

# **The Top 20 Cyber Attacks On Industrial Control Systems**

Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Version 2, December 2020

# ***Table of Contents***

<b>3</b>	— Executive Summary
<b>5</b>	— Introduction
<b>7</b>	— The Top 20 Attacks
<b>20</b>	— Water Treatment System Example
<b>22</b>	— Attack Evaluation
<b>25</b>	— Industrial Internet of Things Design
<b>26</b>	— IIoT Attack Evaluation
<b>27</b>	— Improving ICS Security
<b>29</b>	— Updated Attack Evaluation
<b>32</b>	— Summary
<b>32</b>	— About Waterfall Security Solutions

# Executive Summary

No industrial operation is free of risk, and different industrial enterprises may legitimately have different “appetites” for certain types of risks. Evaluating cyber risk in industrial control system (ICS) networks is difficult, considering their complex nature. For example, an evaluation can consider explicitly or implicitly up to hundreds of millions of branches of a complex attack tree modelling attack interactions with cyber, physical, safety and protection equipment and processes. This paper was written to assist cyber professionals to understand and communicate the results of such risk assessments to non-technical business decision-makers.

This paper proposes that cyber risk be communicated as a Design Basis Threat (DBT) line drawn through a representative “Top 20” set of cyber. These Top 20 attacks are selected to represent cyber threats to industrial sites across a wide range of circumstances, consequences, and sophistication. Many industrial cyber risk practitioners will find the list useful as-is, while expert practitioners may choose to adapt the list to their more detailed understanding of their own sites’ circumstances.

The Top 20 attacks, sorted loosely from least to most sophisticated, are:

- 1 ICS Insider
- 2 IT Insider
- 3 Common Ransomware
- 4 Targeted Ransomware
- 5 Zero-Day Ransomware
- 6 Ukrainian Attack
- 7 Sophisticated Ukrainian Attack
- 8 Market Manipulation
- 9 Sophisticated Market Manipulation
- 10 Cell-phone WIFI
- 11 Hijacked Two-Factor
- 12 IIoT Pivot
- 13 Malicious Outsourcing
- 14 Compromised Vendor Website
- 15 Compromised Remote Site
- 16 Vendor Back Door
- 17 Stuxnet
- 18 Hardware Supply Chain
- 19 Nation-State Crypto Compromise
- 20 Sophisticated Credentialed Insider

A Top 20 DBT diagram for a hypothetical water treatment plant is illustrated in Figure (1).

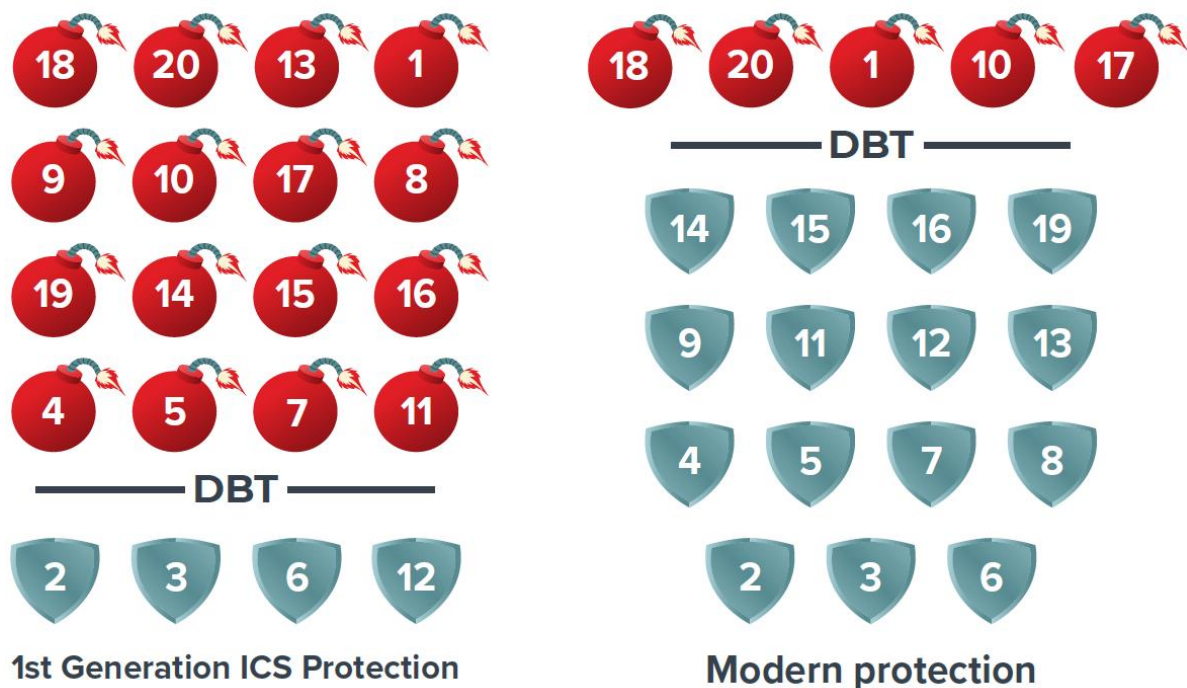


Figure (1) Water treatment system example – two different security postures

In the figure, attacks under the DBT line are defeated reliably. Attacks above the line are not. The “first-generation” DBT illustration at left is of the water treatment system defended by an ICS security program typical of first-generation, best-practice guidance from roughly 2003-2013. The “Modern protection” illustration at right reflects a proposed change to the security program to incorporate modern ICS best practices, including: a strict removable media control policy, Unidirectional Security Gateways and Unidirectional CloudConnect appliances at network perimeters, and an upgrade to the control system test bed.

No network is absolutely secure. Any DBT diagram should therefore illustrate a number of attacks likely to breach the defensive posture under consideration. In any such set of not-reliably-defeated attacks, there is always a least-sophisticated or simplest attack or set of attacks with serious consequences. It is this set that should be the focus of communication with business decision-makers. The question for business decision makers is, “Do these simplest, non-defeated attacks represent acceptable risks, and if not, how much are we willing to pay to close the gap for a particular attack/risk?”

The goal of this paper is to provide a foundation for more consistent cyber risk assessment for industrial sites, and clearer communication of those risks to business decision makers, so that those decision makers can make more informed decisions about funding for industrial cybersecurity initiatives.



# Introduction

The technique for evaluating the risk of cyber-sabotage of industrial processes is highly developed. Essentially, such risk assessments evaluate a typically large inventory of possible cyber attacks against the cyber-physical system in question and render a verdict. Communicating the verdict to business decision-makers who generally lack a deep knowledge of cybersecurity is more difficult, especially for the low-frequency, high-impact (LFHI) type of attacks for which there is little statistical data. The experience of such communications suggests that business decision makers can more easily understand and make effective decisions when given specific examples of cyber attacks, rather than when given abstract risk scores resulting from evaluating millions of attacks.

This paper recommends using a standard set of Top 20 attacks as a methodology for communicating cyber-sabotage risk. The Top 20 set is selected to represent attacks of varying levels of cyber and engineering sophistication, and with varying degrees of undesirable physical consequences. We recommend that a standard Top 20 includes both attacks that are reliably defeated by existing cyber defenses, and attacks that are not so defeated.

The Design Basis Threat (DBT) is a line dividing the list of attacks. The set of attacks below the line are the set of attacks that a site is confident of defeating reliably using an existing, or proposed, security posture. The set above the line represent attacks the site has no such confidence in defeating.

It is the simplest attacks we do not defeat reliably that we use to start our dialog with risk managers. Describe these attacks and their consequences and ask if this situation is acceptable. If not, begin a discussion of how we should draw the DBT line, what security measures might be required to bring about these changes, and what these new measures will cost.

## Reliably Defeating Attacks

To defeat an attack reliably means to prevent the physical consequence of the attack essentially every time this class of attack is launched. For example:

- Antivirus systems – do not defeat common malware reliably, because malware attacks are launched into the wild before antivirus signatures are available for the attacks. If common malware reaches a vulnerable system between the time the malware was launched and the time that AV signatures are available and applied, the targeted system is most likely compromised, despite the deployed AV system.

- Security updates – do not defeat exploits of known vulnerabilities reliably. For example, when an operating system vendor issues a security update, it takes time for the control system vendor to verify that this update is, to the ICS vendor's best understanding, compatible with the vendor's ICS product. It takes additional time for a specific site to test the update on their test bed and determine that the update appears to introduce no new and unacceptable threats to safe and continuous operation. ICS networks are vulnerable to exploits of the known vulnerability during this time interval, despite the existence of a security update program. In addition, security updates are occasionally erroneous, and when erroneous, are not effective in eliminating the known vulnerability that is their motivation.
- Intrusion detection systems and security monitoring systems – are detective, not preventive measures. As important as IDS and security monitoring are to near miss programs as well as ongoing maintenance and optimization of security programs, these measures do not defeat attacks reliably. Intrusion detection and incident response take time. In that time, compromised ICS components and physical equipment may be operated either manually by a remote attacker, or automatically by autonomous malware, which may be enough to bring about the physical consequences the site's security program seeks to prevent.

