WATERFALL®
Stronger Than Firewalls

Written by
Edward Amoroso
& Andrew Ginter

OT SECURITY FOR IT PROFESSIONALS :

AN INTRODUCTION TO INDUSTRIAL CYBER CONTROLS

As a globally recognized expert in the field of industrial control systems security, Andrew Ginter often observes that a common approach to industrial cybersecurity is to protect operational technology (OT) with the same tools and approach as we use when we protect information technology (IT). Demystifying this concept is the topic handled in this series of articles. Recruiting Dr. Edward Amoroso – a veteran cyber and information security professional, professor and author - these two savvy professionals sat down and wrote a series of articles that every IT professional charged with industrial cyber controls should read.

"Learning operational technology security in the context of the Internet of Things is not particularly difficult," Dr. Amoroso explained, "but does require a slightly different mindset than is required for traditional cyber security".

PROGRAM OUTLINE

ARTICLE #1

AN OVERVIEW OF THE OT/ICS LANDSCAPE FOR CYBER PROFESSIONALS

Most cyber security professionals take for granted the *information technology* or *IT* nature of their work. That is, when designing cyber protections for some target infrastructure, it is generally presumed that protections are required for software running on computers and networks. The question of whether some system is *digital* or even *computerized* would seem to have been last relevant to ask in 1970. We all presume that everything is software on CPUs.

The problem is that not everything is software that CPUs control. Cars include mechanical parts that can get only *so hot*; airplanes have wings that can bend only *so far*; factories include assembly lines that can go only *so fast*; and power plants include fluid piping that can only handle *so much*. These tangible entities consist of solids, liquids, and gases, rather than 1's and 0's, so their management requires a different type of component called an *industrial control system* or *ICS*.

> WHEN DESIGNING CYBER PROTECTIONS FOR INFRASTRUCTURE, IT IS GENERALLY PRESUMED THAT PROTECTIONS ARE REQUIRED FOR SOFTWARE RUNNING ON COMPUTERS AND NETWORKS.

The supporting ecosystem that enables industrial control is referred to collectively as *operational technology* or *OT*, and this introduces a new set of cyber security concerns. OT protection is particularly intense, because the physical consequences of compromise may be completely unacceptable, and because many of the security mechanisms that are second nature on IT networks can in fact impair physical operations as badly as a cyberattack. This leads to both puzzles and headaches for cyber security engineers.

Cyber security engineers have thus begun the journey of trying to determine how to apply the best elements of IT security, learned through practical experience over the past three decades, to the OT management and monitoring of ICS. In many cases, IT insights are directly applicable to OT/ICS security; but situations do emerge where the nature of industrial control infrastructure introduces novel malicious threats that require innovative new cyber solutions.

SAFETY AND SECURITY IN OT

The intimate relationship between security and safety concerns in OT environments cannot be understated. Recall, in contrast, that IT security experts will reference the traditional confidentiality, integrity, and availability (CIA) model of threats. The goal of IT security thus becomes putting functional or procedural controls in place that will cost-effectively reduce the CIA-type risks to data assets.

> **THE INTIMATE RELATIONSHIP BETWEEN SECURITY AND SAFETY CONCERNS IN OT ENVIRONMENTS CANNOT BE UNDERSTATED.**

OT experts have a different set of objectives in mind. Obviously, they must deal with the goal of preventing information leaks, malware infections, and availability attacks; but their primary mission emphasis is on safety. That is, to an OT security professional, the most critical objectives involve assurance of safe, sound operation of OT infrastructure in a manner that avoids human casualties and lost production for large, costly physical assets.

IT THREAT EMPHASIS	OT THREAT EMPHASIS
Unauthorized information disclosure	Human injury & environmental disaster
Unauthorized data alteration	Damaged equipment & physical process downtime
Impaired data availability	Unauthorized information disclosure
Traditional CIA of data model	***Preventing incorrect control model***

Figure 1-1. Threat Emphasis in IT versus OT

The emphasis on safety concerns tends to influence OT technology protection in ways that might differ from traditional IT. A commonly cited example is change management, which is important for assuring application of security updates. An IT security team will often prioritize rapid deployment of such updates over all else, where an OT engineer might be more concerned with the risks that software changes pose to worker safety and to uninterrupted physical operations.

