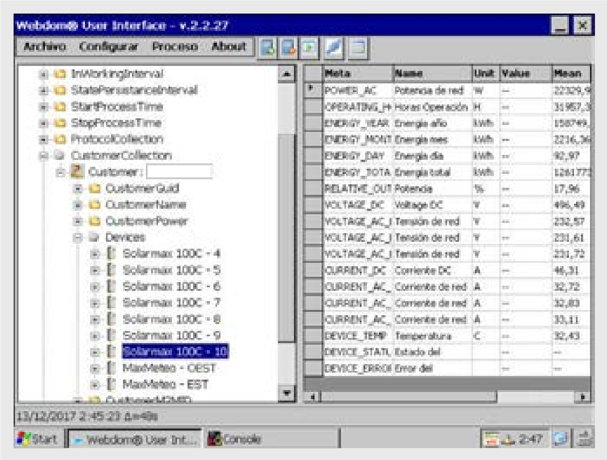


Page displaying readings for temperature, power, flow, etc.

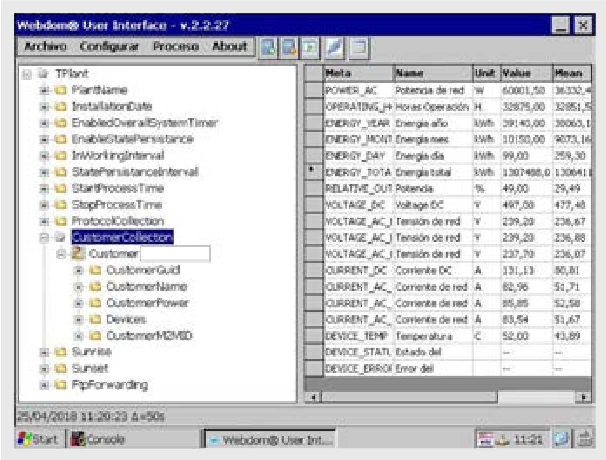
The alarms page displays messages from subsystems. These messages can be investigated, acknowledged, cleared, and/or filtered.



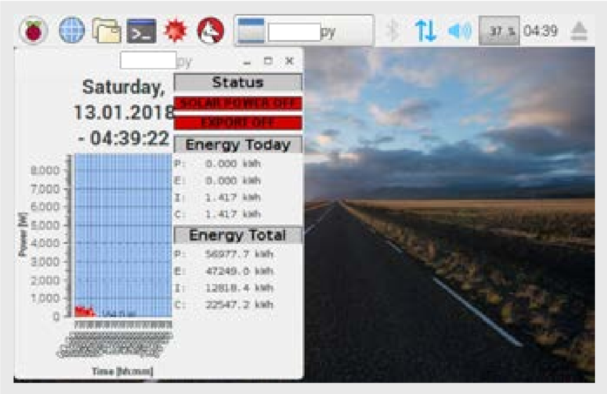
Menu displaying solar panel installations in different regions of Spain. This is possibly an operator's control screen that aggregates statuses as well as allows pushing bulk configuration changes.



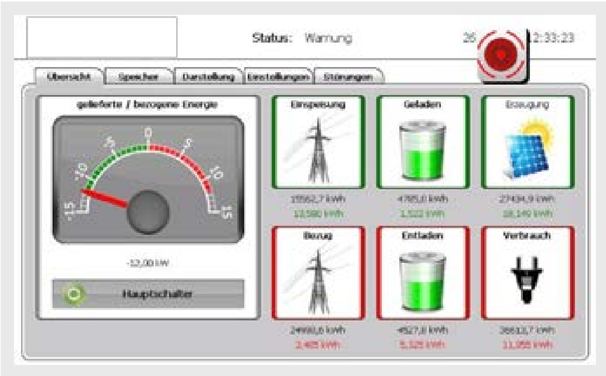
A user database exposed online. This database contains customer data: GUID, name, power, devices, etc., and is thus a big PII leak.



A user database exposed online. This database contains customer data, e.g., GUID, name, power, devices, etc., and is thus a big PII leak.

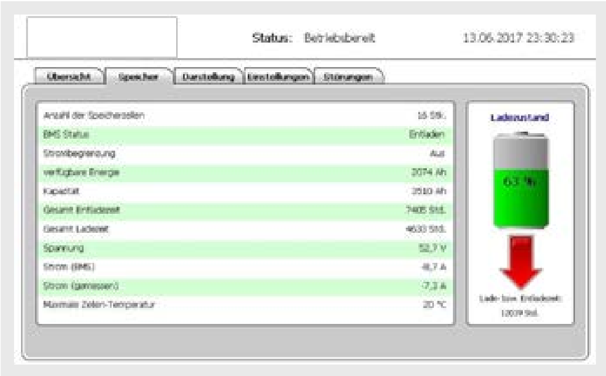


Custom solar energy monitoring script running on a Raspberry Pi. This is primarily for monitoring cell status but has no control over the cells themselves.

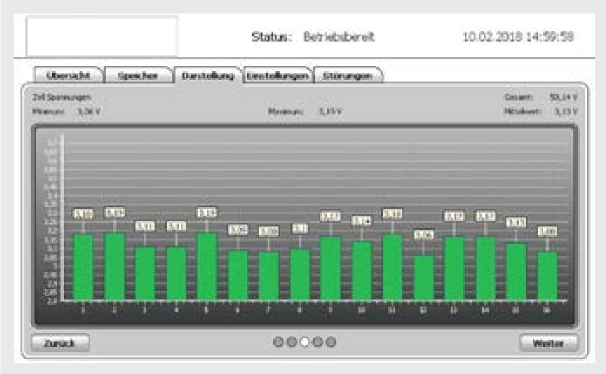


Main menu displaying values for energy consumption, solar energy generation, power storage, power resale to grid, etc.

Page showing that an alarm has been triggered, and the HMI is prompting for user authentication before menu access is granted.

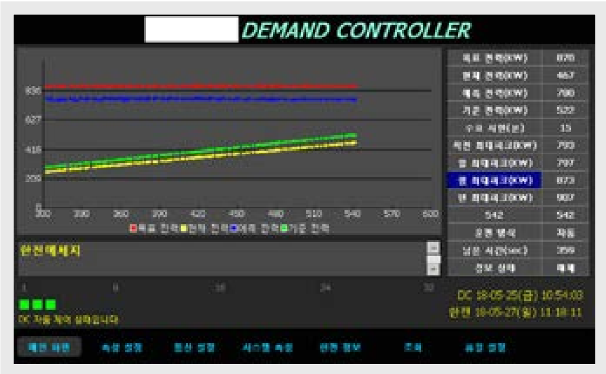


Page displaying the battery status, whether it is charging or discharging and the associated readings.



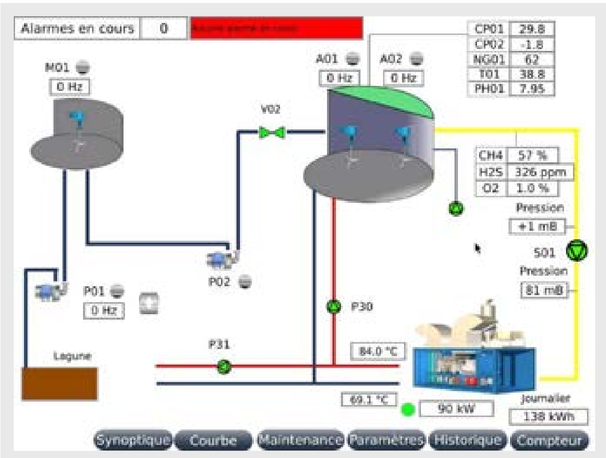
A page displaying an energy-time bar chart.

Main menu for a small hydroelectric plant in Sweden.

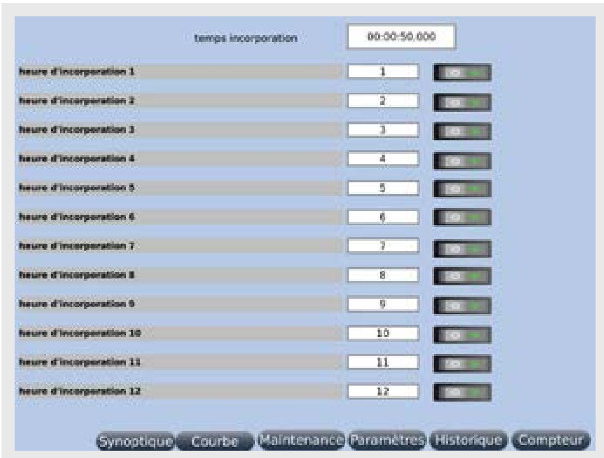


Overview page displaying power generation parameter values.

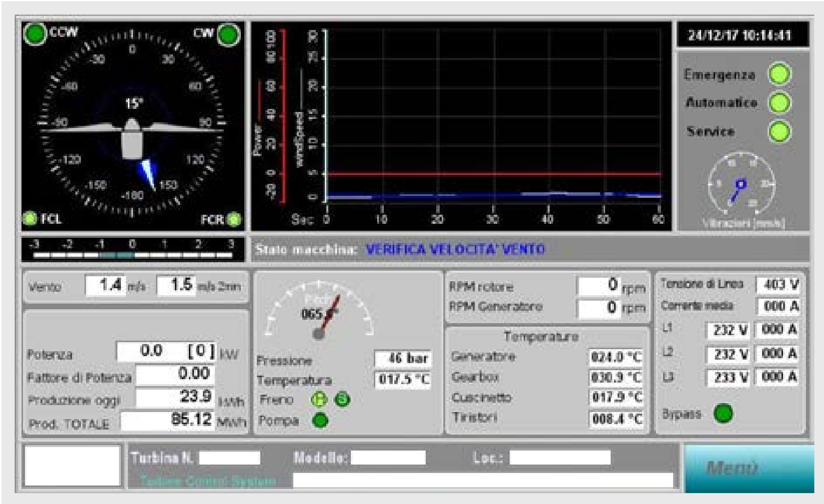
Some power generation parameters. These options are called holiday features use and power use goals.



Main menu showing the different subsystems in this hydroelectric plant. The submenus for overview, maintenance, parameters, history, etc., can be accessed from this page.



System timing control menu.



The controls for this wind turbine are located in Italy. According to additional screenshots found on the turbine manufacturer's website (name deleted for privacy), all aspects of the turbine, i.e., start, stop, reset, and system parameters, can be controlled using this software.

Figure 19. Screenshots of exposed power system HMIs

Our Observations

After studying the Shodan screenshots of exposed HMIs, we make the following observations:

- These HMIs are accessible via unauthenticated VNC servers (a remote desktop sharing tool)[32] that can be located using a public data source, in this case Shodan after paying a small subscription fee.
- A potential attacker can interact with these exposed HMIs using a VNC viewer installed on the device the attacker is using.
- After analyzing the collected screenshots, we observed that only a few of the exposed HMIs required user authentication in the HMI itself — the rest looked free to explore or interact with.
- Many of these exposed HMIs have critical functionalities like start, stop, reset, alarm, parameter changes, etc., which are easily accessible to anyone. If attackers gain access to these exposed HMIs, then they can inflict serious system damage or cause failures.
- Changing screenshots mean the systems are live and are used regularly, which is how Shodan captured different pages. The operators failed to notice and subsequently disable the unauthenticated VNC servers even after the Shodan crawler made repeated visits.

In the next section, we will explore the potential real-world impact of compromising and abusing exposed water and energy systems.

5. Theorizing Real-World Threats

For this research, we collected a diverse range of exposed HMI screenshots using Shodan and Shodan IP histories. The goal for collecting these screenshots was threefold:

1. To prove that HMIs are exposed on the internet and can be easily discovered using public data sources.
2. To demonstrate that all manners of critical infrastructure controllers, e.g., for oil/gas wells, hydroelectric plants, solar farms, water purification plants, are exposed online.
3. To theorize, using the exposed HMIs that we discovered, real-world cyberattacks that corporations need to protect their facilities against and show that these services are not simply exposed but a real risk to the organizations and those who rely on them.

From a small survey we conducted on selected organizations, we found that their primary concern from any attack was always disruption of supply either to or from their facilities.

I. Attacks Against Water Treatment Plants

From our screenshots collection, we selected two HMIs used to control/configure water treatment plants. These controls are highlighted by red ovals in the screenshots.