In contrast, the following are examples of security measures that do defeat a specific class of attack reliably:

- Remote, password-theft, phishing attacks – two-factor authentication based on RSA-style password dongles reliably defeats password phishing attempts. One could postulate an attack that physically steals the password dongle, but that would no longer be a “phishing” attack. A remote attacker who can forge email and produce look-alike websites, but cannot steal physical items locally, is not able to defeat this type of two-factor protection system.
- Encryption key scraping software – trusted platform modules (TPMs) reliably defeat attempts to search compromised computers' memory and persistent storage to steal encryption keys. TPM hardware is designed so that encryption keys never leave the dedicated, cryptographic hardware modules, nor appear in memory in the computer running the TPM. More sophisticated attacks, such as physically dismantling the hardware modules of stolen computers, might succeed in retrieving these encryption keys. Such attacks though, are no longer the indicated attack – software searching a machine's memory and hard drive for keys.
- Internet-controlled malware – unidirectional gateways reliably defeat Internet-controlled malware. The gateways are physically able to send information in only one direction – from a control-critical network to an IT/corporate/Internet network, with no ability to send information back. In unidirectionally-protected networks, no control signal is physically able to be sent from the Internet to malware on a compromised ICS network.

In short, “defeats reliably” is a high standard. Achieving this standard is generally possible only by describing an attack and a target's defences very specifically.

# The Top 20 ICS Cyber Attacks

This section proposes a standard list of 20 cyber attacks to consider when evaluating a defensive design. The list can be useful to sites new to capabilities-based risk assessments. The list can also serve as a standard, representative set of attacks to use when comparing the strength of security postures between sites and between enterprises. Even if experts in an organization decide to define their own list, starting with a standardized list such as the Top 20 can be useful to ensure that a suitably wide range of attacks is considered in the custom assessment process.

Each attack in the list indicates both the level of sophistication of the attack and attackers, and the consequences of the attack:

**Sophistication** is a characteristic of both the attack, and the attacker. Sophistication considers questions such as: Did the attack use standard attack tools downloaded from the Internet, professional-grade tools, or custom-built tools? Are the attackers cyber experts? Do they need to understand the physics of the industrial process, to bring about their attack goals? Do they need to understand the design of relevant industrial control systems enough to connect physical outcomes with cyber manipulations? How much inside information that is not available from public sources do the attackers need in order to design and carry out their attack? Do the attackers have inside assistance? Or can they execute the entire attack from outside of their target organizations?

**Consequences** include physical states of the industrial system that a site seeks to avoid and changes in control system computers that need to be restored to their original state, even if those changes have not yet resulted in measurable effects on the physical process. Physical consequences are most often one of: impaired or poor-quality production, unexpected shutdown of a physical production process, damage to physical equipment, casualties at the site, environmental disasters, and threats to public safety.

The list of 20 attacks is presented in a generally least-sophisticated to most-sophisticated order. Exceptions to this rule occur so that sets of related attacks can be grouped together.

1

## ICS Insider

A disgruntled control-system technician steals passwords by “shoulder surfing” other technicians, logs in to equipment controlling the physical process using the stolen passwords and issues shutdown instructions to parts of the physical process, thus triggering a partial plant shutdown.

**Sophistication:** This is a moderately sophisticated attack. ICS technicians tend to have a good knowledge of how to operate control system components to bring about specific goals, such as a shutdown, but less knowledge of fundamental engineering concepts or safety systems that are designed into industrial processes.

**Consequences:** This class of incident is most often able to cause a partial or complete plant shutdown. More serious physical consequences may be possible, depending on the insider and on details of the industrial process.



## 2

### IT Insider

A disgruntled IT insider “shoulder-surfs” remote access credentials entered by an ICS support technician who is visiting a remote office. The disgruntled insider later uses the credentials to log into the same distant ICS engineering workstation that the technician logged into. The insider looks around the workstation and eventually finds and starts a development copy of the plant HMI. The insider brings up screens at random and presses whatever buttons seem likely to cause the most damage or confusion. These actions trigger a partial plant shutdown.

**Sophistication:** This is an unsophisticated attack. IT insiders generally have little knowledge of cyber systems, control systems or physical processes but often do have social engineering opportunities that can yield credentials able to log into control system networks.

**Consequences:** This class of incident might cause a shutdown or might just cause confusion. At minimum, each such incident triggers an engineering review of settings at the plant, to ensure that no physical equipment has been left misconfigured and able to cause a malfunction in the future.



## 3

### Common Ransomware

An engineer searching for technical information from an ICS-connected engineering workstation accidentally downloads ransomware. The malware exploits known vulnerabilities that have not yet been patched on the industrial network, encrypts the engineering workstation, and spreads to most Windows hosts in the ICS. Most Windows hosts in the industrial network are thus encrypted by the attack, shutting down the control system. The impaired control system is unable to bring about an orderly shutdown. Within a few minutes, the plant operator triggers an emergency safety shutdown.

**Variation:** Ransomware infects an IT workstation and spreads via AUTORUN files on network shares, USB drives, and known network vulnerabilities. The ransomware spreads for several days before triggering the encryption process. Multiple machines on both IT and ICS networks are thus infected, with the same consequences as above.

**Sophistication:** Authors of autonomous ransomware can be very sophisticated cyber-wise, producing malware that can spread quickly and automatically through a network while evading common antivirus systems and other security measures. Such authors though, tend to have no understanding of physical industrial processes or industrial control systems.

**Consequences:** Most often, the minimum damage caused by this kind of incident is an unplanned shutdown lasting for as many days as it takes to restore the control system from backups and restart the industrial process – typically 5-10 days of lost production. In the worst case, important equipment can be irreparably damaged by an uncontrolled shutdown. In this case, replacements for the damaged equipment need to be purchased and installed. Where replacements are not readily available, these replacements must be manufactured first, before they can be installed and activated. Worst-case plant downtime in these latter cases can be up to 12 months.



## 4

## Targeted Ransomware

An attacker with good computer knowledge targets IT insiders with phishing attacks and malicious attachments, gaining a foothold on the IT network with Remote Access Tool (RAT) malware. The attacker uses the RAT to steal additional credentials, eventually gaining remote access to an industrial control system. The attacker seeds ransomware throughout the ICS and demands a ransom. The site quickly disables all electronic connections between the affected plant and outside networks and tries to pay the ransom. The payment mechanism fails, and the ransomware automatically activates, having received no signal from the attacker that the ransom was paid. The ransomware erases hard drives and BIOS firmware in all infected equipment. The plant suffers an emergency shutdown.

**Sophistication:** The attacker is cyber-sophisticated. Increasingly, organized crime organizations are involved with ransomware. These organizations have access to professional-grade malware toolkits, developers, and RAT operators.

**Consequences:** Computer, network and other equipment with erased firmware generally must be replaced – the equipment has been “bricked” in the parlance of cyber attacks. Again, an emergency shutdown may damage physical equipment, delaying start-up for months.

## 5

## Zero-Day Ransomware

An intelligence agency mistakenly leaves a list of zero-day vulnerabilities in operating systems, applications, and firewall sandboxes on an Internet-based command and control center. An attack group, similar to the “Shadow Brokers” who discovered the US National Security Agency (NSA) zero-days, discovers the list and sells it to an organized crime group. This latter group creates autonomous ransomware that propagates by exploiting the zero-day vulnerabilities in file sharing software in the Windows operating system. The malware is released simultaneously on dozens of compromised websites world-wide, and immediately starts to spread. At industrial sites able to share files directly or indirectly with IT networks, the malware jumps through firewalls via encrypted connections to file shares. The compromised file shares infect and encrypt the industrial site, causing an emergency shutdown and damaging physical equipment.

**Sophistication:** Nation-state intelligence agencies are very sophisticated cyber-wise, though generally focused on stealing information rather than causing physical damage. Such agencies routinely discover and/or purchase zero-day vulnerabilities. These agencies have also been known to leak into the public domain some zero days the agencies have discovered or purchased. This attack is very sophisticated cyber-wise but unsophisticated engineering-wise.

**Consequences:** Again, the minimum damage caused by this kind of incident is an unplanned shutdown lasting for as many days as it takes to restore the control system from backups and restart the industrial process – typically 5-10 days of lost production. In the worst case though, important equipment can be irreparably damaged, necessitating costly replacement which make take additional weeks or months.

## 6

## Ukrainian Attack

A large group of hacktivist-class attackers steal IT remote-access passwords through phishing attacks. These attackers eventually compromise the IT Windows Domain Controller, create new accounts for themselves, and give the new accounts universal administrative privileges, including access to ICS equipment. The attackers log into the ICS equipment and observe the operation of the ICS HMI until they learn what many of the screens and controls do. When the group attacks, the attackers take control of the HMI and use it to mis-operate the physical process. At the same time, co-attackers use their administrative credentials to log into ICS equipment, erase the hard drives, and where practical, erase the equipment firmware.

**Variation:** When targeting other kinds of industries, similar attacks are possible, erasing control system equipment and triggering unplanned shutdowns.

**Sophistication:** The attackers here had good knowledge of cyber systems but limited knowledge of electric distribution processes and control systems.

**Consequences:** The Ukrainian attack is reported to have turned off electric power to nearly one quarter million people for up to 8 hours and erased control system equipment at thirty electric substations. Power was only restored when technicians travelled to each of the affected substations, disconnected control system computers and manually/physically turned on power flows again. More generally, unplanned shutdowns are a consequence of this class of attack, and possibly emergency, uncontrolled shutdowns with the potential for equipment damage that accompanies such shutdowns.

