THE TOP 20 CYBERATTACKS

on Industrial Control Systems

Andrew Ginter, VP Industrial Security, Waterfall Security Solutions

Version 1.1, May 2018

CONTENTS

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 attacks. 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 ICS Insider	

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

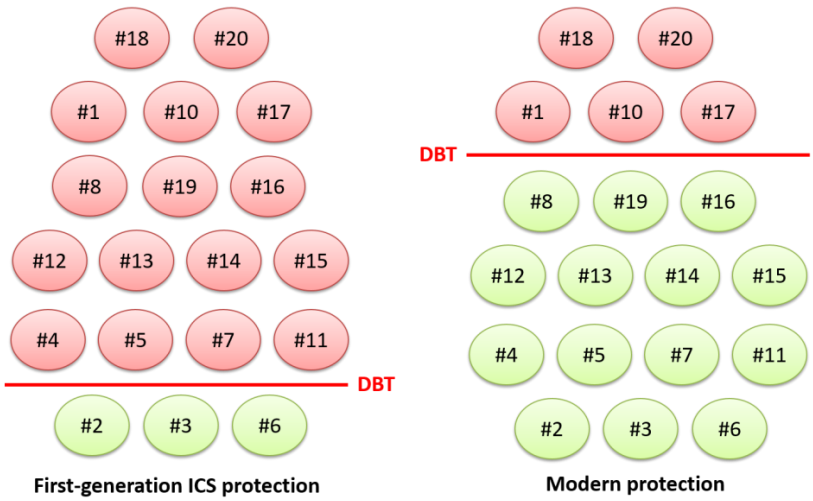

Figure (1) Water treatment system example – two different security postures

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 to this organization, 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 if given specific examples of cyber attacks, 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, with the Top 20 set representing 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 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 measures will cost.

TO DEFEAT RELIABLY

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:

- Anti-virus systems (AV) do not defeat common malware reliably, because attacks are launched into the wild before anti-virus signatures are available for the attacks. If common malware reaches a vulnerable system between the time of malware launch and the time that AV signatures are applied, the system is compromised, even though an AV system is deployed.
- Security updates do not defeat exploits of known vulnerabilities reliably because it takes time for a vendor to create, and end users to install, the updates. Systems are vulnerable in this time interval. 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 (IDS) and security monitoring systems are detective measures, not preventive. Since no set of preventive measures is ever perfect, cyber-security best-practice documents generally all recommend detection and monitoring systems – to understand what activity is normal on a network, to detect as reliably as possible abnormal activity and to trigger incident response actions when suspicious activity is detected. IDS and monitoring systems though, important as they are, do not defeat attacks reliably. This is because intrusion detection and incident response take time. In that time, compromised equipment is being operated either manually by a remote attacker, or automatically by autonomous malware, which may be enough to bring about the consequences we seek to prevent.

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

- Phishing attack for password theft - two-factor authentication based on RSA-style password dongles reliably defeats remote password phishing attempts. One could postulate an attack that physically steals the password dongle, but that would no longer be a “phishing” attack. A distant attacker only able to forge email and produce look-alike websites is not able to defeat this kind of two-factor protection system.
- Encryption key scraping software - trusted platform modules (TPMs) reliably defeat attempts to search compromised equipment’s memory and persistent storage to steal encryption keys. TPM hardware is designed such that encryption keys never leave the hardware modules or 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 – i.e. software searching a machine's memory and hard drive for keys.
- Internet-controlled malware - Unidirectional Security Gateways reliably defeat Internet-controlled malware. The gateways are physically able to send information in only one direction – from an ICS 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, determining that a given security posture defeats a particular attack reliably can be challenging. “Defeats reliably” is a high standard. Achieving this standard is generally possible only by describing a particular attack, or attacker's capabilities, very specifically.

THE TOP 20 ATTACKS

The proposed Top 20 attacks are listed below, in roughly least-sophisticated to most-sophisticated order. The list represents a wide range of industrial cyber attacks useful to compare security postures between sites and between defensive systems. 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 Top 20 list below 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 of the attacker. 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 attacks 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 to design and run their attack? Do the attackers have inside assistance? Or can they operate the entire attack from outside of their target organizations?