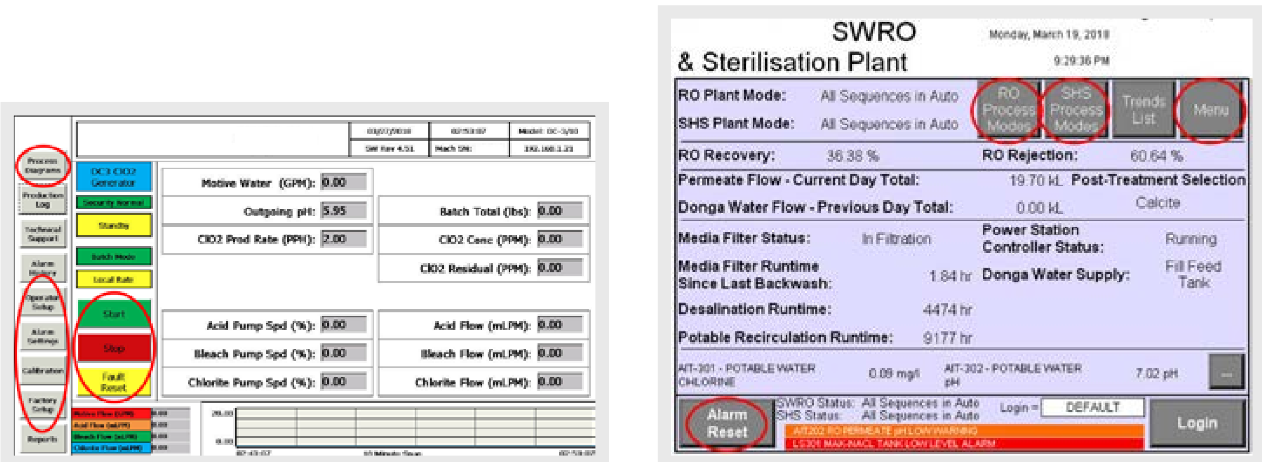


Figure 20. Screenshots of two exposed HMIs for controlling/configuring water treatment plants

The process of sterilizing seawater is one of the important sources of drinking water. The exposed HMIs that we discovered are the main controllers for a water purification plant and a seawater reverse osmosis (SWRO) plant, i.e., seawater to drinking water conversion. A cyberattack against water treatment facilities will adversely affect the drinking water in that region, leading to supply shortages. Impure water will also help spread waterborne diseases, leading to a public health crisis. In Section 2 we already discussed how a similar real-world attack was disclosed by Verizon in 2016.[16]

II. Attacks Against Industrial Water Facilities

We selected two HMIs used to control/configure an industrial water heating facility. These controls are highlighted by red ovals in the screenshots.

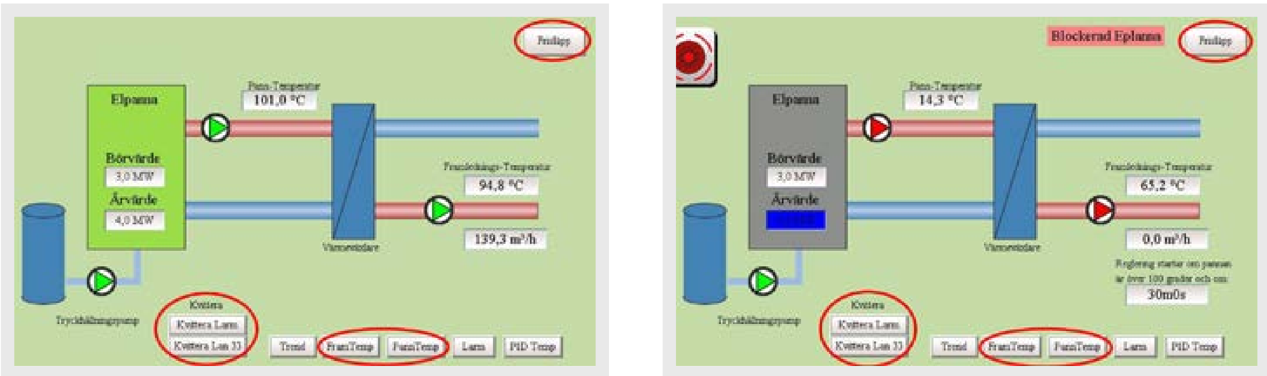


Figure 21. Screenshots of two exposed HMIs for controlling/configuring industrial water heating

As well as being critical to life, water is a critical component of many industrial processes. Water is used for heating, cooling, cleaning, energy transfer via steam, chemicals manufacturing, etc. In our example HMI, large volumes of water are heated and used for some industrial process. Temperature readings of 101 °C suggests the water is converted into steam and then used to either transfer energy or drive certain machines, for example, turbines. A cyberattack against this facility can cause a serious industrial accident if the water is heated to an incorrect temperature, or if the boiler is deliberately overloaded. The second HMI screen shows a boiler malfunction, where the water is not being converted into steam, resulting in production disruption at this facility.

III. Attacks Against Oil and Gas

In this example, we have selected four HMIs that are used to control or configure oil and gas wells.

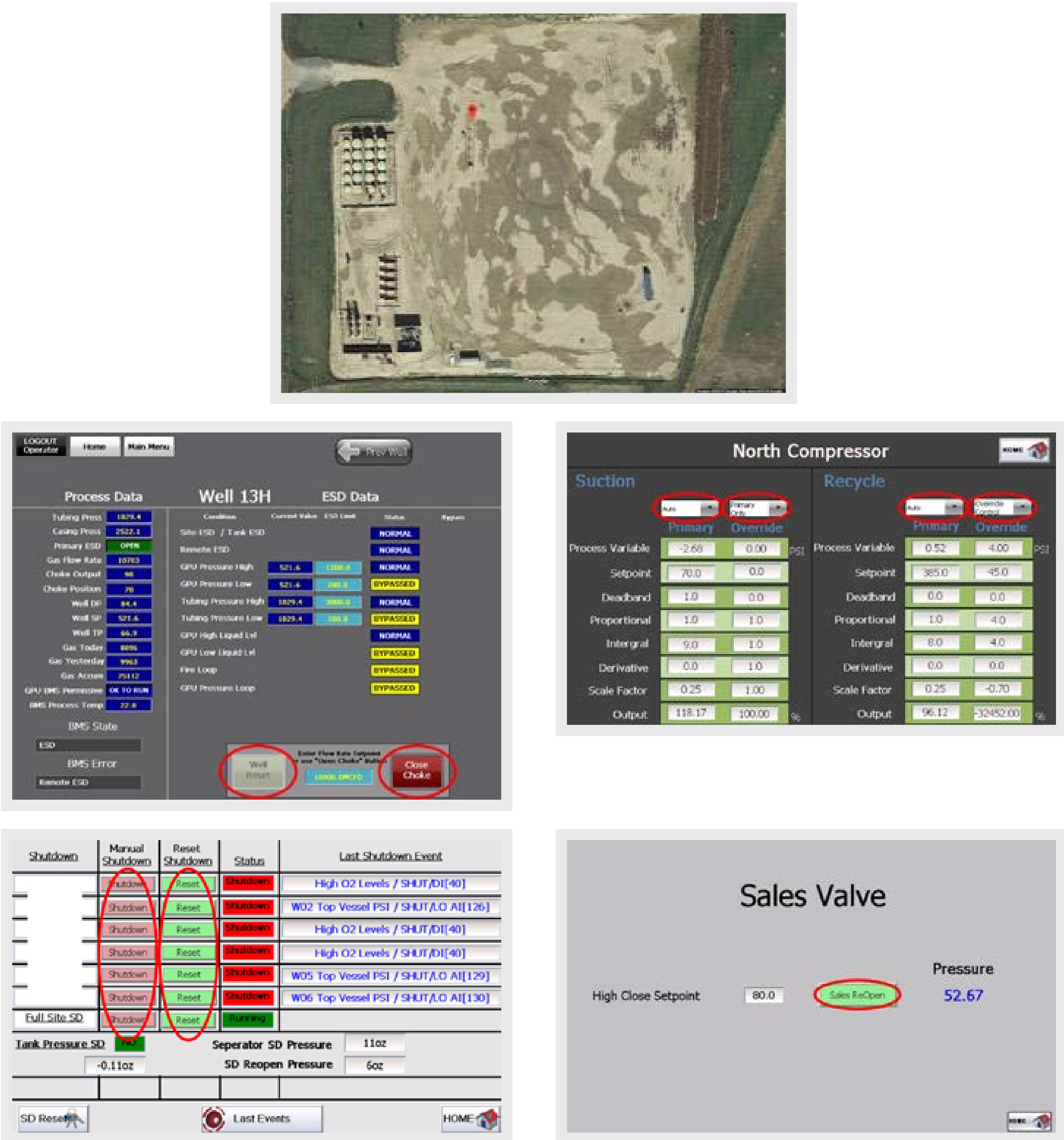


Figure 22. Screenshots of exposed HMIs for controlling/configuring oil and gas wells

Except for a drilling rig found in the Middle East, all of the exposed oil and gas HMIs that we discovered during our research were located in the U.S. Using well identification data (deleted for privacy reasons) and publicly available well information, we were able to locate many of these wells on Google Maps.

Our Google Maps visual investigation showed these wells were being used in one of two ways: 1) the extracted resources were diverted to large collection sites and then transported via major pipelines; 2) the extracted resources were collected and sent to local power plants. The exposed HMI controllers that we found allow an operator to shut down or reset the wells, configure well parameters, and control sales valves. A cyberattack against these well sites can lead to unforeseen failures and shutdowns that could consequently cascade effects further down the supply chain. It can mean heavy losses for the organization involved considering that one pump failure alone can cost up to US$100,000 to US$300,000 per day.[33] On a broader scale, such attacks can cause further consequences by choking local power plants and affecting state or national energy supplies.

IV. Attacks Against Solar Energy

From our screenshots collection, we selected four HMIs that are used to control or configure roof-mounted solar panels and manage solar farms.

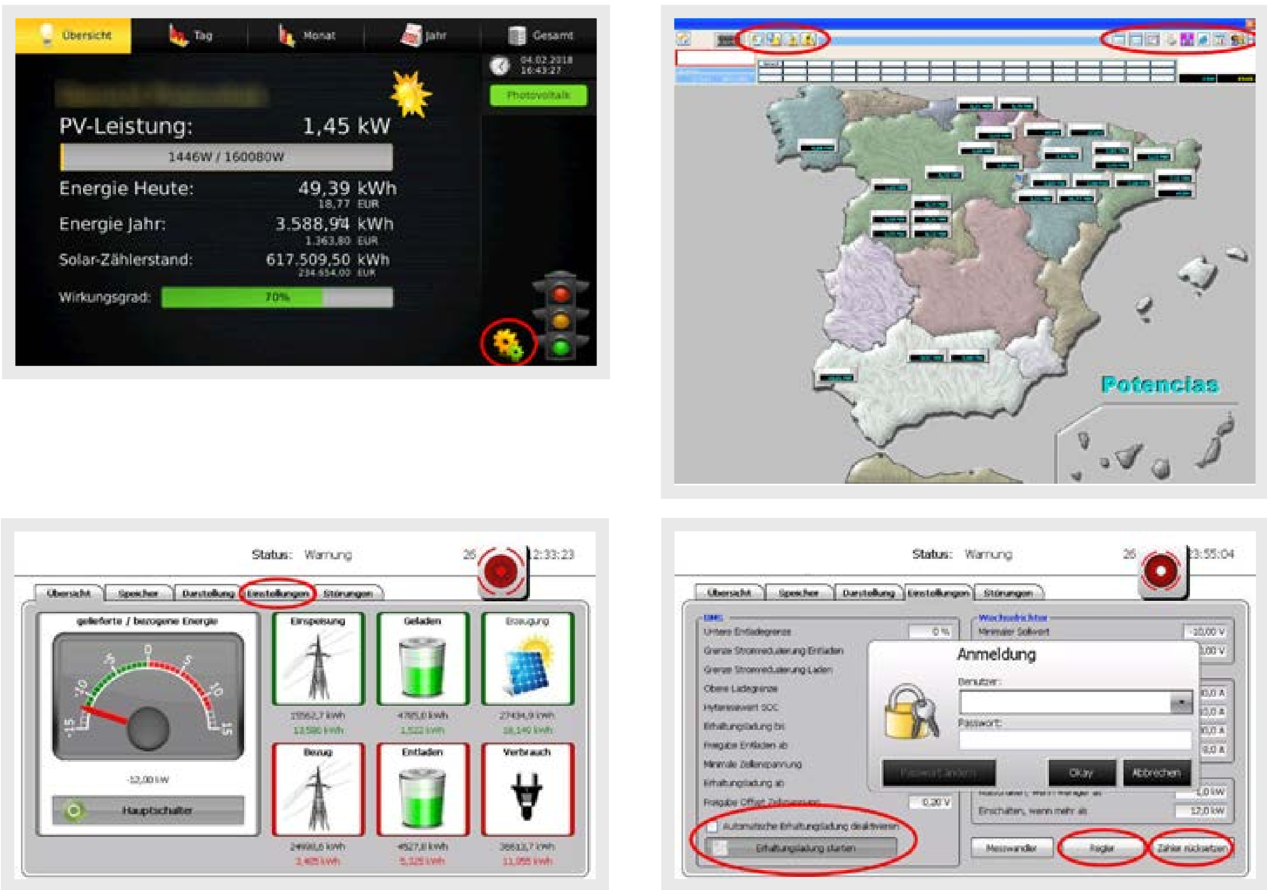
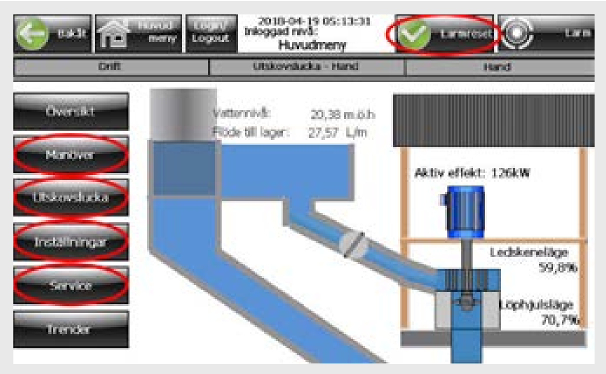


Figure 23. Screenshots of exposed HMIs for controlling/configuring solar-related devices/systems

Roof-mounted solar panels are common in Europe, especially in Germany. The roof-mounted solar panels provide supplementary power to the homes and surplus energy is sold to the national grid. European countries extensively use solar farms to generate electricity for the national grid because solar is a clean energy source. We found three exposed HMIs for controlling roof-mounted home solar panels and one exposed HMI for managing nationally distributed solar farms. A cyberattack against these systems can affect the total available power in the national grid, cause blackouts at homes, and directly affect the revenue of homeowners.