## 7

## Sophisticated Ukrainian Attack

A group of attackers is more sophisticated with respect to cyber-attack tools and the engineering details of electric systems. The attack group phishes a low-volume remote access trojan (RAT) into the IT network, such as the BlackEnergy trojan that was reportedly found on IT networks of the utilities impacted by the Ukrainian attack but was not implicated in the attack.

With the RAT, the attackers search for and find additional credentials, eventually compromising the enterprise domain controller. The attack group creates credentials for themselves and logs into ICS servers, reseeding their RAT on the ICS network and ultimately taking over equipment on the ICS network.

Once inside the ICS network, the attack group connects to protective relays and reconfigures them, effectively disabling the relays. The group now sends control commands to very quickly connect and disconnect power flows to parts of the grid, damaging large rotating equipment such as the pumps used by water distribution systems. The attackers also redirect power flows in the small number of high-voltage transmission substations managed by the distribution utilities, destroying high-voltage transformers by overloading and overheating them.

**Sophistication:** This group of attackers is moderately sophisticated, both cyber-wise and engineering-wise.

**Consequences:** Consequences of this attack are more serious. Large water pumps in water distribution systems are damaged, producing drinking water shortages in the affected cities. High voltage transformers must be replaced on an emergency basis, which can take over a week. There is no world-wide inventory of large, high-voltage transformers – while permanent replacements are manufactured, emergency replacements are moved into place from unaffected substations, thus reducing redundancy and capacity in other parts of the electric grid.

## 8

### Market Manipulation

An organized crime syndicate targets known vulnerabilities in Internet-exposed services and gains a foothold on IT networks. They seed RAT tools into the compromised system, eventually gaining Windows Domain Admin privileges. The attackers reach into ICS computers that trust the IT Windows domain and propagate RAT technology to those computers. Because the ICS computers are unable to route traffic to the Internet, the attackers route the traffic via peer-to-peer connections using compromised IT equipment.

Once in the ICS network, attackers download and analyze control system configuration files. They then reprogram a single PLC, causing it to mis-operate a vital piece of physical equipment, while reporting to the plant HMI that the equipment is operating normally. The equipment wears out prematurely in a season of high demand for the plant's commodity output. The plant shuts down for emergency repair of this apparently random equipment failure.

The same attack occurs at two nearby plants. Once the equipment has failed, the perpetrators erase all evidence of their presence from the affected plants' ICS networks. Prices of the commodity produced at the affected plants spike on commodities markets. When plant production at all plants returns to normal, commodity prices return to normal.

Before and after the attack, the attackers routinely speculate on futures markets for the affected commodity. That these attackers make large profits when commodity prices spike unexpectedly is seen by any potential investigators as normal and legal. The attack is repeated in the next season of high demand.

**Sophistication:** The cyber sophistication of this attack and these attackers is moderate – no zero-days were used, and no code was written. The engineering sophistication of this attack is high. The attackers needed access to an engineer able to interpret the control system configurations, select physical equipment to target, identify the PLC controlling the targeted equipment, download the existing program of the targeted PLC, and design and upload a new program able to wear out the targeted physical equipment prematurely, all while reporting to the HMI that the equipment is operating normally.

**Consequences:** Lost plant production and emergency equipment repair costs.

## Sophisticated Market Manipulation

Sophisticated attackers carry out the market manipulation attack but in a way that is more difficult to defeat. They use known vulnerabilities in Internet-facing systems to compromise the IT network of a services company known to supply services to their real target. The attackers write their own RAT malware and deploy it only at the services company, so that antivirus tools at the services company cannot detect the RAT. The attackers use the RAT to compromise the laptops of personnel who routinely visit the real target. When the attackers detect that the compromised laptops are connected to the real target's IT network, the attackers operate the RAT by remote control and propagate the RAT into the target's IT network.

Inside the target's IT network, the attackers continue to operate the RAT. Intrusion detection systems are blind to the activity of the RAT, because the attack is low-volume, using command lines rather than remote-desktop-style communications. The RAT's command-and-control communications are steganographically-encoded in benign-seeming communications with compromised websites. The attack ultimately propagates to the ICS network, with the same consequences as the Market Manipulation attack.

**Sophistication:** The cyber sophistication of these attackers is high. No zero-days were used, but the attackers developed custom malware with steganographically-encoded communications. The engineering sophistication, like the Market Manipulation attack, is also high.

**Consequences:** Lost plant production for days or weeks and emergency equipment repair costs.

## Cell-phone WIFI

Sophisticated attackers seek to inflict damage on a geography they are unhappy with for some reason. The attackers create a useful, attractive, free cell phone app. The attackers use targeted social media attacks to persuade office workers at critical infrastructure sites in the offending geography to download the free app.

The app runs continuously in the background of the cell phone. While at their critical-infrastructure workplaces, the app instructs the phone to periodically scan for Wi-Fi networks and report such networks to a command and control center. The attackers again, use social media, social engineering and phishing attacks to impersonate insiders at their target organizations, and extract passwords for the Wi-Fi networks. Several of these password-protected networks are part of critical-infrastructure industrial control systems.

The attackers log into these networks using the compromised cell phones and carry out reconnaissance by remote control until they find computer components vulnerable to simple denial of service attacks, such as erasing hard drives or SYN floods. The attackers compromise plant operations, triggering an unplanned shutdown. They then disconnect from the Wi-Fi networks, and then repeat this attack periodically.

Variation: Instead of a cell-phone app, attackers use phishing attacks to seed malware on to the desktop computers of office workers who work at the targeted industrial sites, within physical range of ICS Wi-Fi networks.



**Sophistication:** This attack currently needs a high degree of cyber sophistication, because toolkits enabling this type of hidden Wi-Fi hacking from cell phones currently do not exist on the open Internet. Any attackers currently wishing to use this technique would need to write this malware themselves or purchase it from illicit sources. Once such attack tools are widely and publicly available though, this class of attack will come within the means of any hacktivist group with an imagined grievance with industrial enterprises. The attack needs only very low engineering sophistication.

**Consequences:** Repeated plant shutdowns from a source that is difficult to identify. Plant personnel will presumably, eventually determine that the source of the attack is a Wi-Fi network and will shut down all Wi-Fi at the plant, or at least change all the passwords

11

## Hijacked Two-Factor

Sophisticated attackers seek to compromise operations at an industrial site protected by best-practice industrial security. They write custom RAT malware to evade antivirus systems and target support technicians at the industrial site using social media research and targeted phishing emails. The support technicians activate malware attachments and authorize administrative privileges for the malware because they believe the malware is a video codec or some other legitimate-seeming technology.

Rather than activate the RAT at the industrial site, where the site's sophisticated intrusion detection systems might detect its operation, the attackers wait until the technician victim is on their home network but needs to log into the industrial site remotely to deal with some problem. The technician activates their VPN and logs in using two-factor authentication. At this point the malware activates, moving the Remote Desktop window to an invisible extension of the laptop's screen and shows the technician a deceptive error message, such as "Remote Desktop has stopped responding. Click here to try to correct the problem."

The malware provides remote control of the invisible Remote Desktop window to the attackers. The technician starts another Remote Desktop session to the industrial site, thinking nothing of the interruption. In this way, sophisticated attackers have access to industrial operations for as long as the technician's laptop and VPN are enabled. The only hint of the problem that the ICS IDS sees is that the technician logged in twice. The attackers eventually learn enough about the system to mis-operate the physical process and cause serious damage to equipment or cause an environmental disaster through a discharge of toxic materials.

**Sophistication:** Currently this requires a high level of cyber sophistication, since no such two-factor-defeating remote-access toolkit is available for free download on the open Internet. To bring about a serious physical consequence within a limited number of remote-access sessions, a high degree of engineering sophistication is required as well.

**Consequence:** Any attacker willing to invest in the sophisticated, custom malware required for this type of attack will most likely persist in the attack until significant adverse outcomes are achieved.

Hacktivists unhappy with the environmental practices of an industrial site learn from the popular press that the site is starting to use new, state-of-the-art, Industrial Internet of Things edge devices from a given vendor. The attackers search the media to find other users of the same components, at smaller and presumably less-well-defended sites. The hackers target these smaller sites with phishing email and gain a foothold on the IT and ICS networks of the most poorly-defended of these IIoT client sites.

The hackers gain access to IIoT equipment at these poorly-defended sites and discover that the equipment is running an older version of Linux with many known vulnerabilities, because the poorly-defended site has not updated the equipment firmware in some time. The attackers take over one of the IIoT devices. After looking at the software installed on the device, they conclude that the device is communicating through the Internet with a database in the cloud from a well-known database vendor. The attackers download Metasploit to the IIoT device and attack the connection to the cloud database with the most recently-released exploits for that database vendor.

They discover that the cloud vendor has not yet applied one of the security updates for the database and the attackers take over the database servers in the cloud vendor. In their study of the relational database and the software on the compromised edge devices, the hackers learn that the database has the means to order edge devices to execute arbitrary commands. This is a "support feature" that allows the central cloud site to update software, reconfigure the device, and otherwise manage complexity in the rapidly-evolving code base for the cloud vendor's IIoT edge devices.

The hackers use this facility to send commands, standard attack tools and other software to the Linux operating system in the edge devices in the ICS networks the hackers regard as their legitimate, environmentally-irresponsible targets. Inside those networks, the attackers use these tools and remote-command facilities to carry out reconnaissance for a time and eventually erase hard drives or cause what other damage they can, triggering unplanned shutdowns.