Consequences are primarily physical states of the industrial system that we are trying to avoid, and secondarily changes in control system computers. Physical consequences are most often one of: impaired or poor-quality production, unexpected shutdown of the physical process, damage to physical equipment, injury to workers at the industrial site, or threats to public safety

The Top 20 ICS cyber security attacks are:

#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 shut-down instructions to parts of the physical process, automatically triggering a partial plant shut-down. *Sophistication*: This is a moderately sophisticated attack. ICS technicians tend to have 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 designed into industrial processes. *Consequences*: This class of incident is most often able to cause partial or complete plant shutdowns. 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 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 more or less at random, and presses whatever buttons seem likely to cause the most damage or confusion. These actions trigger a partial plant shut-down. *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 shut-down or might just cause confusion. At best, each such incident triggers an engineering review of settings at the plant, to ensure that no physical equipment has been left mis-configured 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 of the Windows hosts on the industrial control system. Most Windows hosts in the industrial network are encrypted, 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. The emergency shutdown procedure damages important equipment at the plant, impairing production for months, even after the ransomware has been cleaned out of the control system and the plant is restarted. A variation of this attack: ransomware infects an IT workstation and spreads via AUTORUN files on network shares, USB drives, and known network vulnerabilities for a number of days, before triggering the encryption. A number of 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 is able to spread quickly and automatically through a network, and even malware that is able to evade common anti-virus 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 though, important equipment can be irreparably damaged by an uncontrolled shutdown. In this case, replacements for the damaged equipment need to be purchased and installed, and where replacements are not readily available, replacements for damaged equipment must themselves be manufactured, so they can be installed and activated. Worst-case plant downtime in these 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, damaging equipment. It takes a month to replace and reprogram damaged control system computers, and more months before damaged physical equipment is replaced. *Sophistication*: The attacker is cyber-sophisticated. Increasingly, we see organized crime organizations becoming involved with ransomware. These organizations have access to professional-grade malware toolkits and developers, and professional-grade 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.
#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 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 to infect and

	encrypt the industrial site, causing an emergency shutdown and damaging physical equipment. *Sophistication*: Cyber attacks only become more sophisticated over time. Security researchers and others discover zero-day vulnerabilities, and intelligence agencies have been known to "lose track" of the zero days they have discovered or purchased. This attack was very sophisticated cyber-wise, and 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 have learned what many of the screens and controls do. At that time, the group takes over the HMI and uses it to mis-operate the physical process. At the same time, co-attackers use the administrative credentials to log into ICS equipment, erase the hard drives, and where practical, erase the equipment firmware. *Variations*: When targeting other kinds of industries, similar attacks are possible, erasing control system equipment, and triggering unplanned shutdowns. *Sophistication*: This is a summary of the attack techniques used in the 2016 attack on a number of Ukraine electric distribution companies. The attackers had good knowledge of cyber systems, but limited knowledge of electric distribution processes and control systems. *Consequences*: In the case of the attacks on Ukraine, power was shut off to over 200,000 people, for up to 8 hours. Power was only restored when technicians travelled to each of the affected substations, disconnected control system computers, and manually 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 more sophisticated group of attackers used the techniques of the Ukraine attack, and are more sophisticated with respect to cyber-attack tools and the engineering details of electric systems. In addition to the actions of attackers in the UKRAINE ATTACK scenario, the more sophisticated group uses compromised IT domain controllers to defeat two-factor authentication, connects to protective relays and reconfigures them, effectively disabling the relays. The group now very quickly connects and disconnects power flows to the affected consumers, damaging refrigerators, sump pumps, and other motors in consumers' homes and businesses. 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. Many large refrigerators in grocery stores have been rendered inoperable, large water pumps in water distribution systems are similarly damaged, and a large number of smaller pieces of equipment in consumers' homes are rendered inoperable. High voltage transformers must be replaced on an emergency basis, which takes over a week. There is no world-wide inventory of such transformers, so while replacement transformers are manufactured, emergency replacements are acquired by 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 gain 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 via 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 single, 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 - e.g.: gasoline. The plant shuts down for emergency repairs, 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 affected commodity spike on commodities markets. When plant production at all plants returns to normal, commodity prices return to normal. This attack is repeated in the next season of high demand. *Sophistication*: Cyber-sophistication of this attack and these attackers is moderate - no zero-days were used, and no code was written. 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 that equipment, download the existing program of that PLC, and design and upload a new program able to wear out the targeted physical equipment prematurely, while reporting to the HMI that the equipment is operating normally. *Consequences*: Lost plant production and emergency equipment repair costs.
#9 Sophisticated Market Manipulation	More cyber-sophisticated attackers carry out the market manipulation attack, but in a way that is harder to defend against. 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 anti-virus tools cannot detect the RAT. The attackers use the RAT to