V. Attacks Against Power Plants

For power plants, we selected two HMIs used for control and configuration.



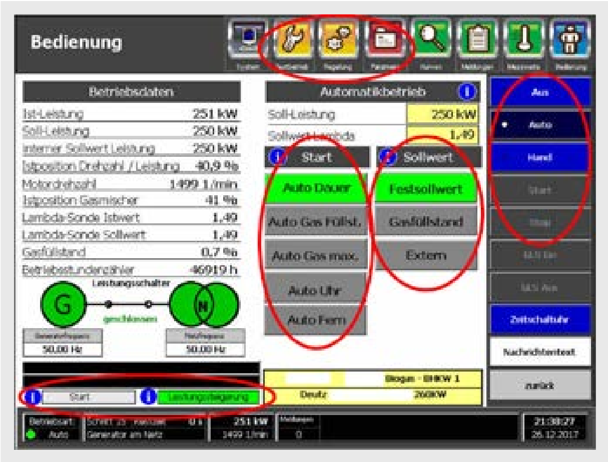


Figure 24. Screenshots of two exposed HMIs for control/configuration in power plants

During our research, we found different types of power plants exposed online, e.g., biogas, hydro, solar, wind, etc. Using data embedded in the exposed HMI screenshots, we were able to locate the actual power plant in Google Maps as demonstrated in the map screenshot in multiple cases. Many of these exposed HMIs have control elements, e.g., Start, Stop, Reset, Settings, Service, etc., freely accessible via the web. A cyberattacker can inflict serious damage to these power plants and, in the process, affect the electricity supply for the region in which the power plant is located. A power supply disruption will affect homes and industries alike, and in rare cases might cause interruptions in the national grid.

VI. Attacks Against Hydroelectric Plants

Some of the exposed systems don't tie directly to an HMI that tells you what the system might be. Instead, there are some cases where there are web cameras monitoring the facility, with specific ICS ports open that then control the devices displayed in the webcam. During the course of our research, we found a system exposed via Shodan based on its webcam information.

Figure 25. Exposed web camera showing a hydro facility

A closer look at the host inside of Shodan showed several web server pages open as well as two control system ports. The two that were open indicated that there is an Omron control system behind the industrial router. The services that were running included a File Transfer Protocol (FTP) server, web services (that turned out to be the industrial router configuration page), four web cameras, a default Internet Information Services (IIS) configuration page, and two ports for the Omron devices. TCP/9600 is used by the Factory Interface Network Service (FINS) protocol by Omron; TCP/44818 is commonly used to also configure the Omron devices.

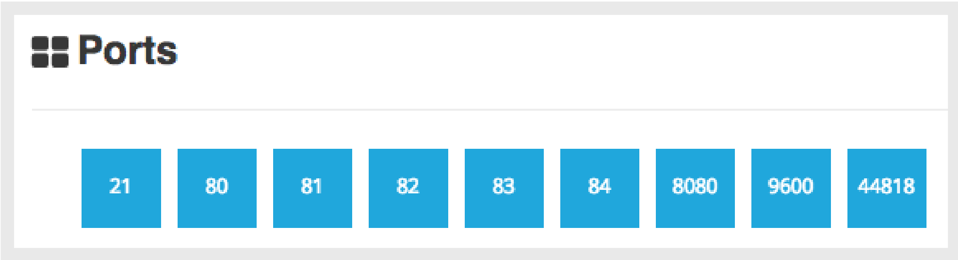


Figure 26. Ports listed open in Shodan

Looking at the exposed cameras on the device, we surmised that it is related to a hydro facility. Based on the information that we collected, we can say that the power plant is located in Italy.

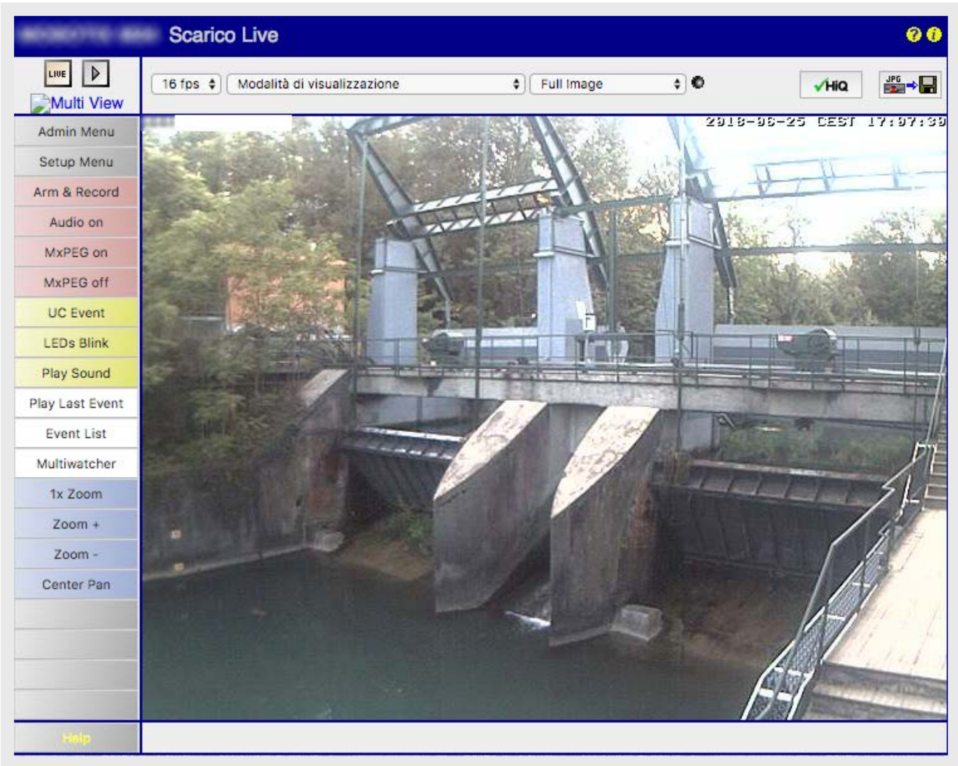


Figure 27. View of the spill gates of the hydro facility

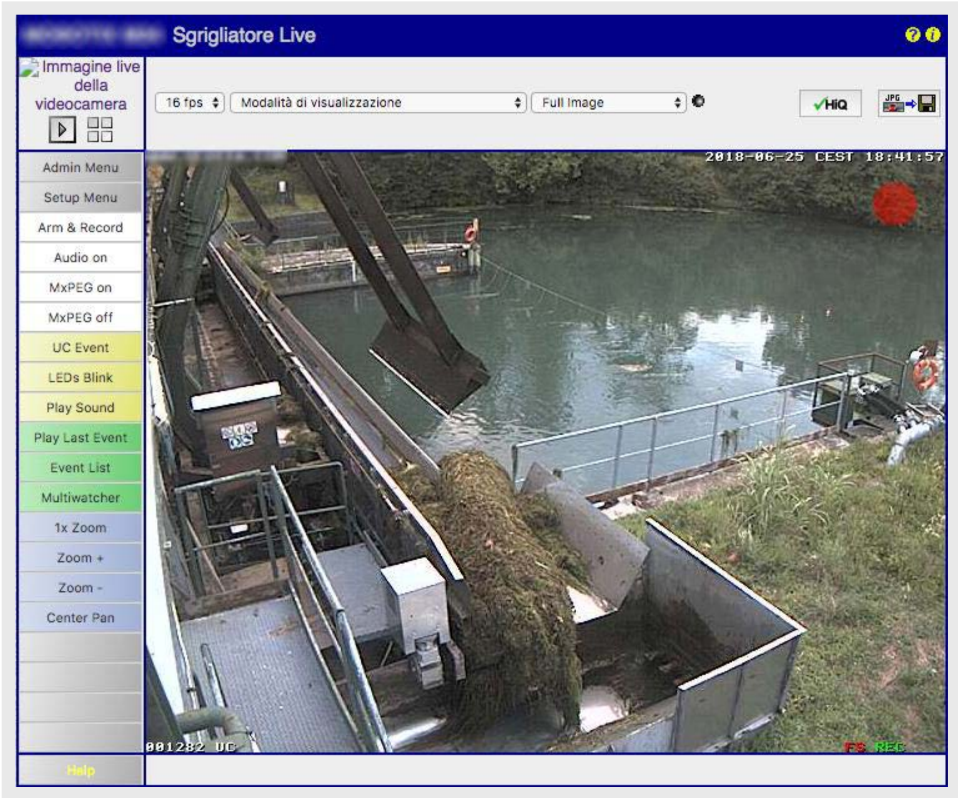


Figure 28. View of inlet into the two units visible in Shodan (Raker Live, if translated from Italian)

The two ports that were open were related to control systems; TCP 9600 and TCP 44818 are two popular control system protocols, Omron FINS protocol and Ethernet/IP. Omron FINS usually communicates over UDP. Shodan indexes both FINS and Ethernet/IP protocols. FINS was added in Shodan in 2015[34] and is one of the numerous ICS protocols supported by the Shodan banner-grabbing system. In most cases, FINS is parsed for an appropriate response. However, in this case it was not, so that prompted us to look into whether the device was an Omron device or not based on the responses from the protocol.

While most of the documentation on the protocol is for its UDP version, this is also included in the TCP version of the protocol, with additional headers and negotiations of a destination address.

For safety and ethical reasons, we did not probe the device ports.

If the host we found is an actual hydro facility with the above-mentioned two ports open, there would be a significant risk to the devices and any operations that may be happening at the time. If this device is truly as it appears, the attacker could watch any action performed against the controlling devices that are exposed via the exposed cameras. This could include the controls of rakes, spill gates, electricity generation or all of the functions depending on the configurations of the controllers.

Discussion on Exposed HMIs

While the number of exposed water and energy HMIs that we discovered was relatively small, it is still a cause for concern because these systems should not be exposed online in the first place. One of the things we observed was that none of the exposed HMIs were owned/operated by any of the well-known big corporations; instead, they were owned/operated by smaller companies. It is important to remember, however, that smaller companies affect the overall security of the larger companies they are connected to. Smaller companies are frequently part of the supply chain that feeds resources to the big corporations; thus, a cyberattack against a small company will indirectly affect the big corporations. Consider the case of an independently owned gas well selling extracted natural gas to a local large power plant. A system failure at the independent gas well because of a targeted cyberattack will cause a drop in gas supply, which could then lead to a reduction in total power generation and ultimately affect the larger plant and everyone who relies on its services. Supply chain dependency means it is critical to protect both big and smaller players — the supply chain is only as robust as its weakest link.

In addition, while it appears that bigger corporations are less likely to have their devices exposed directly on the internet compared to smaller operations, perhaps by being behind a VPN, the risk of attack is still most certainly there. If an attacker does succeed in compromising the main network of a target via a more traditional targeted attack method such as spear phishing, lateral movement will give the attacker access to devices very similar to those in smaller operations already exposed online. The only difference is that these similar devices are protected by a VPN. Unfortunately, by then, it is a VPN the attacker is already connected to.

Because of such sharing of devices between smaller and larger organizations, smaller operations that are directly exposed to the internet can also be leveraged by attackers as a training ground for their real attacks. In case they are detected, or have damaged the equipment, the overall effects to their campaign is much less than if such mistakes occurred on the real and larger target networks.

Other Cyberattacks

Abuse of exposed HMIs is only one of the daily cyberattacks faced by internet-connected ICS devices. Other major risks include the following:

- ***A distributed denial-of-service (DDoS)*** attack is a form of denial of service that involves disrupting a network through a launched attack from multiple individual locations.[35] IoT search engines like Shodan.io and Censys.io have made it possible to easily search for and discover exposed ICS devices. Using botnets, cybercriminals can flood these exposed ICS devices with superfluous network traffic, overloading the devices and knocking them offline. An ICS device knocked offline by a DDoS attack may result in some critical process prematurely halting, or the process could continue to run in an uncontrolled manner, causing serious material damage.