In short, hackers attacked a heavily-defended client of cloud services by pivoting from a poorly-defended client, through a poorly-defended cloud.

**Sophistication:** These attackers are of moderate cyber sophistication. They can download and use public attack tools that can exploit known vulnerabilities, they can launch social engineering and phishing attacks, and they can exploit permissions with stolen credentials. Hacktivists such as these generally have a very limited degree of engineering sophistication.

**Consequences:** Unplanned shutdowns, lost production, and possible equipment damage.

## Malicious Outsourcing

An industrial site has outsourced a remote support function to a control system component vendor – for example: maintenance of the plant historian. The vendor has located their worldwide remote support center in a country with an adequate supply of adequately-educated personnel and low labour costs. A poorly-paid technician at this support center finds a higher-paying job elsewhere. On the last day of employment, this technician decides to take revenge on personnel at a specific industrial client – the same personnel who recently complained to the technician's manager about the technician's performance.

The technician logs into the client site using legitimately-acquired remote access credentials, two-factor credentials and the permanent VPN connection to the targeted site. The technician logs into all the site's control system computers for which the credentials provide access and leaves a small script running on each that, one week later, erases the hard drives on each computer.

**Sophistication:** This is an adversary with limited cyber sophistication and engineering sophistication, who is unable to produce custom malware. This attacker does have credentials and the ability to log into their target remotely and has some knowledge of how that system works – in particular, how to leave a small, simple script running, or schedule such a script to run in the future with administrative privileges.

**Consequences:** The consequences of such an attack vary. For example, no power plant relies on the veracity of its historians for second-by-second operation – at such a target, if the historians were targeted, the consequences would be the loss of historical data since the last backup. Historians targeted at a pharmaceutical plant would more likely trigger the loss of the current batch, since many such plants store their batch records in the historians and are unable to sell products produced in batches whose records are impaired. Such batches can range in value from hundreds of thousands of dollars to hundreds of millions of dollars.

## Compromised Vendor Website

Most sites trust their ICS vendors – but should those vendors' websites be trusted? Hacktivists find a poorly-defended ICS vendor website and compromise it. They download the latest copies of the vendor software and study it. They learn where in the system the name or some other identifier for the industrial site is stored. These attackers are unhappy with a number of industrial enterprises for imagined environmental or other offences and search the public media to determine which of these enterprises use the compromised vendor's software.

The attackers use the compromised website to unpack the latest security update for the ICS software and insert a small script. The attackers repack the security update, sign the modified update with the private key on the web server, and post the hacked update as well as a new MD5 hash for the update.

Over time, many sites download and install the compromised update. At each target, the script activates. If the script fails to find the name of the targeted enterprise in the control system

being updated, the script does nothing. When the script finds the name, it installs another small script to active one week later, erasing the hard drive and triggering an unplanned and possibly uncontrolled shutdown. The one-week delay in consequences makes tracing the attack back to the software update somewhat more difficult.

**Sophistication:** This is a hacktivist-class attack, by attackers of moderate cyber sophistication and limited engineering sophistication. The attackers knew enough about computer systems to use existing tools, permissions and vulnerabilities. They also had enough knowledge to unpack control system products and understand to some degree how they work, as well as unpack and repack security updates.

**Consequences:** The most common consequence of this class of attack is an unplanned shutdown. More serious consequences include the potential for equipment damage due to an uncontrolled shutdown.

15

## Compromised Remote Site

In a SCADA system such as might control an electric distribution system or water distribution system, an attacker targets a substation or pumping station that is physically remote from any potential witnesses. The attacker physically cuts the padlock on a wire fence around the remote station and enters the physical site. The attacker locates the control equipment shed – typically the only roofed building at the site – and again forces the door to gain entry to the shed. The attacker finds the only rack in the small site, plugs a laptop into the Ethernet switch in the rack, and tapes the laptop to the bottom of a piece of computer equipment low in the rack where it is unlikely to be detected. The attacker leaves the site.

An investigation ensues, but the investigators find only physical damage and nothing apparently missing. The extra laptop low in the rack is not noticed. A month later, the attacker parks a car near the remote site and interacts with the laptop via Wi-Fi, enumerating the network and discovering the connections back into the central SCADA site. The attacker uses the laptop to break into equipment at the remote site, and from there into the central SCADA system. The attacker then uses Ukraine-style techniques to cause physical shutdowns.

**Sophistication:** This attack requires physical access to at least one of the remote sites and an investment of physical risk, as well as of equipment in the form of the attack laptop. Hacktivist-class cyber expertise is needed to carry out reconnaissance at the remote site and propagate the attack to the central site. Very limited engineering expertise is needed to bring about a Ukraine-style consequence.

**Consequences:** Interruptions to the movement of electricity, natural gas, water, or whatever else the SCADA system manages are the simplest consequence of this class of attack. Erased hard drives are another simple consequence. Attackers with a higher degree of engineering sophistication could reprogram protective relays or other equipment protection gear, damaging physical equipment such as transformers and pumps. More sophisticated manipulation of pipeline equipment, especially in pipelines transporting liquids, can result in pressure waves able to cause pipeline breaches and serious leaks.



## Vendor Back Door

An industrial site has outsourced a remote support function to a control system component. A software developer at a software vendor inserts a back door into software used on industrial control systems networks. The software may be ICS software or may be driver, management, operating system, networking, or other software used by ICS components. The back door may have been installed with the approval of the software vendor as a “support mechanism” or may have been installed surreptitiously by a software developer with malicious intent.

The software checks the vendor website weekly for software updates and notifies the user through a message on the screen when an update is available. The software also, unknown to the end user, creates a persistent connection to the update notification website when the website so instructs, and permits personnel with access to the website to operate the machine on the ICS network remotely. Hactivist-class attackers discover this back door and compromise the vendor's software-update website with a password-phishing attack. The attackers then use the back door to impair operations at industrial sites associated with businesses the hactivists have imagined that they have some complaint against.

Note that antivirus systems are unlikely to discover this back door, since this is not the autonomously-propagating kind of malware that AV systems are designed to discover. Sandboxing systems are unlikely to discover it either, since the only network-aware behavior observable by those systems is a periodic call to a legitimate vendor's software update site asking for update instructions.

**Sophistication:** To write the back door into the vendor's product source code and into the update web site's source code requires an intermediate degree of cyber sophistication. Such changes are well within the abilities of the software developers working for the vendor though, since such developers are typically hired to produce code that is much more complex than that needed for this type of back door. A moderate degree of cyber sophistication is required of the hactivists who discovered the back door. Only limited engineering sophistication is needed to bring about a plant shutdown. Greater sophistication is needed to cause any more than accidental equipment damage.

**Consequences:** Plant shutdowns and erased hard drives are straightforward consequences for hactivist-class attackers who have carried out this type of attack. More engineering-sophisticated attackers can cause equipment damage and sometimes put worker safety or public safety at risk.

## Stuxnet

Sophisticated attackers target a specific and heavily-defended industrial site. They first compromise a somewhat less-well-defended services supplier, exfiltrating details of how the heavily-protected site is designed and protected. The adversaries develop custom, autonomous malware to target the heavily-defended site specifically and bring about physical damage to equipment at the site. The autonomous malware exploits zero-day vulnerabilities. Service providers carry the malware to the site on removable media. Antivirus scanners are blind to the custom, zero-day-exploiting malware.

**Sophistication:** This class of attack demands a high degree of engineering sophistication to understand the physical process and control system components and to bypass equipment protection and safety systems in an attack. The attack demands a high degree of cyber sophistication as well, to create autonomous, custom malware that is undetectable by the specific cybersecurity technologies deployed at the target site.

**Consequences:** The Natanz uranium enrichment site targeted by Stuxnet is thought to have suffered several months of reduced or zero production of enriched uranium, because of the interference of the Stuxnet worm in the production process. The site is also estimated to have suffered the premature aging and destruction of 1000-2000 uranium gas centrifuge units. More generally, this class of attack can bypass all but physical safety and protection mechanisms and could bring about loss of life, public safety risks and costly equipment damage.

18

## Hardware Supply Chain

A sophisticated attacker compromises the IT network of an enterprise with a heavily-defended industrial site. The attacker steals information about which vendors supply the industrial site with servers and workstations, as well as which vendors routinely ship such equipment to the site. The attacker then develops a relationship with the delivery drivers in the logistics organization, routinely paying drivers modest sums of money to take two-hour lunch breaks, instead of one-hour breaks.

When IT intelligence indicates that a new shipment of computers is on its way to the industrial site, the agency uses the two-hour window to break into the delivery van, open the packages destined to the industrial site, insert wirelessly-accessible single-board computers into the new equipment, and repackage the new equipment so that the tampering is undetectable. Some time after IT records show that the equipment is in production, the attackers access their embedded computers wirelessly, to manipulate the physical process. The attackers eventually impair equipment protection measures, crippling production at the plant through what appear to be a long sequence of very unfortunate random equipment failures.