	compromise the laptops of personnel who routinely visit the real target. When they 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, and 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*: Cyber-sophistication of this attack and 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 high. *Consequences*: Lost plant production and emergency equipment repair costs.
#10 Cell-phone WIFI	Sophisticated attackers seek to inflict damage on a geography they are unhappy with for some reason. The attackers create an attractive cell phone app - call it the world's fanciest free flashlight app. The attackers use targeted social media attacks to persuade office workers at critical infrastructure sites in the offending geography to download the app, which requests more permissions than a flashlight app should really request, but these workers are not cyber-sophisticates and think nothing of it. 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 WIFI 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 the target organization, and extract passwords for the WIFI 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 look around the networks 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, disconnect from the WIFI networks, and repeat a few days later. *Variation*: Plant malware on the laptops of office workers who work within range of ICS WIFI networks. *Sophistication*: This attack currently needs a high degree of cyber-sophistication, because toolkits enabling this kind of hidden WIFI hacking from cell phones currently do not exist on the open Internet, and so attackers need to write this malware themselves, or buy it. Once such attack tools are widely and publicly available, this class of attack will come within the means of hacktivist groups annoyed 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 should eventually determine that the source of the

	attack is a WIFI network and shut down all WIFI 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. So, they write custom RAT malware to evade anti-virus systems, and target support technicians at the industrial site using social media research and targeted phishing emails. The 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 laptops screen, and shows the technician a useful error message along the lines of "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 the ICS IDS sees is the technician logged in twice. The attackers eventually learn enough about the system to mis-operate the physical process enough to seriously damage 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, likely requires a high degree of engineering sophistication as well. *Consequence*: Any attacker willing to invest sophisticated, custom malware in this kind of attack is most likely going to persist in the attack until significant adverse outcomes are achieved.
#12 IIoT Pivot	Hacktivists annoyed 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 particular vendor. The attackers search the media to find other users of the same components, at smaller and presumably less-well-defended sites. The hacktivists target these sites with phishing email and gain a foothold on the IT and ICS networks of the most poorly-defended of these IIoT-using sites. The hacktivists gain access to the vendor's IIoT equipment at the sites and discover that the operating system for these devices is an older version of Linux, with many known vulnerabilities. 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 exploit for that database vendor. They discover that the cloud vendor has not yet applied a security update for that vulnerability and they 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 hacktivists 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 in this edge device. The hacktivists use this facility to send commands and standard attack tools and other software to the edge devices in those ICS networks the hacktivists regard as environmentally-irresponsible targets. Inside those networks, the attackers use these tools and remote-command facilities to look around for a time and eventually erase hard drives or cause what other damage they can, triggering unplanned shutdowns. In short, hacktivists 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 usually have a very limited degree of engineering sophistication. *Consequences*: Unplanned shutdowns, lost production, and possible equipment damage.
#13 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 world-wide remote support center in a country with an adequate supply of adequately-educated personnel, and low labor and other operational costs. A poorly-paid technician at this support center finds a higher-paying job elsewhere, and before leaving, decides to take revenge on personnel at a particular industrial site - personnel who complained to the technician's manager about the technician's performance. The technician uses her legitimately-acquired remote access and two-factor credentials, and the VPN to the targeted site to gain access to the site. The technician logs into all of the computers she has access to, and leaves a tiny script running on each that, one week later, erases the hard drives on each computer. *Sophistication*: This is an adversary with limited cyber sophistication, or 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*: 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 likely trigger the loss of the current batch, since many such plants store their batch records in the historians and are unable to sell product for batches whose records are impaired. Such batches can range in value from hundreds of thousands of dollars to hundreds of millions of dollars.
#14 Compromised Vendor Website	Most of us trust our ICS vendors - but should we trust their websites? Hacktivists find a poorly-defended ICS vendor website and compromise it. They download the latest copies of the vendor software and study it. In particular, they learn where in the system the name or some other identifier for the industrial site is stored. These attackers then determine which of the industrial enterprises that the attackers are currently annoyed with are identified in public media as users of this 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 re-pack 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. *Sophistication*: This is a hacktivist-class attack, by attackers of moderate cyber sophistication, and limited engineering sophistication. The attackers did know enough about computer systems to use existing tools, permissions and vulnerabilities. They did have enough knowledge to unpack control system products and understand to some degree how they work, as well as unpack and re-pack security updates. *Consequences*: Most often, the consequences of this class of attack is an unplanned shutdown. However, if enough of the control system is affected by a simultaneous shutdown, the failure may trigger an uncontrolled shutdown which in many industries risks equipment damage.
#15 Compromised Remote Site	SCADA systems are control systems that use wide-area-network communications, such as power grids and pipelines. In such systems, remote sites such as substations and pumping stations are typically unstaffed, with limited physical security, such as a wire fence, locks and perhaps video surveillance. In this scenario, an attacker physically cuts the padlock on a wire fence around a 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. He walks over to the only rack in the site, plugs a laptop into the switch, and tapes it 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 WIFI, 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. She then uses Ukraine-style techniques to cause physical shut-downs. *Sophistication*: This attack requires physical access to at least one of the remote sites, and an investment of physical risk, as well as equipment - the laptop. Hacktivist-class cyber expertise is needed to break into the remote site and 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 remote station 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 liquids pipelines, can result in pressure waves able to cause pipeline breaches and leaks.
#16 Vendor Back Door	A software developer at a software vendor inserts a back door into software used on industrial control systems networks. This may be ICS software, or it may be driver, management, operating system, networking, or other software used on the ICS network. The back door may have been installed with the blessing 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. Hacktivist-class attackers discover this back door, compromise the vendor's software-update website with a password-phishing attack on the vendor, and use the back door to impair operations at industrial sites belonging to enterprises the hacktivists have imagined they have some complaint against. Note that anti-virus systems are unlikely to discover this back door, since this is not the autonomously-propagating kind of malware 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. *Consequences*: Plant shutdowns and erased hard drives are easy to bring about by hacktivist-class attackers who have carried out this kind of attack. More engineering-sophisticated attackers can most likely cause equipment damage, and sometimes even put worker safety or public safety at risk.