- ***Vulnerability exploitation*** is the deliberate exploitation of known weaknesses in a software program in order to compromise the system; the end goal is almost always malicious.[36] ICS devices have plenty of publicly undisclosed vulnerabilities that an attacker can exploit in order to compromise the system. As of writing, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) website listed 923 advisories and 124 Alerts.[37] ICS vulnerabilities are difficult to patch because of various reasons, including the following: devices are physically located in remote geographical locations; devices are controlling critical processes that don't allow for downtime; the operator's mindset could be,"If it isn't broken, then don't fix it."

- ***Lateral movement*** in a cyberattack typically involves activities related to credential theft, reconnaissance, and infiltration of other computers to target more critical devices or systems.[38] Attackers compromise a machine inside an organization's network, in this case an exposed ICS controller. Using the compromised machine as a beachhead, they attempt to gain access and spread to other networked computers — including the core business network. In this way, an exposed ICS device could be the cause of a compromise to some backend database server, for example, as has happened in real-world cases in the past. Lateral movement also uses the victim's own resources against the victim, for example, the attacker will use legitimate Windows features and tools used by IT administrators to move around the network. Lateral movement normally happens at human speed and takes time to succeed. Stealth is an important factor in lateral movement. The goal is to remain undetected and deeply penetrate the victim's network.

6. The Cybercrime Underground Targeting the Water and Energy Industries

One of the most challenging tasks in cybercrime investigation is attribution. While it is very difficult to pinpoint exactly who the guilty party is, it is far easier to categorize attackers and their motives — and we include some of the main ones below. The risk of each of these targeting a particular water- or energy-related organization will vary greatly depending on the organization, what it specializes in, and the political climate, among others. Nevertheless, the list below includes the general categories any such organization should factor into its threat models.

- **Nation-states** are the first attackers that come to mind when thinking about CI attacks such as on the energy and water industries. In fact, many of the attacks detailed in Section 2 are thought to have originated from this category. An organization's risk exposure to such an attack will be influenced as much by the current political climate as what the organization does.

- **Organized criminal syndicate** intrusions can be split into two categories. The first are gangs who steal and sell sensitive data, encrypt documents and demand ransom, compromise machines to run botnets or cryptominers, etc. The second are gangs who have been contracted by governments to conduct cyberespionage campaigns or to carry out politically motivated disruptive or destructive cyberattacks. From a protection point of view, the second category can be treated much like nation-states; we will talk more about the more financially motivated attackers later in this section.

- **Cyberterrorists** are another group that will frequently be thought of as a risk to CI organizations, as they aim to launch potentially disruptive or destructive cyberattacks against power plants, transportation networks, industrial manufacturing facilities, natural resource sector companies, etc. Their goal is to cause physical destruction of property, potential loss of life, and the spread of fear. Again, the risk here to an organization will be heavily influenced by politics and ideology in the countries where they operate.

- **Competitors** spying on each other go back to the origins of trade. Competitors may be looking for information such as intellectual property, production data, pricing information, customer information, etc. In extreme cases, competitors might launch disruptive or destructive cyberattacks against their competition in order to gain a stronger foothold in the market. Later in this section, we detail several examples of such competitive espionage discussed in criminal undergrounds.
- **Hacktivists** are internet activists. They attack cyberassets in order to draw attention to their causes and frequently choose high-visibility/high-profile targets. Their targets and their causes are often not synonymous. Large corporations are frequent targets of hacktivists who are protesting causes such as environmental damage, corporate greed, etc. We do not cover hacktivism in detail in this research, but Trend Micro has released a very detailed paper on the subject earlier this year.[39]
- **Script kiddies and random hackers** represent the vast majority of threat actors targeting exposed cyberassets in our experience. These are people who scan the internet to discover exposed IoT or industrial IoT (IIoT) devices, either out of curiosity or to cause mischief. They may end up watching "the view" through an open webcam, stealing information, changing settings on connected devices, blackmailing victims, etc. We detail several examples of this later in this section.

The Underground Scene

Within the cybercrime underground itself, discussions of attacks for energy and water industries seem to be lower than expected given the criticality of such systems. Today's modern underground is mostly focused on monetization and the "required qualification and efforts to possible outcome" ratio for attacks on the energy and water industries does not look competitive compared to low-hanging fruits in other industries. Energy and water industries are of course subject to the same mass malware attacks as other industries and can fall victim even to threat actors who are less inclined to perform targeted attacks like script kiddies, due to the importance of the systems they support.

Due to this poorer return on investment (ROI) compared to more traditional attacks, and given that ICS attacks do not have the same financial scalability as more widespread attacks, these sectors seem to have two *polar groups of interest*. On one side, there are the sophisticated groups related to industrial espionage or state-sponsored actors (discussed in Section 2). On the other, there are the more opportunistic or curious attackers who have learned of such exposed ICS/SCADA equipment through services like Shodan, Censys and others. These two groups represent the main attack groups, but there are also a number of other less common groups focused on specific topics. Those we will also outline below.

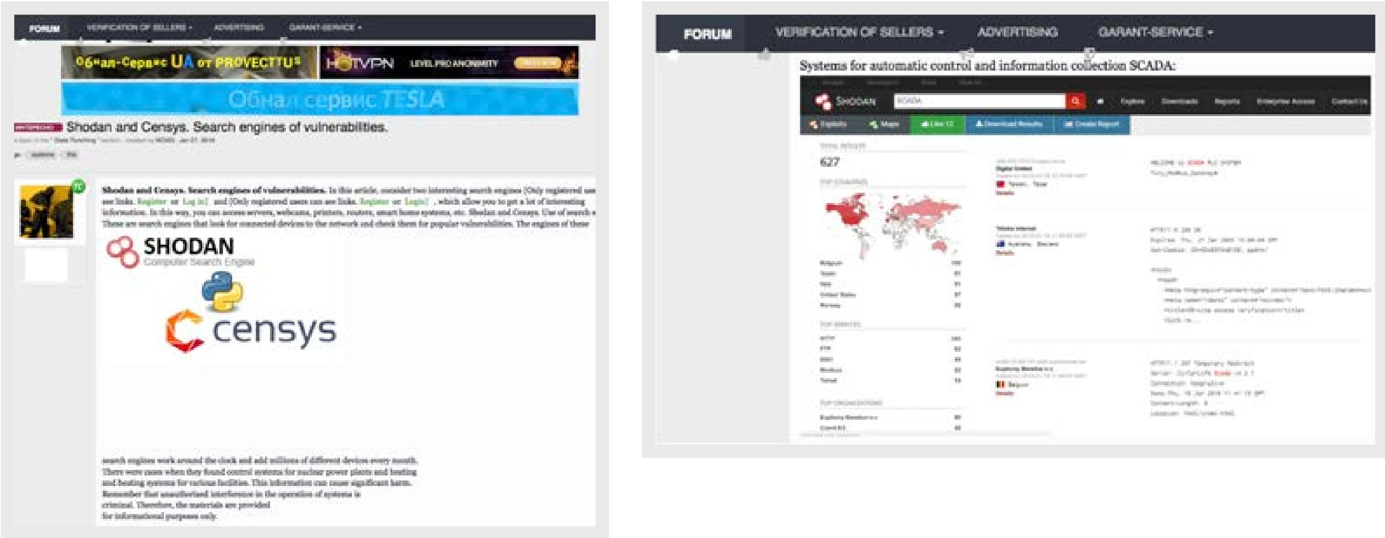
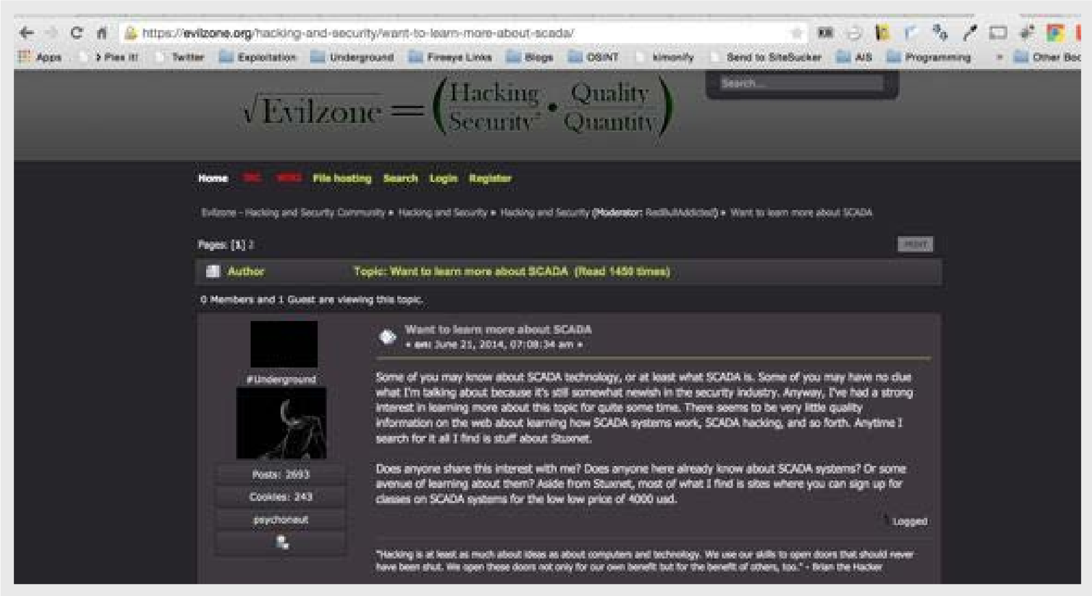


Figure 29. Forum discussion about vulnerable device search engines with SCADA examples

Discussions on underground forums about the industry can be categorized into several groups:

- Discussions about Shodan or Censys findings, particularly in the context of exposed industrial equipment being among the more lucrative IoT devices to exploit, like home routers[40] or exposed cameras.[41]
- Discussions from people who would like to learn about SCADA security and don't want to pay high prices for more professional training.



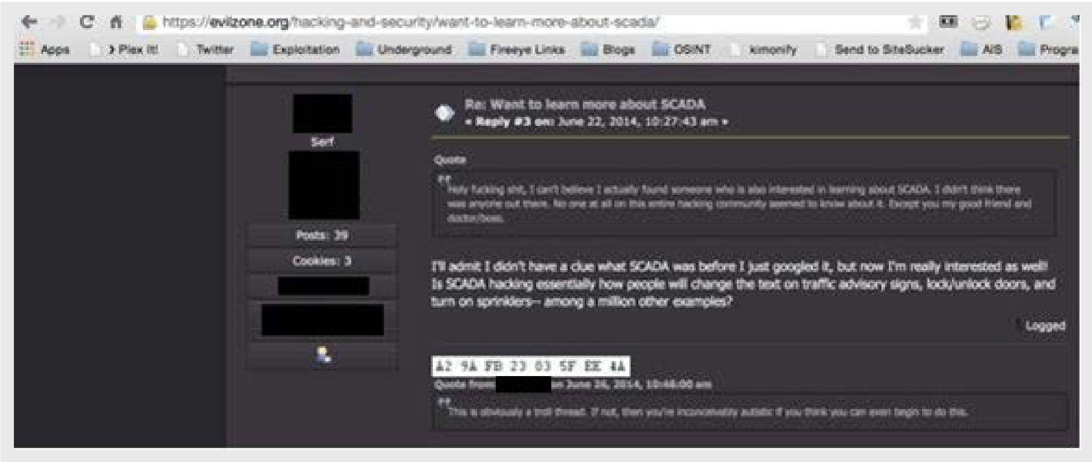


Figure 30. Translated screenshot of actors who are sharing knowledge or want to learn about ICS/SCADA systems

- Discussions from opportunistic attackers or the group of potential buyers of information or access to exposed infrastructure, which would include credentials for ICS/SCADA systems. These buyers may have different backgrounds, which are further listed below.
    - Potential targeted attack actors looking for an easy initial point of entry for exposed systems on target networks. They join discussions during the reconnaissance phase of their attack to explore less time-consuming methods, while being very careful of their operations security (OPSEC).