**Sophistication:** This is an attack by a very sophisticated adversary. This attacker has physical operatives able to carry out covert actions, such as breaking into the delivery van and quickly disassembling, modifying, reassembling, and repackaging the compromised equipment. The attacker is cyber-sophisticated, maintaining a long-term presence on the target's IT network and understanding the design of a variety of computer equipment well enough to know how to subtly insert additional hardware into that equipment. The attacker has a high degree of engineering sophistication as well, to understand the structure of the physical process, the control systems, and the equipment protection systems in enough detail to design and carry out physical sabotage, making damaged production equipment look like random failures.

**Consequences:** Costly equipment failures and plant production far below targets.

19

## Nation-State Crypto Compromise

A nation-state grade attacker compromises the PKI encryption system, either by stealing certificates from a well-known certificate authority, or by breaking a popular crypto-system and so forging certificates. The attacker compromises Internet infrastructure to intercept connections from a targeted industrial site to software vendors. The attacker deceives the site into downloading malware with what appears to be a legitimate vendor signature. The malware establishes peer-to-peer communications that are steganographically tunneled through ICS firewalls and DMZs on what appear to be legitimate vendor-sanctioned communications channels. The nation-state adversary operates the malware by remote control, learning about the targeted site. The adversary creates custom attack tools which, when activated, cause the release of toxins into the environment, serious equipment damage and a plant shutdown.

**Sophistication:** This is a very sophisticated adversary able to defeat the encryption, certificates and cryptographic hashes that are the foundation of many security programs.

**Consequences:** Public safety risks and possible loss of life, costly equipment damage and lost production.

20

## Sophisticated Credentialed ICS Insider

A sophisticated attacker bribes or blackmails an ICS insider at an industrial site. The insider systematically leaks information to the attackers about the design of the site's physical process, control systems and security configurations. The attacker develops custom, autonomous malware designed to defeat the deployed security configurations. The insider deliberately releases the malware on the system with the insider's credentials. A few hours later the malware activates. A day later, there is an explosion that kills several workers, causes a billion dollars in damage to the plant, and shuts the site down for 12-18 months.

**Sophistication:** This is an attacker with a high degree of sophistication in physical operations, able to bribe or blackmail the insider. This attacker has a high degree of engineering sophistication as well, to determine what cyber attack has not been anticipated by the site's safety and equipment protection systems and to determine how to defeat those protections. The attacker also has a high degree of cyber sophistication to produce undetectable, custom, autonomous malware.

**Consequences:** Loss of life, costly equipment damage and lost production.

# Water Treatment System Example

To illustrate using the 20 standard attacks to compare the strength of different security postures, we need a target, and an initial security program. As a target, consider a water and wastewater treatment system. Cybersecurity priorities for the site include:

1. Worker safety – prevent casualties at the site – safety hazards include large reservoirs and pipes able to fill with water, whether or not site personnel are physically at risk inside those pipes and reservoirs, as well as large reservoirs of toxic chlorine gas and fluoride solutions.
2. Public safety – do not route unclean water or water injected with toxic amounts of fluoride into the water distribution system in quantities that put public safety at risk or that trigger “boil water” advisories.
3. Reliability – manage reservoirs, pumping and treatment systems such that quantities, costs, and schedules for clean drinking water comply with service-level agreements with the water distribution utility.

We assume that the control system for the plant is protected to first-generation ICS security best practices, published roughly 2003-2013:

- Only firewalls separate networks at very different levels of criticality.
- Encryption is enabled on all IT and ICS equipment and connections that support such configuration.
- Individual user accounts and passwords are configured on all equipment that supports them, with only the usual exceptions in the ICS space, such as for equipment with only a single account, or HMI workstations that cannot afford to lose visibility into the physical process if operators were to log out and log back in during a shift change.
- The pumping station SCADA WAN uses private, leased telecommunications infrastructure.
- A DMZ separates ICS from IT networks and contains a remote-access jump host, a plant historian, and the plant's Active Directory, AV and other servers synchronized to their respective IT counterparts.
- A comprehensive security-update program is in place. Industrial plant systems cannot be updated as quickly as can IT systems, and because comprehensive testing of the updates on a reliability test-bed takes a long time, most control system components are not updated automatically.
- Antivirus systems are deployed on all equipment that support the corporate AV vendor, with automatic updates.



- Network monitoring information is sent directly from network equipment in the ICS network, through the DMZ, into a central corporate IT NOC/helpdesk in another city.
- Copies of ICS network traffic are fed into a large network intrusion detection analysis engine on the IT network via SPAN and mirror ports on ICS switches.
- Logs, AV alerts, IDS alerts, and other types of security information are sent from ICS equipment to an IT-based SOC.

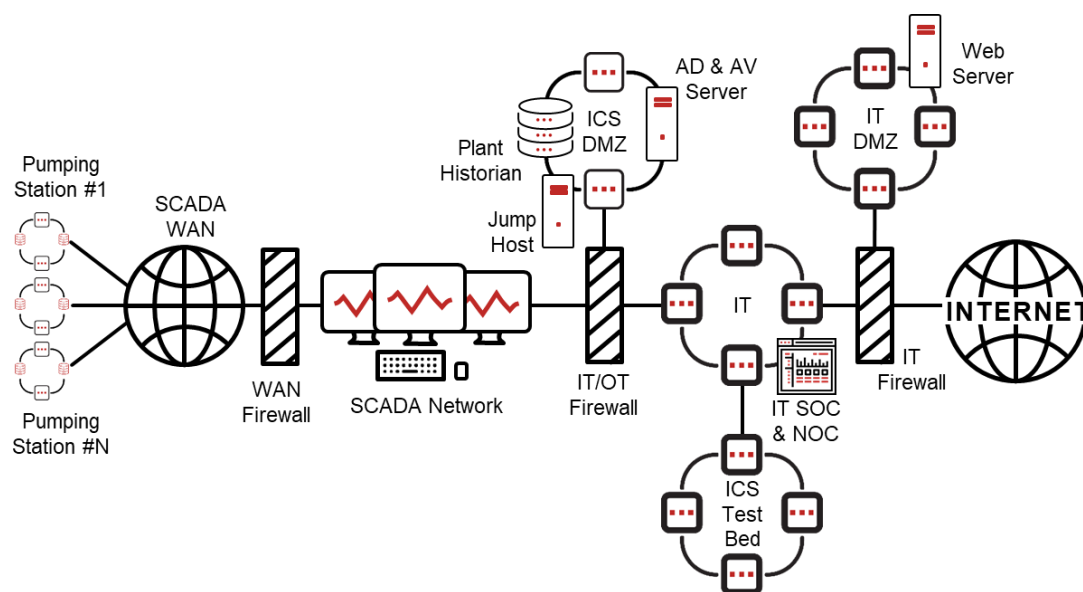









Figure (2) First-gen ICS best-practice water treatment network overview

Third-party service providers have remote access credentials, can log into IT networks and from IT networks into ICS networks via an ICS DMZ jump host. Policies, procedures, responsibilities, and training have been documented and executed according to the IT best practices of the day.

# Attack Evaluation

Evaluating the 20 example attacks against the above system yields the results below. In the list below, a “defeated” status means the attack is defeated reliably, while “not defeated” means that there is not a high degree of confidence in reliably defeating the indicated attack.

-  **1 ICS Insider – not defeated:** None of the indicated security controls prevent an insider from issuing an inappropriate “shut down” command that the insider is authorized to issue.
-  **2 IT Insider – defeated:** IT best practices include two-factor authentication for the remote-access jump host, which reliably defeats social-engineered remote access passwords.
-  **3 Common Ransomware – defeated:** IT best practices applied to ICS networks mean that ICS equipment cannot browse the Internet or download ransomware. Such best practices also forbid hosts that are configured to execute “AUTORUN” files.
-  **4 Targeted Ransomware – not defeated:** Two-factor authentication might prevent the attacker from pivoting through the IT network into the ICS network. A targeted remote-control attack of moderate sophistication, however, can create new accounts on a compromised IT domain controller and two-factor-less accounts on the jump host. Intrusion detection systems on the IT network might or might not detect the attacker, depending on how much effort the attacker is making to minimize their footprint and on how busy the outsourced SOC and enterprise incident response teams are with other apparently higher-priority emergencies.
-  **5 #5 Zero-Day Ransomware – not defeated:** The site has a file sharing server set up in the DMZ to minimize the use of USB drives on ICS equipment. Many ICS and IT workstations have access to that server. If the zero-day attack reaches the ICS before antivirus signatures have been updated and before firewall sandbox security updates are in place, the site will be compromised.
-  **6 #6 Ukrainian Attack – defeated:** A hacktivist-class attack relies on stolen passwords and known vulnerabilities in network-exposed services. Two-factor authentication defeats stolen passwords and no vulnerabilities are exposed to network attacks.
-  **7 #7 Sophisticated Ukrainian Attack – not defeated:** These protections do not defeat targeted, low-volume RAT malware. Once inside the network, the described standard remote-control attack techniques are likely to yield the credentials needed to propagate the attack into the ICS network. Intrusion detection systems on the IT network might detect the attack, depending on how much effort the attackers are making to minimize their footprint and on how busy the outsourced SOC and enterprise incident response teams are with other emergencies.

**8 Market Manipulation – not defeated:** Drinking water is not a commodity traded on most futures exchanges and so technically this attack does not apply. However, in the interests of illustrating how this attack fares against the indicated protections, this section assumes the water site is a legitimate target for market manipulation attacks.