	Sophistication: To write the back door into the vendor's product source code, and into the update web site's source code, takes an intermediate degree of cyber sophistication. Such source code is of course well within the abilities of software developers working for the vendor though, since such developers are typically hired to produce code that is much more complex than what is needed for this kind of back door. A moderate degree of cyber sophistication is required of the hacktivists who discovered the back door. Only limited engineering sophistication is needed to bring about a plant shutdown. Greater sophistication is needed to bring about equipment damage and safety-impairing scenarios.
#17 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 that one site, and bring about physical damage to equipment at the site. The autonomous malware exploits zero-day vulnerabilities. Services providers carry the malware to site on removable media. Anti-virus scanners are blind to the custom, zero-day-exploiting malware. *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 equipment, and could bring about loss of life, public safety risks and costly equipment damage. *Sophistication*: This class of attack demands high degree of engineering sophistication, to understand the physical process and control system components, and bypass equipment protection and safety systems with an attack. The attack demands a high degree of cyber sophistication as well, to encode that new attack into custom malware that is undetectable by the specific cyber security technologies deployed at the target site.
#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 that equipment to the site. The attacker then develops a relationship with the delivery drivers in the logistics organization, routinely paying the driver modest sums of money to take 2-hour lunch breaks, instead of 1-hour breaks. When IT intelligence indicates that a new shipment of computers is on its way to the industrial site, the agency uses the 2-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 then re-package 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 string of very unfortunate, random, equipment failures. *Consequences*: Costly equipment failures and plant production far below targets. *Sophistication*: This is an attack be a very sophisticated adversary. This attacker has the physical "feet on the street" to carry out covert actions, such as breaking into the delivery van, and quickly disassembling, modifying, re-assembling, and re-packaging 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 enough to understand 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 enough to design and carry out physical sabotage and making damaged equipment look like random failures.
#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 the certificate. The attacker compromises Internet infrastructure to intercept connections from the site to software vendors and deceives the site into downloading malware with what appears to be legitimate vendor signatures. The malware sets up peer-to-peer communications 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. *Consequences*: Public safety risks and possible loss of life, costly equipment damage and lost production. *Sophistication*: This is a very sophisticated adversary able to defeat the encryption, certificates, signing and cryptographic hashes that are the foundation of many security programs.
#20 Sophisticated Credentialed ICS Insider	A sophisticated attacker bribes an ICS insider at an industrial site. The insider systematically leaks information to the attackers about the design of the physical process, and of the industrial control system. The attacker develops custom, autonomous malware. 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 a number of workers, causes a billion dollars in damage to the plant, and shuts the site down for 12-18 months. *Consequences*: Loss of life, costly equipment damage and lost production. *Sophistication*: This is an attacker with a high degree of sophistication in physical operations, to bribe the insider, a high degree of engineering sophistication to determine what cyber attack has not been anticipated by the site's safety and equipment protection systems, or to determine how to defeat those protections, and a high degree of cyber sophistication to produce undetectable, custom, autonomous malware.