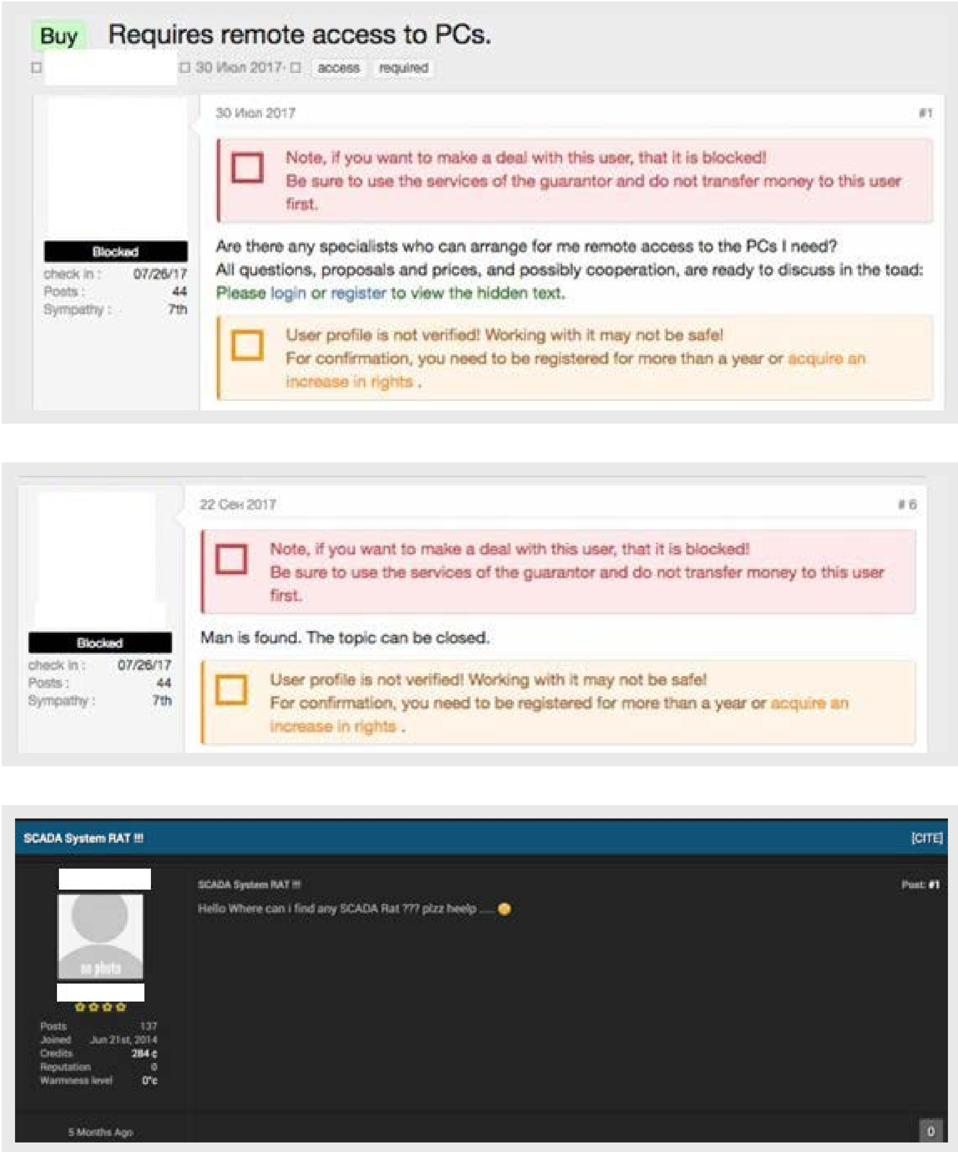


Figure 31. Request for help accessing particular hosts to buy a SCADA RAT on underground forums

- Employees of companies in this industry trying to get information for personal enrichment or career growth through illicit means like blackmail. We have discussed such cases in our recent study on digital extortion.[42]

- Requests related to possible attacks on a competitor. The aim of the buyer could be to gain an advantage in business, to disrupt the competitor or business process compromise (BPC).

Figure 32. Request for shareholder databases of several oil companies

- Opportunistic sellers or sellers who had success with hacking an industry target, but now don't know what to do with the information they have collected, for example an oil company employee database or exposed equipment.

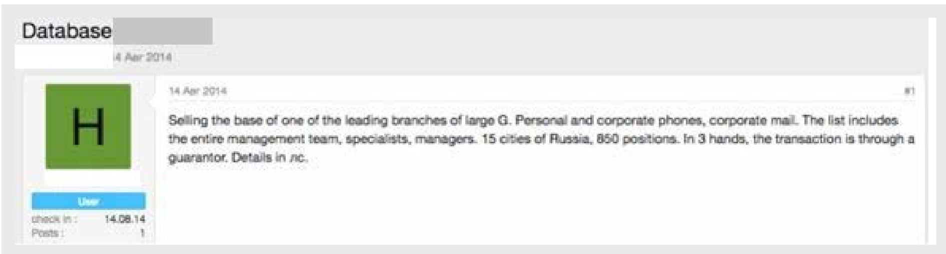


Figure 33. Post selling an employee database of an oil company

- Requests for information and discussions on new vulnerabilities and exploits for ICS/SCADA equipment.

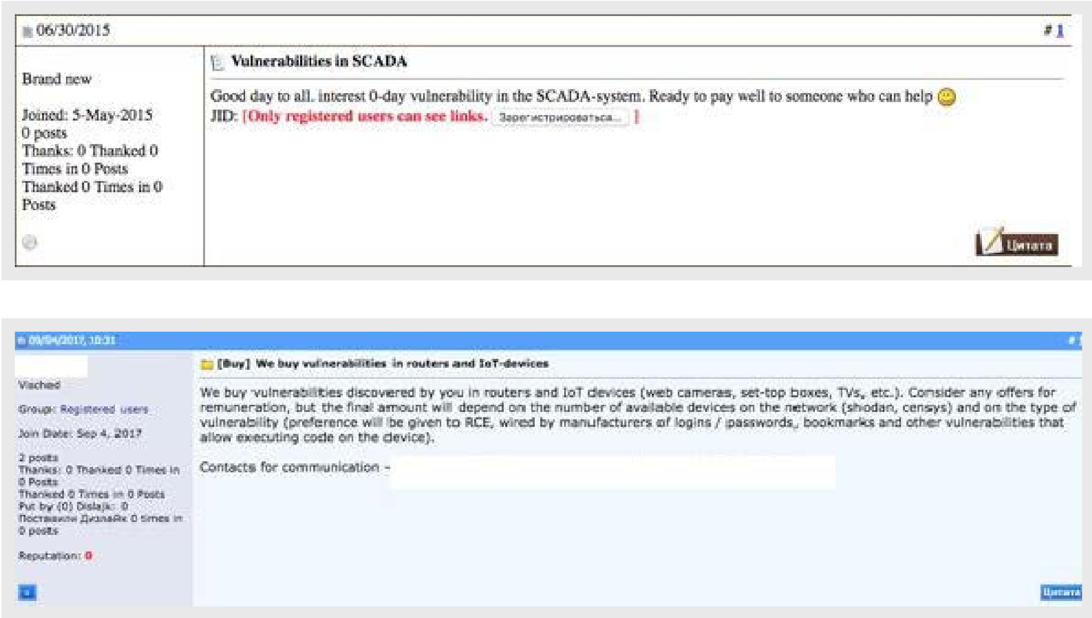


Figure 34. Discussions on SCADA vulnerabilities

- Reposts of bug bounty competitions from industry vendors who are willing to test their equipment security in the wild.

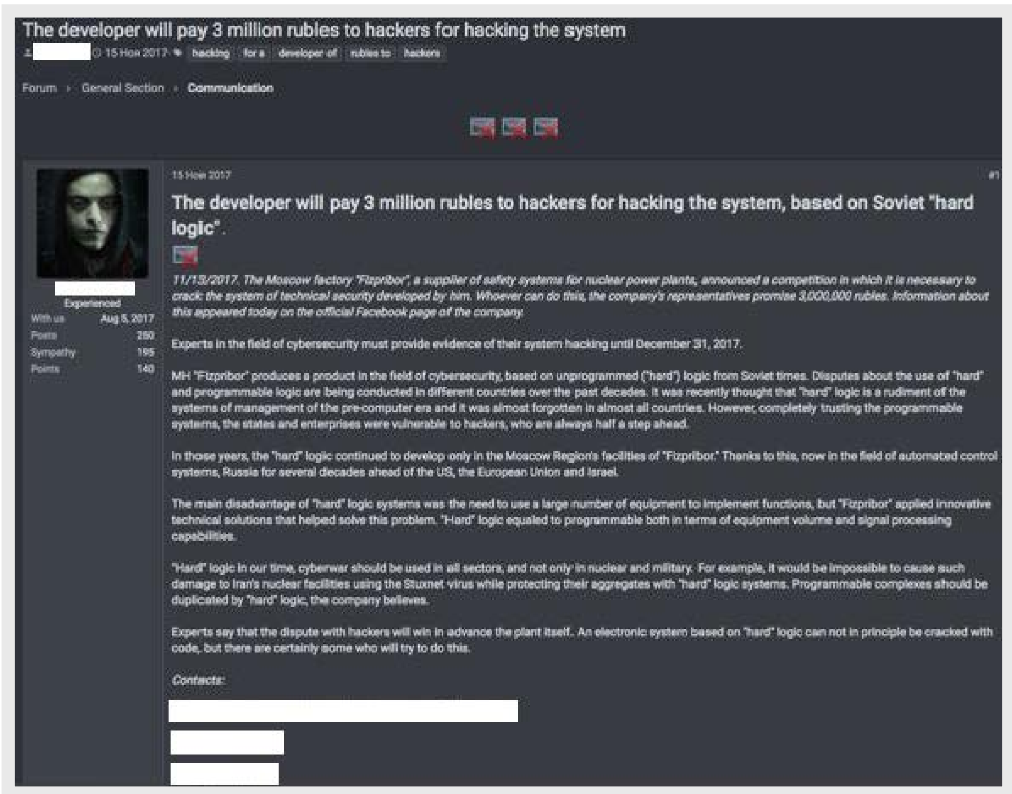
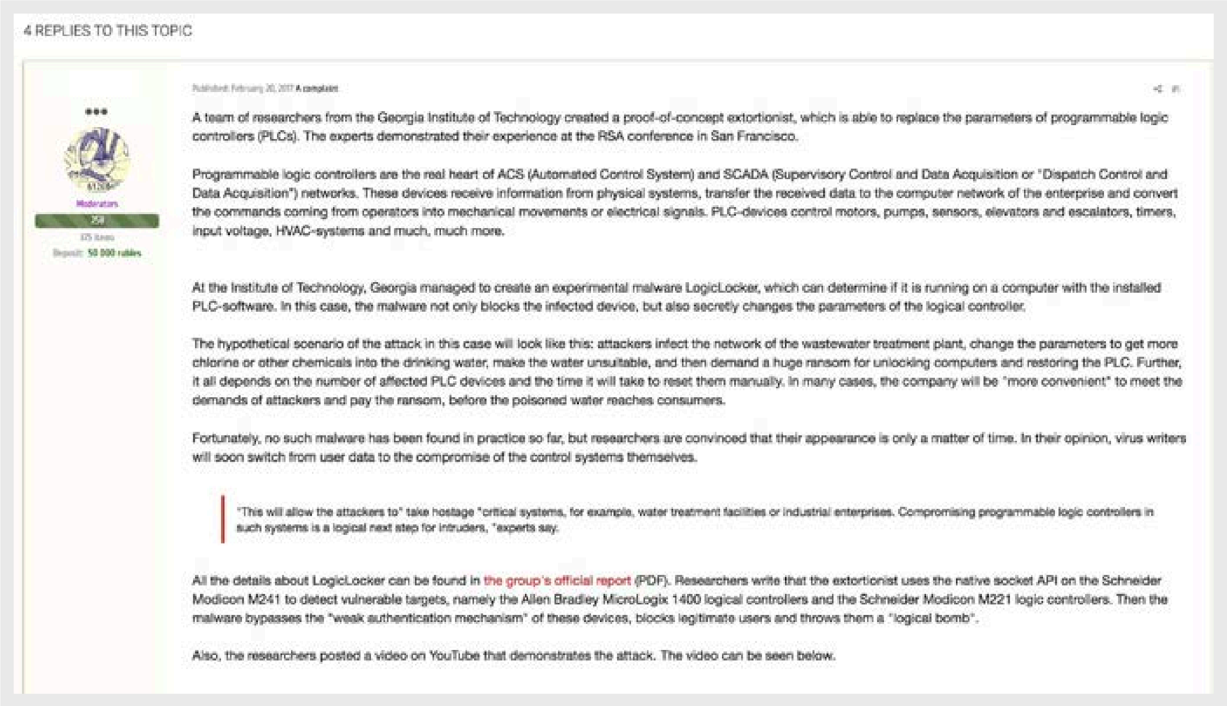


Figure 35. Discussion on a bug bounty program for safety equipment at nuclear plants

- News about attacks and proofs of concept (PoCs) related to the energy and water industries.



4 REPLIES TO THIS TOPIC

Published February 20, 2017 A complaint

A team of researchers from the Georgia Institute of Technology created a proof-of-concept extortionist, which is able to replace the parameters of programmable logic controllers (PLCs). The experts demonstrated their experience at the RSA conference in San Francisco.

Programmable logic controllers are the real heart of ACS (Automated Control System) and SCADA (Supervisory Control and Data Acquisition or "Dispatch Control and Data Acquisition") networks. These devices receive information from physical systems, transfer the received data to the computer network of the enterprise and convert the commands coming from operators into mechanical movements or electrical signals. PLC-devices control motors, pumps, sensors, elevators and escalators, timers, input voltage, HVAC-systems and much, much more.

At the Institute of Technology, Georgia managed to create an experimental malware LogicLocker, which can determine if it is running on a computer with the installed PLC-software. In this case, the malware not only blocks the infected device, but also secretly changes the parameters of the logical controller.