In this case, even when security updates are installed promptly on Internet-facing servers, there may be times when proof-of-concept exploits circulate in the wild for vulnerabilities for which no updates exist yet. Intrusion detection systems may eventually detect the operation of professional attackers using low-grade attack tools, but by then the damage may already be done.

**9 Sophisticated Market Manipulation – not defeated:** Attackers this sophisticated do not need to log into ICS sites through a jump host – they more often compromise the IT domain controller. Once compromised, the attackers can schedule commands to run on ICS equipment, reaching into DMZ file servers and downloading their low-volume, peer-to-peer, steganographically-encrypted malware. Intrusion detection systems might or might not detect this type of attacker, depending on how much effort the attacker is making to minimize their footprint and on how busy the outsourced SOC and enterprise incident response teams are with other emergencies.

**10 Cell-phone Wi-Fi – not defeated:** IT best practices do not forbid encrypted Wi-Fi zones in ICS networks. IT best practices do not guarantee that permissions on ICS networks prevent logging into equipment with stolen passwords and erasing hard drives. Intrusion detection systems might report unusual Wi-Fi connections to ICS Wi-Fi networks, but identifying the source of such connections can be difficult and time-consuming. Not all attacks of this class will be reliably detected and remediated in time to prevent consequences.

**11 Hijacked Two-Factor – not defeated:** This sophisticated attack uses low-volume malware and exploits permissions rather than vulnerabilities, so standard security update and antivirus protections on the technician's laptop are blind to the attack. To intrusion detection systems at the water treatment site, the incoming connection is simply a technician logging into the control system through the jump host and legitimately manipulating the operation of the control system. All this is normal activity.

**12 IloT Pivot – defeated:** There are no IloT edge devices in the control system and so IloT-targeted attacks cause no harm.

**13 Malicious Outsourcing – not defeated:** At least some vendors have remote access through the jump host. Disgruntled employees at these vendors have the opportunity to log into the ICS and impair operations. The consequences of such attacks depend on the cyber and engineering sophistication of the disgruntled attackers.

**14 Compromised Vendor Website – not defeated:** Antivirus sandbox techniques can have difficulty detecting this class of malware when the malware activates only on specific machines. Software upgrade testing techniques generally do not include a step where the clock is set forward repeatedly to trigger suspicious behaviour from embedded malware.

**15 Compromised Remote Site – not defeated:** First-generation ICS protections might or might not defeat a hacktivist-class intrusion of this type. The remote site's firewall might be configured to permit connections to a wide range of ICS hosts, providing the hacktivist with a large selection of attack targets, some of which are likely to provide access deeper into the control system. Intrusion detection systems at the central site might, or might not, detect the activity of the hacktivist in time to prevent consequences.

**16 Vendor Back Door – not defeated:** In ICS networks configured to first-generation protection standards, connections between ICS equipment and specific Internet-based IP addresses belonging to software vendors are often permitted, bypassing the DMZ, precisely to check for security updates. ICS software is generally configured never to update automatically, but a configuration that allows the software to alert site personnel when updates are available is not unusual.

**17 Stuxnet – not defeated:** Custom malware designed specifically with zero-day exploits to defeat the water utility's security-update, antivirus and intrusion detection systems will defeat those systems.

**18 Hardware Supply Chain – not defeated:** Depending on the sophistication of the attacker, physical tampering can be made arbitrarily difficult to detect. Intrusion detection systems designed to detect rogue access points may not detect rogue Wi-Fi clients. Host-based protections on existing hosts cannot prevent this kind of supply chain attack from introducing new cyber assets and Wi-Fi communications into a network environment.

**19 Nation-State Crypto Compromise – not defeated:** Cryptosystems are the foundation of many software-based security technologies. When a cryptosystem is compromised, these protections fail to detect command insertion, falsified security updates and other forgeries.

**20 Sophisticated Credentialed ICS Insider – not defeated:** It is very difficult to reliably defeat compromised insiders assisting very sophisticated attackers.

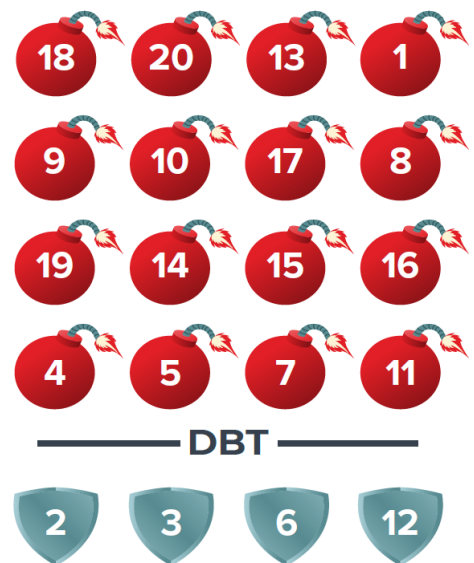


Figure (3) Design Basis Threat for first-gen ICS security program

Given the analysis above, the DBT for this set of attacks and this target is illustrated in Figure (3). In the figure, the attacks below the DBT line are reliably defeated by the security posture. Those above the line are not defeated reliably.



# Industrial Internet of Things Design

These assessment results can now be used as a baseline to understand the impact of proposed control system and security posture changes. For example, the water site might be considering an upgrade of their control system to use new “Industrial Internet of Things” capabilities:

- Industrial Internet of Things (IIoT) edge devices are sensors and actuators with their own CPUs and software that do not rely on conventional PLCs or HMIs to operate. IIoT edge devices generally connect directly to Internet-based cloud services with those connections forwarded through multiple layers of ICS firewalls. The cloud services are generally able to receive data from the devices, update firmware in the devices and are often able to send control, optimization, and other information to the devices.
- Outsourced “cloud” service providers offer so-called “big data analysis” services as well as other expert-level services to industrial sites. Again, the expectation is that these Internet-based cloud providers have continuous monitoring access to the ICS equipment and software they are monitoring, as well as continuous or on-demand remote access to those systems in order to adjust the systems for optimal performance.

In this example, the water site wishes to deploy vibration, oil quality and other measurement edge devices for all large water pumps and other rotating equipment in the central water treatment site. This means deploying many edge devices from many vendors, with each edge device connected through layers of firewalls to its respective vendor's cloud site or sites. In addition, the site wishes to:

- Outsource security monitoring services to an Internet-based SOC provider,
- Outsource management and support of their primary water treatment ICS software to the software's vendor, and
- Outsource the support and management of several other software applications as well.

The changed elements of the ICS network architecture are illustrated below:

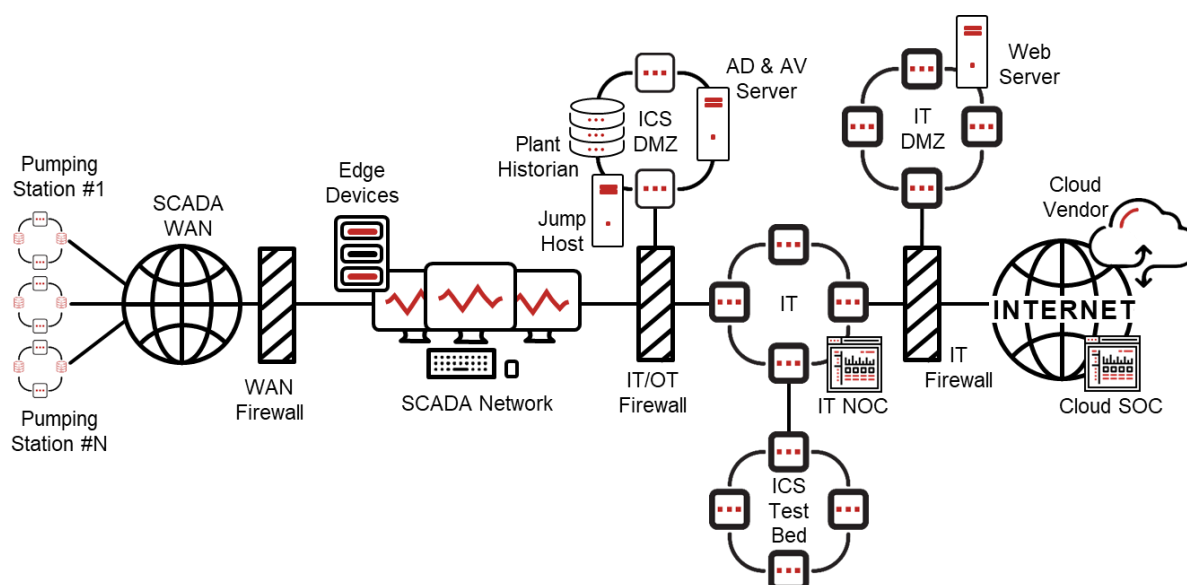


Figure (4) IIoT Water Treatment Plant Network

# IloT Attack Evaluation

The capabilities-based assessment using the top 20 attacks is repeated on the proposed IloT design for the water treatment system. The results of only two attacks change:

- 3 #3 Common Ransomware – not defeated:** Each new IloT edge device needs connections to one or more Internet/cloud services. Best practice in non-IloT installations is to configure IT/OT and other firewalls to permit connections to specific Internet IP addresses only. Since cloud services migrate across the Internet, such rules are impractical for IloT sites. The water treatment plant, like most IloT sites, therefore proposed to delete the “deny all access to the Internet” rule from their IT/OT firewall. With the proposed change, equipment on ICS networks can now reach out to Internet sites and download common ransomware.
- 12 #12 IloT Pivot – not defeated:** Unlike conventional ICS equipment, IloT edge devices communicate directly with cloud servers rather than moderate their communications through a chain of intervening DMZ networks, servers, and protocol changes. This permits attacks to pivot through vendor (cloud) Internet sites much more easily than is the case with conventional ICS components.