WATER TREATMENT SYSTEM EXAMPLE

Consider a water and wastewater treatment system. Cybersecurity priorities for the site include:

1. Do not kill or injure anyone at the site. Safety hazards include large reservoirs and pipes able to fill with water, whether or not personnel are in the way, and large, toxic reservoirs of chlorine gas and fluoride solutions.
2. Do not route unclean water into the water distribution system in quantities that puts public safety at risk, or triggers “boil water” advisories.
3. Manage reservoirs, pumping and treatment systems such that clean drinking water is available in quantities, costs and according to schedules that comply with service-level agreements with the water distribution system.

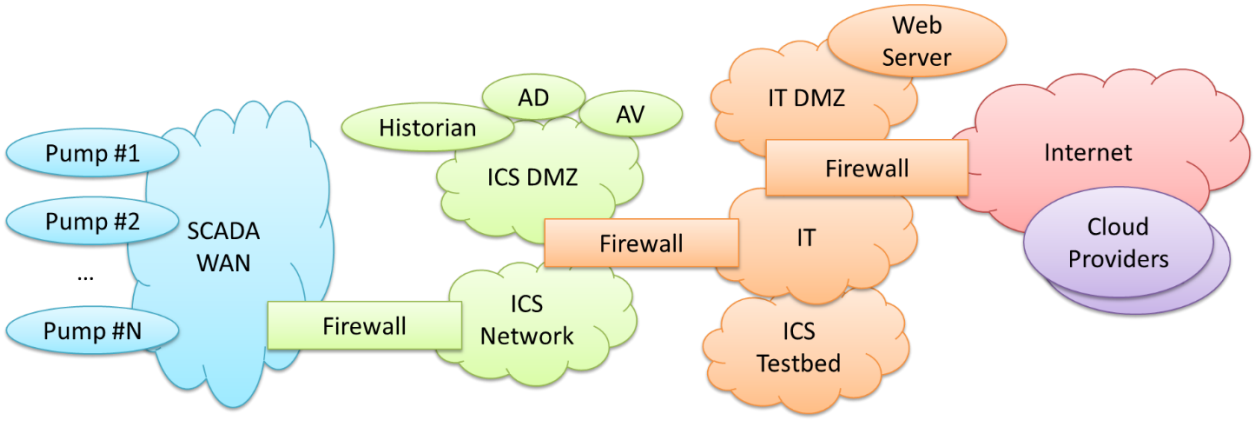

Figure (2) First-gen ICS best-practice water treatment network overview

A water treatment control system is protected to first-generation ICS security best practices, published roughly 2003-2013:

- Firewalls separate networks at grossly different levels of trust,
- Encryption is enabled on all IT and ICS equipment and connections that support such,
- Individual user accounts and passwords are set up on all equipment that supports such, with only the usual exceptions in the ICS space, e.g.: 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 on shift change,
- The pumping station SCADA WAN is private, leased telecoms infrastructure,
- A DMZ separates the ICS from IT networks, containing a remote-access jump host, plant historian, and plant AD, AV and other servers synchronized to the IT AD servers,
- A comprehensive security update program is in place. Industrial plant systems cannot be updated as quickly as can IT systems, because comprehensive testing of the updates on a reliability test-bed takes a long time, most control system networks are not updated automatically.
- Anti-virus systems are deployed on all equipment that supports 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 from switch span and mirror ports are fed into a large network intrusion detection analysis engine on the IT network, and

- Logs, AV alerts, IDS alerts, and other security information is sent directly from ICS equipment, through the DMZ, IT and Internet networks to a third-party cloud security monitoring and analysis service.