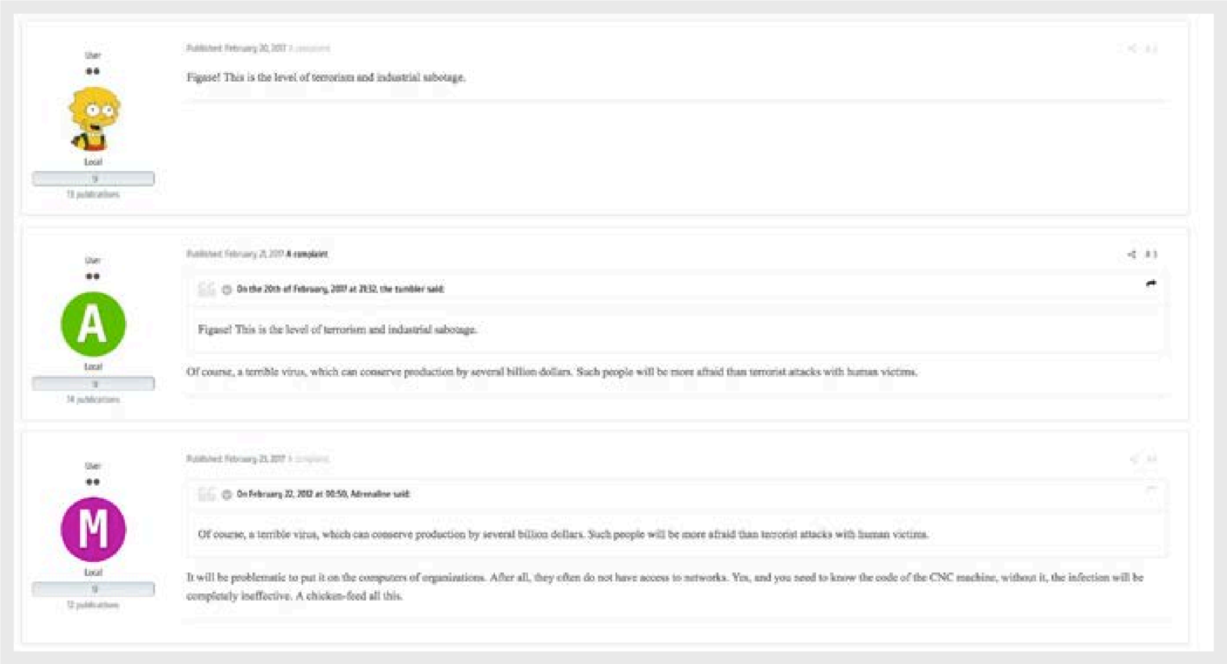
The hypothetical scenario of the attack in this case will look like this: attackers infect the network of the wastewater treatment plant, change the parameters to get more chlorine or other chemicals into the drinking water, make the water unsuitable, and then demand a huge ransom for unlocking computers and restoring the PLC. Further, it all depends on the number of affected PLC devices and the time it will take to reset them manually. In many cases, the company will be "more convenient" to meet the demands of attackers and pay the ransom, before the poisoned water reaches consumers.

Fortunately, no such malware has been found in practice so far, but researchers are convinced that their appearance is only a matter of time. In their opinion, virus writers will soon switch from user data to the compromise of the control systems themselves.

> "This will allow the attackers to" take hostage "critical systems, for example, water treatment facilities or industrial enterprises. Compromising programmable logic controllers in such systems is a logical next step for intruders, "experts say.

All the details about LogicLocker can be found in the group's official report (PDF). Researchers write that the extortionist uses the native socket API on the Schneider Modicon M241 to detect vulnerable targets, namely the Allen Bradley MicroLogix 1400 logical controllers and the Schneider Modicon M221 logic controllers. Then the malware bypasses the "weak authentication mechanism" of these devices, blocks legitimate users and throws them a "logical bomb".

Also, the researchers posted a video on YouTube that demonstrates the attack. The video can be seen below.



User

Local

Published February 20, 2017

Figase! This is the level of terrorism and industrial sabotage.

User

Local

Published February 21, 2017 A complaint

On the 20th of February, 2017 at 21:32, the tumbler said:

> Figase! This is the level of terrorism and industrial sabotage.

Of course, a terrible virus, which can conserve production by several billion dollars. Such people will be more afraid than terrorist attacks with human victims.

User

Local

Published February 21, 2017

On February 22, 2012 at 00:50, Adrenaline said:

> Of course, a terrible virus, which can conserve production by several billion dollars. Such people will be more afraid than terrorist attacks with human victims.

It will be problematic to put it on the computers of organizations. After all, they often do not have access to networks. Yes, and you need to know the code of the CNC machine, without it, the infection will be completely ineffective. A chicken-feed all this.

Figure 36. Discussion of ransomware for SCADA PoC from Georgia Tech University

7. Conclusion

It is safe to assume that in most countries the energy sector is their top critical infrastructure. This is not difficult to imagine especially in major industrial economies where almost every aspect of the economy is directly dependent on a steady energy supply. Water is a natural extension of the energy sector, with water being a key component in hydroelectric and geothermal plants. In itself, water is a necessity of life. News outlets cover prominent cyberattacks against CI (e.g., Black Energy, Triton, Stuxnet, Shamoon, etc.) and overall spread the message that protecting CI against cyberattacks should be of the highest priority for the organizations that operate it.

Given the widespread messaging about the need to protect CI, we set out to discover just how well protected CI sectors were in reality using the energy and water sectors as our research targets. All of our explorations were done using OSINT techniques *requiring ZERO interaction with the devices and/or systems themselves*. We mostly used publicly available data sources but also mined Trend Micro Smart Protection Network (SPN) feedback data for malware detection statistics. We created techniques for manipulating the data we collected to gain new insights. To cover all bases we also looked into criminal underground forums, searching for chatter around CI attacks.

We summarized our findings and observations below:

- Using Shodan and Shodan IP histories, we collected data on internet-exposed energy and water HMIs. All the oil and gas HMIs we found were located in the U.S., with the only exception being a drilling rig controller in the Middle East. Exposed biogas HMIs were found only in Europe, with Germany and France having the most number of these devices/systems exposed online. Power system HMIs were found mostly in Europe, one in Asia, and surprisingly none in North America. Water utility HMIs were discovered all over the globe. The HMIs we discovered were accessible via unauthenticated VNC servers; a potential attacker can interact with these exposed HMIs using a VNC viewer. Alarmingly, many of these exposed HMIs have critical functionalities like start, stop, reset, alarm, parameter changes, and so on, easily accessible by anyone. If an attacker accesses these exposed HMIs, then they can inflict serious system damage or cause failures.

- We didn't want to exclusively depend on Shodan for all our data, so we searched for other public data sources that we also used in our analysis. Google was very helpful in searching for ICS/SCADA device landing pages when we knew the page title and "inurl" keywords. Nmap is the best tool for collecting data about open ports and services when the target's IP range is known, so we went about devising methods to find IP ranges for water and energy organizations using public data. Websites like Electrical Japan, Descartes Labs, Picbleu and Energy Charts gave us the physical locations of energy and water facilities. Using a technique we call GeoStalking, done using Maxmind's GeoIP database, we were able to find ranges of IP addresses in the immediate vicinity of the facilities we were able to locate. It won't come as a complete surprise to us to learn that potential attackers are already using similar techniques to find and scan the IP ranges of their targets.
- Now that we have established how to consistently find devices/systems inside energy and water facilities using public data sources, we used our knowledge of ICS to theorize real-world cyberattacks against these facilities exploiting the exposed devices/systems and to determine their true damage potential. In many cases, using the embedded metadata we were even able to locate the physical facilities via Google Maps. Previously published Trend Micro research papers on ICS/SCADA honeypots — two in 2013[5, 6] and one in 2015[7] — have proven that exposed ICS/SCADA controllers are frequently scanned and attacked (i.e., system parameters and configurations being changed) by attackers from around the globe. So it is conceivable to assume that the live ICS devices/systems we discovered to be exposed online may have been subject to both passive and active cyberattacks.
- Our exploration in the criminal underground forums yielded some interesting results and conclusions. Our initial expectation was that, due to the poor ROI compared to traditional cyberattacks, ICS attacks would not have the same appeal as other widespread cyberattacks. ICS attacks were thus expected to be the exclusive domain of sophisticated state-sponsored actors. However, digging deeper in the forums we made some unexpected discoveries. We found people looking to learn about SCADA security in underground forums because they didn't want to pay for expensive courses. We found threat actors looking to purchase ICS/SCADA credentials and information about exposed devices/systems, possibly for use in reconnaissance activities or for lateral movement attacks. There were even cyberattacks requested against competitors to disrupt them and gain a competitive advantage. Finally, there were opportunistic sellers who have hacked an industry target and are trying to monetize the stolen data. Thus, we conclude that interest in ICS/SCADA isn't scarce as initially expected; the volume of requests is not large, yet the interest is real.

So how secure is CI in reality? The answer is a bit of a mixed bag. First and foremost, while the number of exposed energy and water devices/systems that we discovered was relatively small, it is still a cause for concern because these systems should not be exposed online in the first place. The good news is that we didn't find exposed assets from the well-known big corporations and/or state-owned entities that operate CI. The exposed assets that we found were mostly owned/operated by small companies. However attackers are not bound by the same restrictions that researchers are bound by — so this does not mean larger companies are necessarily fully secure. The bad news is that smaller companies frequently are part of the supply chain that feeds resources to big corporations; thus, a cyberattack against a small company can indirectly affect bigger corporations. Supply chain dependencies means it is critical to protect both big and smaller players alike — the supply chain is only as robust as its weakest link. While CI cybersecurity awareness is steadily growing and significant steps have been taken to secure CI, its protection could still definitely be better improved. Otherwise we would not have been able to find all the exposed devices/systems discussed in this paper. The process of improvement will take time, given the complexity of CI systems and the large number of players involved in the industry, but creating awareness about the vulnerable areas that need immediate attention helps expedite the process, and is the primary goal of this research.

Appendix

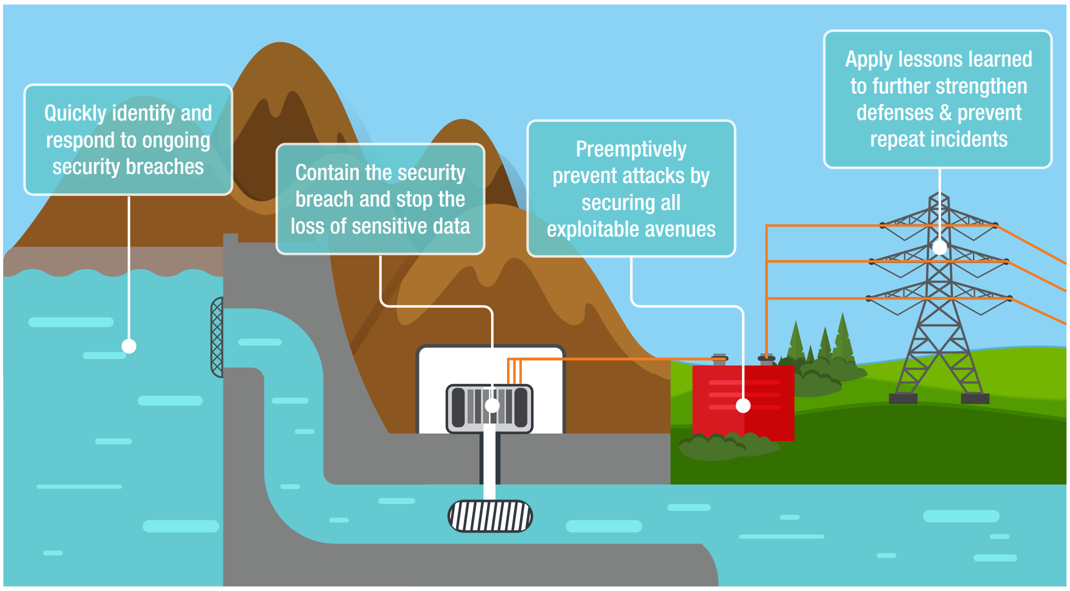
Protecting the Water and Energy Sectors

Defensive Strategies for Industrial Control Systems

(Most of the sections here are derived from a previously published article.[43])

In today's competitive global market for commodities and manufactured goods, reliance on natural resources for economic development and fluctuating geopolitical climates have all contributed to making industries targets of cyberespionage campaigns, and in extreme cases, disruptive and destructive cyberattacks. These cyberespionage campaigns are geared toward ensuring interest groups have access to the latest technical knowledge and intelligence that will help them maintain a competitive advantage and thrive in a market-driven global economy. Cyberespionage campaigns are also used for conducting carefully planned strategic or retaliatory cyberattacks against a nation's critical infrastructure.

Cyberattack and data breach prevention strategies should be considered an integral part of daily business operations. Ultimately, no defense is impregnable against determined adversaries. The key principle of defense is to ***assume compromise*** and take the necessary countermeasures.