The DBT diagram for the proposed changes is contrasted with the original DBT diagram in Figure (5).

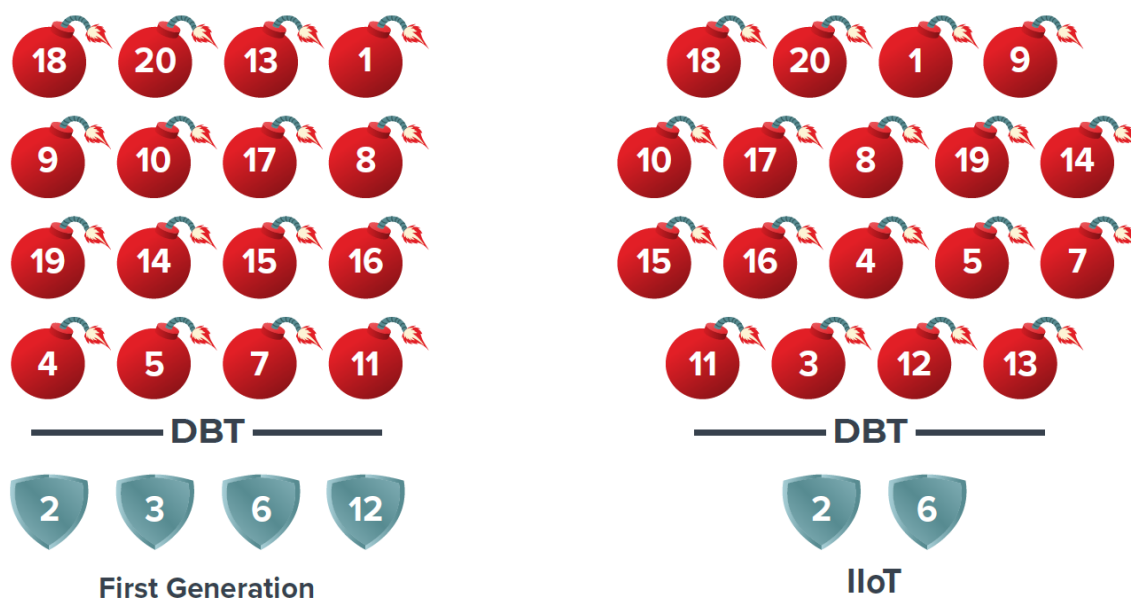


Figure (5) First-generation vs IloT Design Basis Threat

Most practitioners know instinctively that increased connectivity yields increased attack opportunities and so expect the IloT security posture to be worse than the original security posture. The DBT approach with a standard set of top 20 attacks confirms this instinct and makes the difference easily visible to nontechnical decision makers.

The water utility's business decision makers, seeing this illustration, express dissatisfaction with both the proposed and current states of security in the water treatment utility. When asked to explain these attacks that are not defeated reliably, the security team does so. Explanations of attacks generally start with the simplest attacks that are not defeated reliably, since attackers with a range of attack techniques available to them often choose the simplest, cheapest attacks that work.

No security posture is infallible – there are always attacks above the DBT line. Any site with no such attacks for their security posture either needs to define more powerful attacks or needs to consider whether the effectiveness of their security posture has been misrepresented.

Again, the business decision makers in this example express dissatisfaction, and ask the security team what can be done to improve ICS security, on a limited budget. The team then evaluates a modern design.

## Improving ICS Security

The ICS network engineering team proposes to implement a number of practices they have seen discussed in recently published government best-practice documentation: Unidirectional Security Gateways, Unidirectional CloudConnect, strict removable media controls, and security testing on the ICS test-bed:

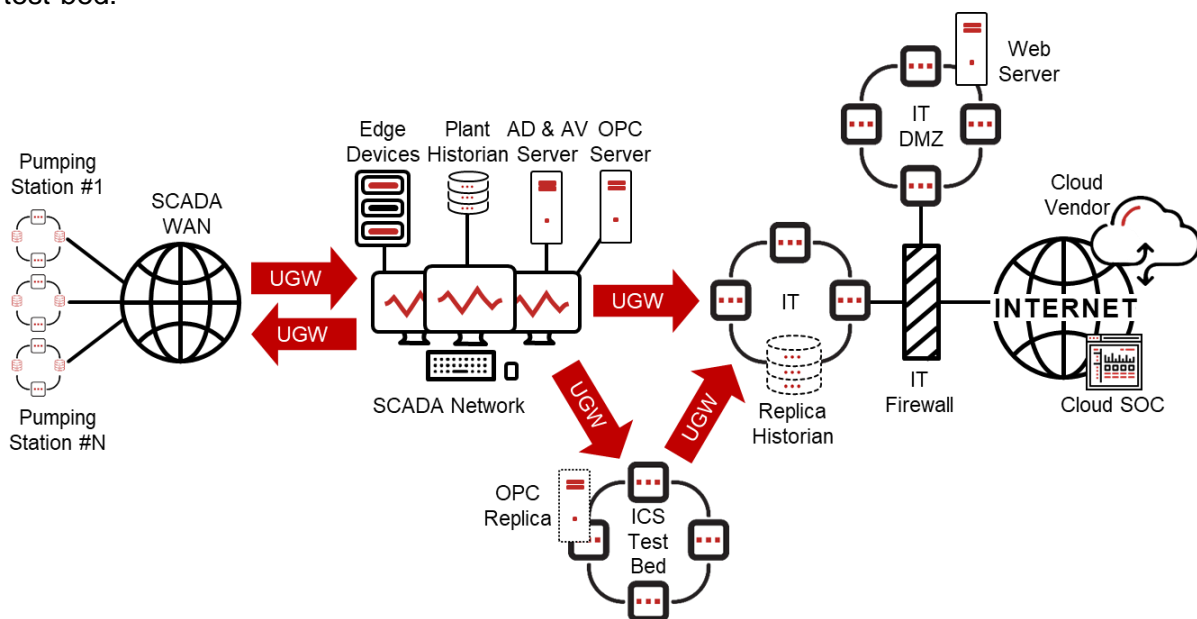


Figure (6) Modern ICS-security water treatment network proposal

- Waterfall Security Solutions' Unidirectional Security Gateways are combinations of hardware and software. The hardware is physically able to transmit information in only one direction. The software replicates servers and emulates devices, typically from ICS networks to external networks, such as corporate networks and the Internet. External users and applications interact with the replicas as if they were the original servers. Since the gateway hardware is physically able to transmit information in only one direction, a gateway deployment makes clients on the destination side of the gateway able to monitor ICS servers via the gateway's replicas, without any physical ability to control, compromise or in any way influence sensitive ICS equipment.

- Waterfall Unidirectional CloudConnect systems use Unidirectional Gateway technology to connect ICS networks directly to IT-based and Internet-based cloud services. CloudConnect systems gather data from industrial networks, including from Industrial Internet of Things (IIoT) edge devices, translate the data into cloud-friendly formats and transmit the data to cloud service providers over encrypted, reliable, Internet-friendly transports. For example, CloudConnect systems often send raw packet data and other security monitoring data to central IT and cloud-based IDS and security monitoring centers.
- Strict removable media controls mean that the ability of ICS equipment to mount, read from, and write to removable media such as USB drives and DVD's is disabled. Any attempt to use such media on an ICS asset results in security alerts and a reminder from the security team that the offending user has just breached site safety rules. An ICS file server is replicated by the Unidirectional Gateways to the IT network, so that removable media is not needed for routine tasks transferring ad-hoc files from the ICS network to the IT network. Any files that must enter the ICS network are written to removable media, scanned by eight different anti-virus engines on a stand-alone cleansing workstation, and copied to new, known-good media. That media is then transferred to a second ICS workstation that makes the new files available on the ICS file server.
- An upgraded test bed serves to test security as well as reliability of files entering a network that are complex enough to contain malware, such as ICS software updates. Such files are opened on the test bed under the gaze of a high-sensitivity malware detection system. The test bed is in every way the water utility can manage, an exact copy of the utility's ICS network. Any malware programmed to recognize hosts and activate on the ICS network, should recognize the test bed as ICS hosts, activate, and be detected. In short, the upgraded water treatment system test bed serves as both a test bed and a sandbox.











The new network is illustrated in Figure (6):

- Two independent Unidirectional Gateways are deployed at the interface to the SCADA WAN with direct connections to SCADA Communications Front End (CFE) equipment.
- Remote management of pumping station sites is still possible via remote access workstations at the water treatment plant, workstations that are electrically connected to the SCADA WAN in a badge-in secure room.
- A Unidirectional Gateway is deployed to replicate the plant historian to an IT replica, so that IT applications such as the web server have access to live industrial data.
- The reliability/security test bed is connected unidirectionally to the ICS network, meaning live data from the ICS network can be replicated to the test bed for testing and training purposes, but no malware, malfunctioning software, or errors in configuring the test/training system are physically able to send any signal to the live ICS network that might cause the water treatment plant to malfunction.
- Unidirectional CloudConnect systems are deployed to replicate network packets, logs and other security data from the ICS network and the test bed to the outsourced security monitoring provider.