Third-party service providers have remote access credentials and can log into IT networks and from IT networks into ICS networks via a DMZ jump server. Policies, procedures, responsibilities and training have been documented and executed according to IT best practices. Figure (2) is a high-level network diagram for the utility.

ATTACK EVALUATION

Evaluating the twenty example attacks against the above system yields the results below. In the table 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 equipment configured to run "AUTORUN" files.
#4 Targeted Ransomware	Not Defeated	Two-factor authentication might prevent the attacker from pivoting through the IT network into the ICS network, but a targeted remote-control attack of even moderate sophistication 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 detect the attacker, it depends 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.
#5 Zero-Day Ransomware	Not Defeated	The site has a file sharing server set up in the DMZ to minimize 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 anti-virus signatures have been updated or the firewall sandbox security updates are in place, the site will be compromised.
#6 Ukrainian Attack	Defeated	A hacktivist-class attack relies on stolen passwords and known vulnerabilities in network-exposed services. None such are exposed in the water system's architecture.

#7 Sophisticated Ukrainian Attack	Not Defeated	Two-factor authentication might prevent the attacker from pivoting through the IT network into the ICS network, but a targeted remote-control attack of even moderate sophistication 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 detect the attacker, it depends 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.
#8 Market Manipulation	Not Defeated	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 update yet exist. 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 so 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, it depends 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 WIFI	Not Defeated	IT best practices do not forbid encrypted WIFI zones in ICS networks. IT best practices are no guarantee that permissions on ICS networks prevent logging into equipment with stolen passwords and erasing hard drives. Intrusion detection systems might report on unusual WIFI connections to ICS WIFI networks, but identifying the source of such connections can be difficult and time-consuming. It is not clear that 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 anti-virus 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 jump host, through the jump host to the control system, and manipulating the operation of the control system. All of this is normal.
#12 IIoT Pivot	Not Defeated	Unlike conventional ICS equipment, IIoT edge devices communicate directly with cloud servers rather than moderate their communications through a chain of intervening DMZ networks and other servers as do conventional ICS

		communications. This permits attacks to pivot through vendor (cloud) Internet sites much more easily than is the case with conventional ICS components.
#13 Malicious Outsourcing	Not Defeated	Vendor technicians using their permissions to log into ICS servers is a permitted activity. Such technicians carrying out minor reconfiguration of the ICS servers they have passwords for is also permitted, and normal, from the perspective of intrusion detection systems. At the water system, the most likely consequence of this class of attack depends on the type of outsourcing. For outsourced historian management, the consequence is some cyber cleanup. For outsourced control system management, the central technician may well understand enough about the control system and physical process to configure more serious consequences, such as a script to persistently send shutdown commands to pumps all night long, resulting in drinking water reservoirs empty in the morning, which should have been full and ready for the day's load.
#14 Compromised Vendor Website	Not Defeated	Anti-virus 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 behavior 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. Or the firewall might be configured very cautiously, permitting almost no connectivity with the central site. 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, anti-virus 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 WIFI clients. Host-based protections on existing

		hosts cannot prevent this kind of supply chain attack from introducing new CPUs, hosts and WIFI 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, all bets are off.
#20 Sophisticated Credentialed ICS Insider	Not Defeated	It is very difficult to reliably defeat compromised insiders fronting for sophisticated attackers.

Given the analysis above, the DBT for this set of attacks and this target can be illustrated as in Figure (3).

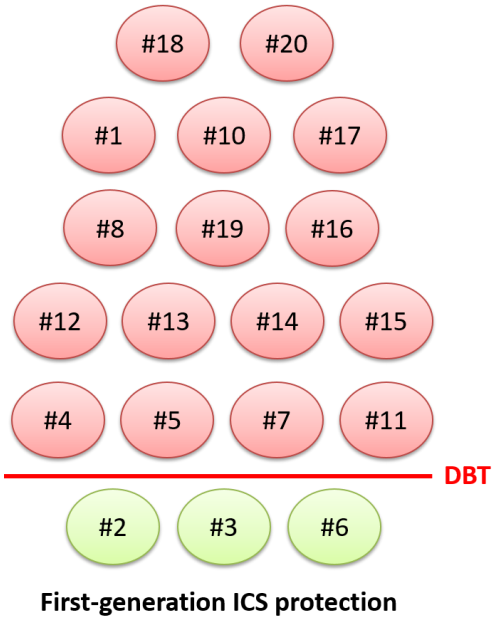

Figure (3) Design Basis Threat for first-generation ICS security program

The water utility's business decision makers, seeing this illustration, express dissatisfaction with the state of security in the water treatment utility. They may ask "what are these attacks that are not defeated reliably?" We as security practitioners should explain to them attacks not defeated reliably, as well as any attacks they show special interest in. When we explain attacks, we 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 that we can talk to management about. Any practitioner who sees no such attacks for their security posture either needs to define more powerful attacks or needs to think hard about whether they have misrepresented the effectiveness of their security posture.