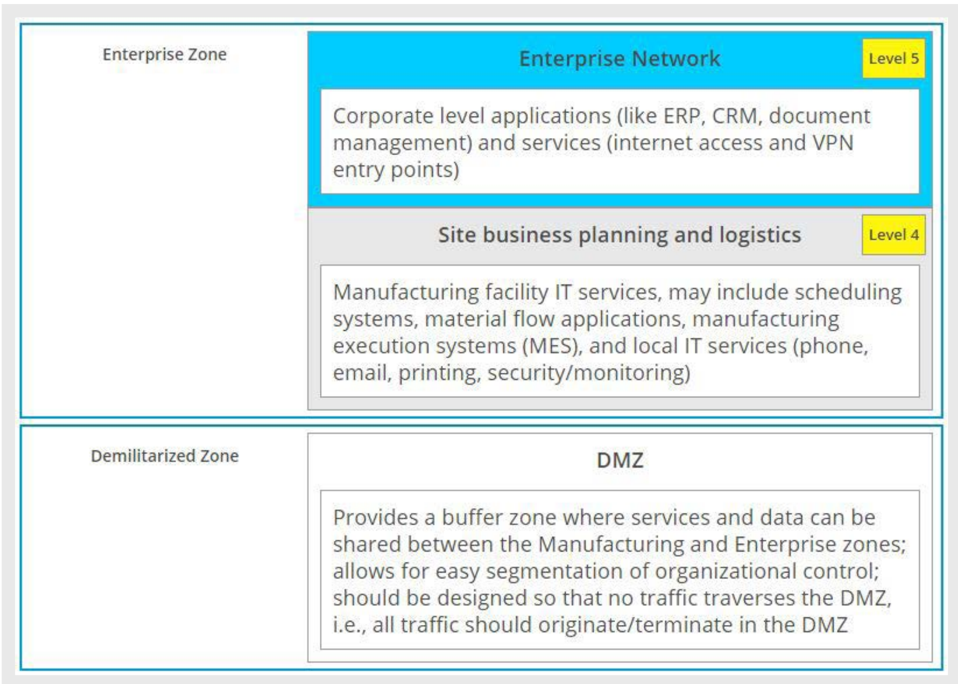


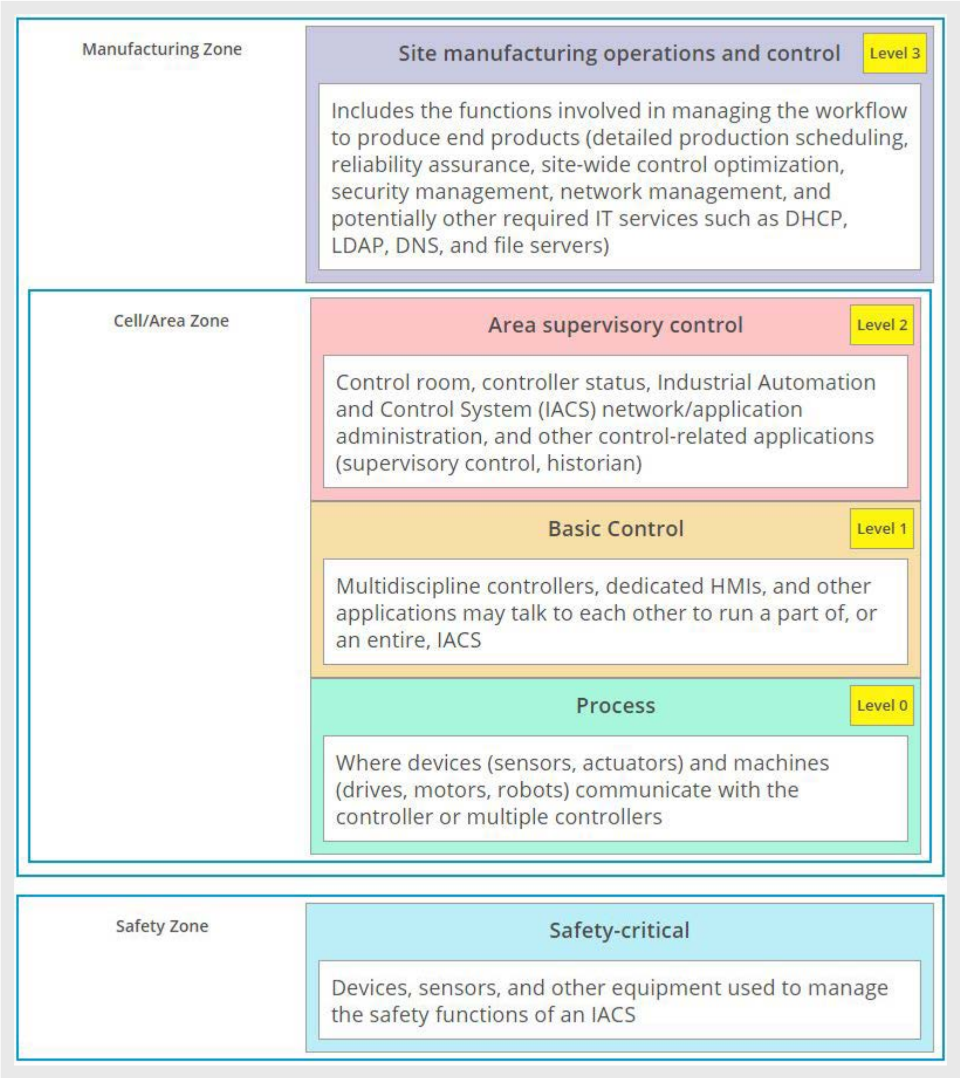
Cyberattacks and data breaches are inevitable. Thus, having effective alert, containment, and mitigation processes are critical. In this section, we present recommendations for defense against attacks and breaches. We start with a framework on how ICS networks should be viewed, then discuss strategies on how to secure specific network-related components, include recommendations for working securely with third parties, and finally discuss how to deal with insider threats.

Network Segmentation

In the manufacturing sector, one widely adopted model is the Purdue Model for Control Hierarchy, which categorizes equipment and devices into a hierarchy of functions.[44] The International Society for Automation's (ISA-99) Committee for Manufacturing and Control Systems Security identified the levels and logical framework shown as follows.

The framework identifies five zones and six levels of operations.





ICS Security Strategies

> "Cyber security starts by developing an understanding of the risks an organization faces, and those it may expose its clients and other stakeholders to. Given some of the applications of ICS, these risks can extend beyond financial and business risks and include loss of life and injury. It is therefore imperative that organizations consider their exposure to cyber threats, assess the resulting risks, and implement safeguards accordingly."
>
> ***- Public Safety Canada***

To help with this, Public Safety Canada created a list of recommended best practices that organizations should follow in order to secure their ICS environments.[45]

Strategy	Recommendations
1. Network Segmentation	The purpose of network segmentation is to partition the system into distinct security zones and implement layers of protection to isolate critical parts of the system using a policy enforcement device.
2. Remote Access	A variety of technologies are available today that provide “secure” remote access to computer systems such as firewalls, Virtual Private Network (VPN), callback (for dial-up), multi-factor authentication, user access control, and intrusion detection. Often, ICS are used in remote location where connectivity is limited. For this reason, ICS often uses dial-up connections. Such connections should be secured.
3. Wireless Communications	Wireless access to the ICS network introduces risks similar to remote access with some additional threat vectors (e.g. unauthorized individual accessing the wireless network from outside the physical security perimeter of the plant). Additionally, the wireless medium is extremely susceptible to denial of service (DoS) attacks.
4. Patch Management	Patch management is an important component of an overall control system security strategy. In many cases, the only effective mitigation for a newly discovered vulnerability is to install a vendor released software patch or update
5. Access Policies and Control	Access control is a wide-ranging topic that covers all aspects of controlling access to a network, device or service, including physical and electronic access.
6. System Hardening	Hardening the components of the system means locking down the functionality of the various components in the system to prevent unauthorized access or changes, remove unnecessary functions or features, and patch any known vulnerabilities.
7. Intrusion Detection	All systems require some method of monitoring system activity and identifying potentially malicious events in the network. Without this ability to monitor a system, minor security issues will remain undetected until they become critical security incidents.
8. Physical and Environmental Security	Physical access to critical ICS assets should be limited to only those who require access to perform their job and only using approved or authorized equipment. In addition to physical access control, critical equipment such as ICS needs to be appropriately hardened and protected from environmental hazards.
9. Malware Protection and Detection	In general, the benefits of running anti-virus software on ICS hosts far outweigh the risk that the anti-virus software will have a negative impact on the system.
10. Awareness	ICS security training and awareness of personnel is an essential tool for reducing cyber security risks. It is critical that any ICS security program have a training and awareness program so that employees understand their role and what is expected of them. Knowledgeable and vigilant staff is one of the most important lines of defense in securing a system.
11. Periodic Assessment and Audits	Numerous factors affect the security of a system throughout its life cycle. Therefore, it is important to periodically test and verify that the system is still configured for optimal security.

Strategy	Recommendations
12. Change Control and Configuration Management	Change management policy and procedures are used to control modifications to hardware, firmware, software, and documentation to ensure the ICS is protected against improper modifications prior to, during, and after commissioning.
13. Incident Planning and Response	A comprehensive cyber incident response plan should include both proactive measures and reactive measures. Proactive measures are those that can help prevent incidents or better allow the organization to respond when one occurs, whereas reactive measures can help detect and manage an incident once it occurs.

Securing Collaborative Network Environments

Organizations regularly employ contractors and third-party vendors to provide them with goods and services such as equipment rental, catering, transportation, consultancy, maintenance, etc. Contractors in turn might hire sub-contractors, all of which contribute to a challenging cyber ecosystem especially when the vendors, contractors, and sub-contractors all have operational needs to access the corporate network. Partnerships expand opportunities, but they also increase cybersecurity risks. Cybercriminals are successfully compromising contractors and third-party vendors and leveraging them as backdoor pathways into their targeted corporate networks. The retailer Target was victimized in one of the largest credit card data breaches ever in November 2013. It later emerged that the cybercriminals broke into Target's network via a third-party HVAC vendor who had access to Target's corporate network.[46] Third-party vendors and contractors don't have uniform cybersecurity policies and practices. This creates exploitable weaknesses in the operations chain, as was demonstrated in the case of Target. IT collaboration described from a "castle" perspective means inviting partners across the traditional moat: not everyone inside is safe, not everyone outside is dangerous.

Collaborative network environments pose unique challenges for IT. IT needs to be involved in the initial planning and development stages so they can do risk assessment to determine proper IT solutions design. If IT does not fully understand the terms and requirements of the partnership agreement, then they might be restricted to just providing tactical solutions in an ad-hoc manner. Lack of IT involvement in the planning and development stages also means IT solutions might not meet required compliance standards. Incorrectly granting access to digital assets increases the risks of security breaches and can violate contractual agreements with third parties. According to *Manage Risk in a Collaborative Network Environment with Partners and Vendors* by Zoltan Palmai, here are a few suggestions for keeping CIs secure.[47]

New partnership considerations for IT include:

- Insider threat complacency
- Insider threat ignorance
- Insider threat malice
- No operating agreement terms for digital assets
- No standardized operating agreements with partners
- Application licensing agreements
- Export compliance laws
- Risks of intellectual property leakage
- Privacy regulations
- Changes to the operating terms over time, etc.

Different partners will require different access privileges to project data, corporate data, applications, etc. and IT needs to carefully set up digital boundaries to prevent security breaches via third parties who have access to the corporate network. Third party requests should be reviewed by IT, Legal, and relevant Departments. There should be rigorous implementation of the IT solutions, proper documentation, and regularly scheduled compliance reviews/revalidation based on assessed risks. Risk assessment considerations include:

- Partner reputation
- International or domestic partnerships
- Cyber security risks in the country of operations
- Corruption in country of operations
- Joint operations risk scenarios
- Type of legal joint venture entity (IT should have pre-defined operation models to support different joint venture operating environments and their associated risks.)

Security best practices include:

- Identifying intellectual property and safeguarding them
- Confining intellectual property access to a need-to-know basis, and
- Training employees to protect intellectual property

Strategies for securing the corporate network include:

- Deploying Network Access Control (NAC) to build a secure front. This enables the authentication of users and devices before they are allowed to connect to the corporate network.
- Implementing identity awareness, the process of establishing and recording user and device identities and their associated access control policies. The stored identity defines and manages access for every type of network user and device used.
- Using identity-aware firewalls, which will enable control of the network and servers based on access policies defined for each connecting user or device.
- Strengthening policy enforcement by integrating the access control and identity- awareness components into a final network architecture solution that is capable of enforcing access policies on wired, wireless, and VPN networks, regardless of how and where users connect.