The proposed defensive posture is evaluated against the 20 attacks as follows.



# Updated Attack Evaluation

-  **ICS Insider – not defeated:** None of the indicated security controls prevent an insider from issuing an inappropriate “shut down” command that the insider is authorized to issue.
-  **IT Insider – defeated:** No online message or signal from the IT network has any way to reach the control-critical network. The unidirectional gateways at the IT/OT interface are physically able to send information in only one direction – to the IT network, not from the IT network to the critical network.
-  **Common Ransomware – defeated:** No browsing of the Internet is possible through a unidirectional gateway. Strict removable media controls mean that no media-resident malware can reach control-critical equipment either.
-  **Targeted Ransomware – defeated:** No remote-control signal from the IT network or the Internet can reach any control-critical network through the unidirectional gateway.
-  **Zero-Day Ransomware – defeated:** No ransomware can defeat the unidirectional gateway’s physical protection, even with zero-day exploits. Sophisticated, AV-evading ransomware arriving on physical media is deployed first to the isolated test-bed, where the activity of the ransomware is detected by the high-sensitivity IDS either when installed or when the clock on the entire test-bed is advanced to test for time-bombed malware.
-  **Ukrainian Attack – defeated:** No remote-access or remote-control signal can penetrate the IT/OT gateway, not even with stolen passwords or stolen two-factor authentications.
-  **Sophisticated Ukrainian Attack – defeated:** No remote-access or remote-control signal can penetrate the IT/OT gateway.
-  **Market Manipulation – defeated:** No Internet-based attack can reach the unidirectionally-protected critical network.
-  **Sophisticated Market Manipulation – defeated:** No Internet-based attack can reach the unidirectionally-protected critical network.
-  **Cell-phone Wi-Fi – not defeated:** In this plan, the security team did not propose forbidding encrypted Wi-Fi zones in control-critical networks, nor did the site forbid cell phones. Scanning for such networks, phishing passwords, and connecting to the networks via compromised cell phones is still possible.

- 11 Hijacked Two-Factor – defeated:** No Internet-based attack can reach the unidirectionally-protected critical network. Remote support, when needed, can be carried out with unidirectional Remote Screen View, which makes screens from workstations on control-critical networks visible to web browsers on external IT and Internet networks. Such visibility though, confers no ability for the remote user to control the critical workstations. Control must be carried out by insiders with access to the indicated workstations' mice and keyboards, usually with a voice connection to external support personnel who provide verbal advice to site personnel, based on the contents of the live screen images replicated to the support provider.
- 12 #12 IIoT Pivot – defeated:** No Internet-based attack can reach the unidirectionally-protected critical network.
- 13 #13 Malicious Outsourcing – defeated:** No attack from any external vendor network can reach the unidirectionally-protected networks. Again, any vendor access to a critical network is via Remote Screen View. Engineers at the site will schedule the execution of software into the future on multiple machines only when they have a clear understanding of the reason for, and consequences of, such execution.
- 14 #14 Compromised Vendor Website – defeated:** All new vendor software is deployed first on the reliability/security test bed. In this attack scenario, the software detects that it has been installed on what appears to be a fully-functional industrial network. When the clock on the test bed is advanced, the malware activates, erasing hard drives. The test bed is quickly restored from backup images, with no harm done to the critical network.
- 15 #15 Compromised Remote Site – defeated:** The unidirectional gateway replicating SCADA system instructions to remote sites across the SCADA WAN is not physically able to transmit any attack information back into the control-critical network. The gateway oriented to monitor remote sites is unable to open new connections from a compromised remote site into the critical network – the gateway is a client of devices at remote sites, not a server that forwards arbitrary attack files, or a firewall or router that forwards arbitrary attack packets.
- 16 #16 Vendor Back Door – defeated:** Unidirectional gateways are not routers, are unidirectional, and for both reasons are unable to propagate TCP connections from malware on control-critical devices to command and control centers, whether or not those control centers are part of ICS-vendor websites.
- 17 #17 Stuxnet – not defeated:** The consequences of malware such as the historical Stuxnet worm may not be visible on test-bed networks, however faithfully those test beds try to emulate an ICS environment. The consequences of Stuxnet were visible only in the physical process.
- 18 #18 Hardware Supply Chain – not defeated:** Malicious behaviour of new equipment might be observed by the high-sensitivity IDS on the test-bed network. However, attackers who know this test bed exists might also know how long new equipment is tested on the test-bed before being deployed into production. Attackers could simply delay their use of malicious hardware until they are confident that the hardware has passed test and is deployed on the production SCADA system.

**19 #19 Nation-State Crypto Compromise – defeated:** Protections for the ICS network are physically unidirectional, not software-based, or cryptographic.

**20 #20 Sophisticated Credentialed ICS Insider – not defeated:** It is very difficult to reliably defeat compromised insiders who are cooperating with sophisticated attackers.

A DBT summary for the analysis above is compared to the summaries from the first-generation and IloT security postures in Figure (7). The improved security program reliably defeats a much larger set of attacks than does the original program. Residual risks in the new DBT are all risks that require physical access to the SCADA site, or very costly and sophisticated attacks from the most sophisticated of nation-state-grade adversaries.

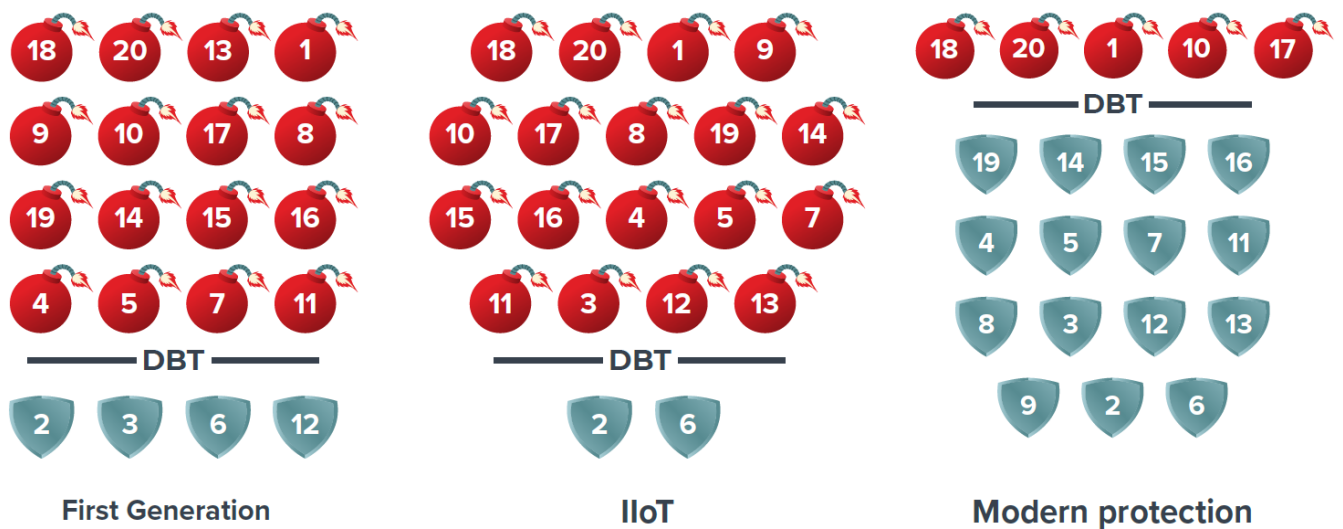


Figure (7) Water treatment system example – three different security postures

In this example, business decision-makers can easily see and understand the improvement in the proposed security posture. This makes it easier for these decision-makers to decide which risks are acceptable and which justify authorization and funding for security program changes.

# Summary

A given security program/posture can only be evaluated if we have a clear understanding of the kinds of attacks that might target the protected industrial site. This paper:

- Proposes a representative Top 20 list of ICS cyber attacks
- Illustrates how to evaluate those attacks against a given defensive posture, and
- Illustrates how to communicate residual risk to business decision-maker as a Design Basis Threat line drawn through example attacks.

Nothing is ever completely secure - any DBT diagram should illustrate attacks that will breach the defensive posture under consideration. In any such set of not-reliably-defeated attacks, there is always a least-sophisticated or simplest attack or set of attacks with serious consequences. It is this set that should be the focus of communication with business decision-makers. Do such attacks represent acceptable risks?

When the answer is “no” we can evaluate attacks above the DBT line against proposed new security measures to see whether the line moves. In the water treatment system example, we see how a modest investment in modern ICS protection with Unidirectional Gateway and removable media controls protections produces a dramatic improvement in risk posture.

## About Waterfall Security Solutions

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall's products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases, and protocols in the market. For more information, visit [www.waterfall-security.com](http://www.waterfall-security.com).

Waterfall's products are covered by U.S. Patents 7,649,452, 8,223,205, and by other pending patent applications in the US and other countries. “Waterfall”, the Waterfall Logo, “Stronger than Firewalls”, “In Logs We Trust”, “Unidirectional CloudConnect”, and “CloudConnect, and “One Way to Connect” are trademarks of Waterfall Security Solutions Ltd. All other trademarks mentioned above are the property of their respective owners. Waterfall Security reserves the right to change the content at any time without notice. Waterfall Security makes no commitment to update content and assumes no responsibility for any mistakes in this document.