Again, 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.

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:

- 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.

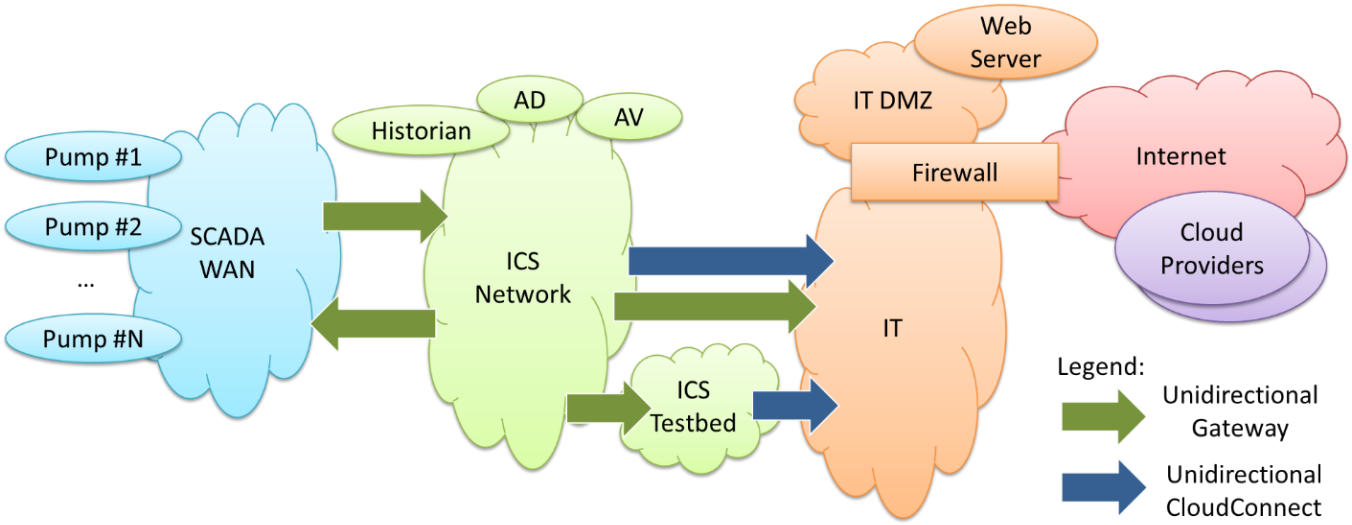

Figure (4) Modern ICS-security water treatment network proposal

The new network is illustrated in Figure (4):

- 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

#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.	Unchanged

#2 IT Insider	**Defeated**	No online message or signal from the IT network has any way to reach the ICS network any more. The Unidirectional Security Gateway at the IT/OT interface are physically able to send information in only one direction - to the IT network, not to the ICS network.	Unchanged - still defeated, but because of Unidirectional Gateway now, not two-factor authentication.
#3 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 sensitive ICS equipment either.	Unchanged - still defeated, but because of Unidirectional Gateway & removable media controls now, not firewall rules & AUTORUN policies
#4 Targeted Ransomware	**Defeated**	No remote-control signal from the IT network or the Internet can reach the ICS network through the Unidirectional Gateway.	Changed to defeated
#5 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.	Changed to defeated
#6 Ukrainian Attack	**Defeated**	No remote-access or remote-control signal can penetrate the IT/OT gateway.	Unchanged – still defeated, but because of Unidirectional Security Gateways now, not two-factor authentication
#7 Sophisticated Ukrainian Attack	**Defeated**	No remote-access or remote-control signal can penetrate the IT/OT gateway.	Changed to defeated
#8 Market Manipulation	**Defeated**	No Internet-based attack can reach the unidirectionally-protected ICS.	Changed to defeated