Recommendations for Managing Supply Chain Threats

(This section was derived from the Securing Connected Hospitals paper published in partnership with HITRUST. It has been modified to fit the scope of this research paper.[48])

To manage the growing risk of supply chain attacks, organizations need to develop or improve their risk management programs. We recommend the following actions:

- Perform vulnerability assessment of new devices/equipment to determine if they pose any cyber risks or not prior to connecting them to the corporate and/or ICS network. This assessment is to ensure that the functional integrity of the device/equipment has not been compromised on the manufacturer's end.
- Bring your own device (BYOD) programs should include authentication using network access controls (NAC) before allowing access to the network for an employee's mobile phones, tablets, and items like USB drives. Purchase devices/equipment from manufacturers who go through rigorous security assessment of the products during design and manufacture. This ensures the purchased devices/ equipment have had proper vulnerability assessment done and poses a low risk inside the corporate and/or ICS network.
- Develop a plan for patching and updating software and/or firmware in devices/equipment that are used in key or critical processes.
- Perform risk assessment of all suppliers and vendors in the supply chain.

- Perform thorough background checks on all employees who may have physical access to computers or equipment. This includes all temporary, contract, seasonal, and volunteer staff. Background checks should not be a one-time-only-affair done during hiring, but instead should be repeated every couple of years to ensure employees don't have any subsequent undisclosed criminal records.
- Identify third-party vendor software and perform security and vulnerability testing to ensure they are safe from hackers. Penetration testing of the corporate network by professional pentesting companies is highly recommended.

Securing Against Insider Threats

Insiders are trusted individuals or persons of authority who have access privileges but use those privileges to steal data. Motivations for insider threats could be money, ideology, coercion and ego. Frequently, more than one of these motives are at play. Insider threats could be a challenging task, and prevention and mitigation techniques can either be categorized as technical and non-technical.[49]

Technical steps to prevent insider attacks make use of security best practices. Insider attacks should be prioritized the same as external attacks. Similar to external attacks, insider attacks cannot be prevented, and so organizations need to detect such threats as quickly as possible. Monitoring and keeping a log of activities, for example, what data is moving through or going out the network, can identify suspicious behavior and potential insider threats. The key principle of defense is to assume compromise, including insiders — for example, an attacker could use compromised user accounts to navigate the corporate and ICS networks. Set up proper access controls to ensure that employees access only information they need for their daily tasks. To prevent leaks, credentials of employees no longer with the organization should be immediately revoked.

Non-technical means of security are equally effective in preventing insider threats. Insider attacks could be motivated by employee discontent. Professional management practices in handling delicate situations, recognizing and rewarding employees, and looking after employee well-being all help in diffusing potential insider threats. In a nutshell, happy employees are less likely to turn against their employers.

References

1. Michael Assante. (9 January 2016). *SANS Industrial Control Systems Security Blog.* "Confirmation of a Coordinated Attack on the Ukrainian Power Grid." Last accessed on 28 August 2018 at https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid.

2. United Nations. (16 May 2018). *United Nations*. "68% of the world population projected to live in urban areas by 2050, says UN | UN DESA Department of Economic and Social Affairs." Last accessed on 31 August 2018 at https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

3. Homeland Security. (11 July 2017). *Homeland Security*. "Critical Infrastructure Sectors." Last accessed on 26 July 2018 at https://www.dhs.gov/critical-infrastructure-sectors.

4. Tyson Macaulay. (2009). Critical infrastructure: Understanding its component parts, vulnerabilities, operating risks, and interdependencies. Boca Raton, FL: CRC.

5. Kyle Wilhoit. (15 March 2013). *TrendLabs Security Intelligence Blog*. "Who Is Really Attacking Your ICS Devices?" Last accessed on 13 June 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/.

6. Kyle Wilhoit. (27 August 2013). *TrendLabs Security Intelligence Blog*. "The SCADA That Cried Wolf: Who Is Really Attacking Your ICS Devices Part 2." Last accessed on 13 June 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/the-scada-that-cried-wolf-whos-really-attacking-your-ics-devices-part-2/.

7. Kyle Wilhoit. (5 August 2015). *Trend Micro*. "The Gaspot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers." Last accessed on 24 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-gaspot-experiment?_ga=2.188009064.1386592368.1535432678-2082030732.1523520172.

8. HD Moore. (22 January 2015). *Rapid7 Blog*. "The Internet of Gas Station Tank Gauges." Last accessed on 24 August 2018 at https://blog.rapid7.com/2015/01/22/the-internet-of-gas-station-tank-gauges/.

9. Abigail Pichel. (14 July 2014). *Trend Micro*. "HAVEX Targets Industrial Control Systems." Last accessed on 29 August 2018 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/139/havex-targets-industrial-control-systems.

10. Phil Muncaster. (14 October 2014). *Infosecurity Magazine*. "Microsoft Zero Day Traced to Russian 'Sandworm' Hackers." Last accessed on 28 August 2018 at https://www.infosecurity-magazine.com/news/microsoft-zero-day-traced-russian/.

11. Kyle Willhoit and Jim Gogolinski. (16 October 2014). *TrendLabs Security Intelligence Blog*. "Sandworm to Blacken: The SCADA Connection." Last accessed on 28 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/.

12. Brian Gorenc and Fritz Sands. (23 May 2017). *TrendLabs Security Intelligence Blog*. "The State of SCADA HMI Vulnerabilities." Last accessed on 28 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

13. Kim Zetter. (3 March 2016). *Wired*. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Last accessed on 31 August 2018 at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

14. Kyle Wilhoit. (11 February 2016). *TrendLabs Security Intelligence Blog*. "KillDisk and BlackEnergy Are Not Just Energy Sector Threats." Last accessed on 31 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

15. Dustin Volz. (11 March 2016). *Reuters*. "U.S. to blame Iran for cyber attack on small NY dam: Sources." Last accessed on 31 August 2018 at https://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WC2NH.

16. John Leyden. (24 March 2016). *The Register*. "Water treatment plant hacked, chemical mix changed for tap supplies." Last accessed on 31 August 2018 at https://www.theregister.co.uk/2016/03/24/water_utility_hacked/.

17. Andy Greenberg. (13 June 2017). *Wired*. "'Crash Override': The Malware That Took Down a Power Grid." Last accessed on 1 September 2018 at https://www.wired.com/story/crash-override-malware/.

18. Anton Cherepanov and Robert Lipovsky. (17 June 2017). *Welivesecurity by Eset*. "Industroyer: Biggest threat to industrial control systems since Stuxnet." Last accessed on 1 September 2018 at https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

19. Blake Johnson, Dan Caban , Marina Krotofil, Dan Scali, Nathan Brubaker and Christopher Glyer. (14 December 2017). *FireEye*. "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure." Last accessed on 4 September 2018 at https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

20. Feike Hacquebord. (12 January 2017). *TrendLabs Security Intelligence Blog*. "How Cyber Propaganda Influenced Politics in 2016 " Last accessed on 4 September 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cyber-propaganda-influenced-politics-2016/.

21. Ellen Nakashima. (8 July 2017). *The Washington Post*. "U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks." Last accessed on 4 September 2018 at https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?noredirect=on&utm_term=.c45f426aa3d1.

22. United States Computer Emergency Readiness Team. (15 March 2018). *United States Computer Emergency Readiness Team*. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Last accessed on 4 September 2018 at https://www.us-cert.gov/ncas/alerts/TA18-074A.

23. The search engine for the Internet of Things. (n.d.). Last accessed on 4 September 2018 at https://www.shodan.io/.

24. Shodan. (14 December 2017). *Asciinema*. "Downloading all Images for an IP (including historical)." Last accessed on 4 September 2018 at https://asciinema.org/a/152721.

25. Paulino Calderon. (2017). Nmap: Network Exploration and Security Auditing Cookbook (2nd ed.). Birmingham, UK: Packt.

26. Julie Bort. (28 August 2014). *Business Insider*. "Term Of The Day: 'Google Dorking'." Last accessed on 4 September 2018 at https://www.businessinsider.com/term-of-the-day-google-dorking-2014-8.

27. 発電所データベース. Power plant database (n.d.). Last accessed on 4 September 2018 at http://agora.ex.nii.ac.jp/earthquake/201103-eastjapan/energy/electrical-japan/data.html.ja.

28. Descartes Labs: Search. (n.d.). Last accessed on 4 September 2018 on https://search.descarteslabs.com/.

29. Fraunhofer Institute for Solar Energy Systems (n.d.). Map of Power Plants | Energy Charts. Last accessed on 4 September 2018 at https://www.energy-charts.de/osm.htm?country=ALL.

30. Picbleu. (9 March 2018). *Picbleu*. Last accessed on 4 September 2018 at https://www.picbleu.fr/page/carte-des-59-centrales-nucleaires-en-france-usines-et-stockage.

31. Detect Online Fraud and Locate Online Visitors. (n.d.). Last accessed on 5 September 2018 at https://www.maxmind.com/.

32. Bradley Mitchell. (5 July 2018). *Lifewire*. "What Is Virtual Network Computing (VNC)?" Last accessed on 11 September 2018 at https://www.lifewire.com/vnc-virtual-network-computing-818104.

33. Sanjeev Verma. (15 October 2018). *IoT Business News*. "Revealing the power of IoT in Oil and Gas." Last accessed on 17 October 2018 at https://iotbusinessnews.com/2018/10/15/69300-revealing-the-power-of-iot-in-oil-and-gas/amp/.

34. John Matherly. (9 February 2015). *Shodan Blog*. "Why Control Systems Are On the Internet." Last accessed on 4 September 2018 at https://blog.shodan.io/why-control-systems-are-on-the-internet/.

35. Trend Micro Glossary of Terms. (n.d.). *Trend Micro*, "Distributed denial of service (DDoS)." Last accessed on 4 September 2018 at https://www.trendmicro.com/vinfo/au/security/definition/distributed-denial-of-service-ddos.

36. Dave Piscitello. (10 August 2015). *iCann*. "Threats Vulnerabilities and Exploits oh my." Last accessed on 8 June 2018 at https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my.

37. ICS-CERT. (2018). *ICS-CERT*. "Information Products." Last accessed on 8 June 2018 at https://ics-cert.us-cert.gov/Information-Products.

38. Trend Micro. (11 July 2013). "Lateral Movement: How Do Threat Actors Move Deeper Into Your Network?" Last accessed on 8 June 2018 at http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf.

39. Marco Balduzzi, Ryan Flores, Lion Gu, and Federico Maggi. (22 January 2018). *Trend Micro*. "Digital Vandals: Exploring the Methods and Motivations behind Web Defacement and Hacktivism." Last accessed on 4 September 2018 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists.

40. Fernando Mercês. (2 May 2018). *TrendLabs Security Intelligence Blog*. "Cryptocurrency-Mining Malware Targeting IoT, Being Offered in the Underground." Last accessed on 5 September 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-targeting-iot-being-offered-in-the-underground/.

41. Trend Micro Forward-Looking Threat Research Team. (8 May 2018). *Trend Micro*. "Exposed Video Streams: How Hackers Abuse Surveillance Cameras." Last accessed on 5 September 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras.

42. David Sancho. (30 January 2018). *TrendLabs Security Intelligence Blog*. "Digital Extortion: A Forward-looking View." Last accessed on 5 September 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/digital-extortion-forward-looking-view/.

43. Numaan Huq. (10 January 2017). *Trend Micro*. "Defensive Strategies for Industrial Control Systems." Last accessed on 5 September 2018 at https://www.trendmicro.com/vinfo/ph/security/news/cyber-attacks/defensive-strategies-for-industrial-control-systems.

44. Paul Didier, Fernando Macias, James Harstad, Rick Antholine, Scott A. Johnston, Sabina Piyevsky, Mark Schillace, Gregory Wilcox, Dan Zaniewski, and Steve Zuponcic. (9 September 2011). *Cisco and Rockwell Automation*. "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. Last accessed on 9 June 2018 at http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter2.html.

45. Public Safety Canada. (2 December 2015). *Government of Canada*. "Industrial Control System (ICS) Cyber Security: Recommended Best Practices." Last accessed on 9 June 2018 at http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-en.aspx.

46. Brian Krebs. (5 February 2014). *KrebsonSecurity*. "Target Hackers Broke in Via HVAC Company." Last accessed on 9 June 2018 at http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

47. Zoltan Palmai. (January 2016). *Cyber Security for Oil & Gas Canada*. "Manage Risk in a Collaborative Network Environment with Partners and Vendors." Last accessed on 9 June 2018. https://cybersecurityoilgas.iqpc.com/downloads/manage-risk-in-a-collaborative-network-environment-with-partners-and-vendors.

48. Mayra Rosario Fuentes and Numaan Huq. (5 April 2018). *Trend Micro*. "Securing Connected Hospitals." Last accessed on 28 July 2018 at https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf.

49. Jim Gogolinski. (9 December 2014). *TrendLabs Security Intelligence Blog*. "Insider Threats 101: The Threat Within." Last accessed on 9 June 2018 at http://blog.trendmicro.com/trendlabs-security-intelligence/insider-threats-101-the-threat-within/.

TREND MICRO™

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. Optimized for leading environments, including Amazon Web Services, Microsoft®, VMware®, and more, our solutions enable organizations to automate the protection of valuable information from today's threats. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With almost 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

Securing Your
Connected World