#9 Sophisticated Market Manipulation	**Defeated**	No Internet-based attack can reach the unidirectionally-protected ICS.	Changed to defeated
#10 Cell-phone WIFI	**Not Defeated**	IT best practices do not forbid encrypted WIFI zones in ICS networks. IT best practices are no guarantee that permissions on ICS networks prevent logging into equipment with stolen passwords and erasing hard drives. Intrusion detection systems might report on unusual WIFI connections to ICS WIFI networks, but identifying the source of such connections can be difficult and time-consuming. It is not clear that all attacks of this class will be reliably detected and remediated in time to prevent consequences.	Unchanged
#11 Hijacked Two-Factor	**Defeated**	No Internet-based attack can reach the unidirectionally-protected ICS. Remote support, when needed, can be carried out with unidirectional Remote Screen View, which makes screens from workstations on ICS networks visible to web browsers on external IT and Internet networks. Such visibility though, confers no ability for the remote user to control the ICS workstations though. 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 image replicated to the support provider.	Changed to defeated
#12 IIoT Pivot	**Defeated**	No Internet-based attack can reach the unidirectionally-protected ICS.	Changed to defeated
#13 Malicious Outsourcing	**Defeated**	No attack from any external vendor network can reach the unidirectionally-protected ICS.	Changed to defeated

#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 targeted ICS 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 unidirectionally-protected ICS network.	Changed to defeated
#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 ICS network. The gateway oriented to monitor remote sites is unable to open new connections from a compromised remote site into the ICS network - the gateway is a client of devices at remote sites, not a server, or a router.	Changed to defeated
#16 Vendor Back Door	**Defeated**	Unidirectional Security Gateways are not routers, and are unidirectional, and are for both reasons unable to propagate TCP connections from ICS-resident malware to command and control centers, whether those control centers are in ICS vendor websites or not.	Changed to defeated
#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.	Unchanged
#18 Hardware Supply Chain	**Not Defeated**	Malicious behavior 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 know they are on the production system, and not the test bed.	Unchanged

#19 Nation-State Crypto Compromise	**Defeated**	Protections for the ICS network are physically unidirectional, not software-based or cryptographic.	Changed to defeated
#20 Sophisticated Credentialed ICS Insider	**Not Defeated**	It is very difficult to reliably defeat compromised insiders fronting for sophisticated attackers.	Unchanged

A comparison of the DBT for the analysis above, and the analysis from the original security posture is illustrated in Figure (5). The modern best-practice security program reliably defeats a much larger set of attacks than does the original first-generation 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 nation-state-grade adversaries.

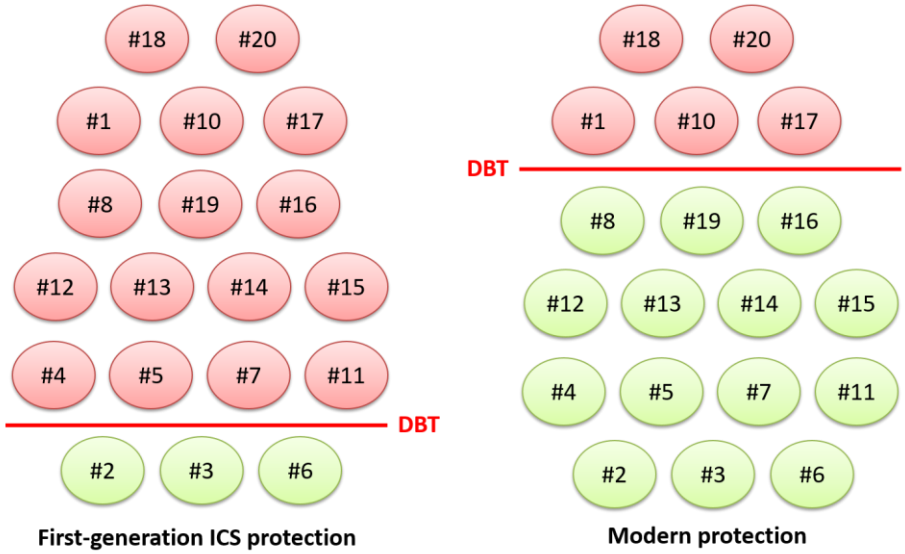

Figure (5) Water treatment system example – two different security postures

In this example, business decision-makers can see and understand the improvement in the proposed security posture. This makes it easier for these decision-makers to decide whether risks are acceptable, and when appropriate, authorize 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