PURDUE MODEL OF OT/ICS

To explore options for how OT/ICS infrastructure might include proper mitigation of cyber risk, it helps to use a common model of OT – and the most popular choice is the *Purdue Enterprise Reference Architecture*, established over two decades ago. The hierarchical model specifically includes four layers of networks to support decision-making and control for industrial applications in the context of both OT and IT monitoring and support.

Before reviewing the model, some brief encouragement for traditional IT security experts trying to navigate OT/ICS: While the terminology of manufacturing control, plant management, and industrial operations might look different and daunting, you should have little trouble extrapolating your own understanding of how an enterprise runs with these newer concepts. Don't get hung up on aspects of the model you might find confusing. Just move on.

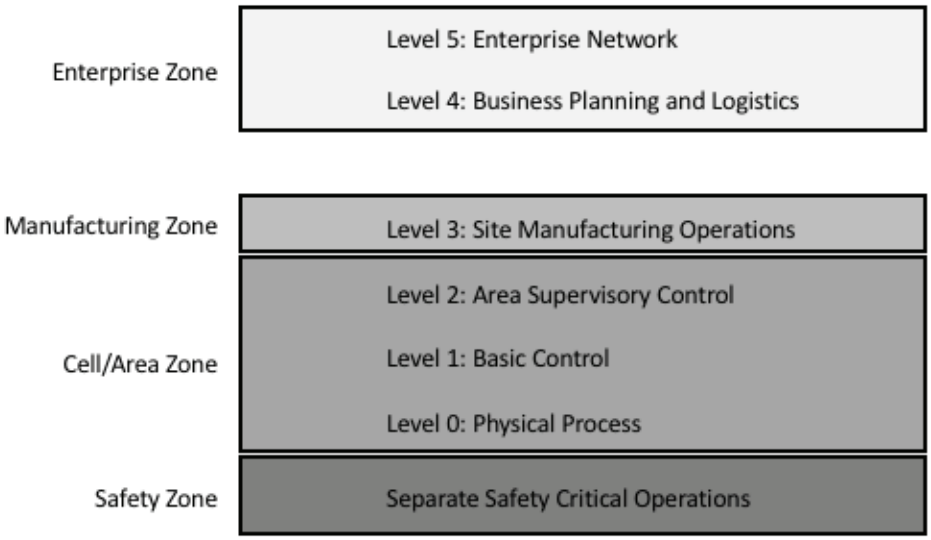


Figure 1-2. Purdue Enterprise Reference Architecture

Level 0 includes the physical processes for industrial application. Level 1 includes the basic instrumentation that controls physical layer systems. Level 2 includes supervisory control and data acquisition (SCADA) functions and human interfaces. Level 3 includes support for site manufacturing and industrial operations. Level 4 supports business planning, logistics, and other management considerations. Level 5 involves enterprise IT and network systems.

As an overlay to these six ICS functional levels, four zones of operation are identified in the model: Levels 4 and 5 are referred to collectively as the *enterprise zone*; Level 3 is referred to as the *manufacturing zone*; Levels 2, 1, and 0 are referred to collectively as the *cell/area zone*; and a fourth *safety zone* is defined that includes air-gapped systems that monitor and manage physical Layer 0 systems. None of these levels or zones are hard and fast; they are a guide.

It is worth emphasizing that references to safety in the context of OT/ICS infrastructure cannot be understated. Traditional safety procedures and mechanisms have become an essential component of the emerging cyber security programs. For example, if an administrator notices evidence of malware in critical control systems, then procedures for safety-focused emergency shutdowns are not only practiced, but might even be required by local laws.

IT IS WORTH EMPHASIZING THAT REFERENCES TO SAFETY IN THE CONTEXT OF OT/ICS INFRASTRUCTURE CANNOT BE UNDERSTATED.

PHYSICAL AND PERIMETER SECURITY FOR OT/ICS

Unique security challenges emerge at each layer in the Purdue model. First, it is obvious that any physical devices or systems must be locally protected against on-site physical tampering or hands-on

sabotage by compromised staff. Motivation for such attacks can range from nation-state guidance to employee disgruntlement. While hands-on attacks do not cascade and cannot be done remotely, this does not make them any less dangerous when they do occur.

As a result, ICS infrastructure generally includes mature, well-developed, facility controls. Personnel are carefully vetted and authenticated before given access to equipment and systems. Buildings, factory floors, equipment rooms, and physical plants are typically accessible only to badge-carrying personnel, and well-policed by on-site security guards with the authority to act if necessary. For these reasons, most people see physical controls as essential to overall ICS security programs.

The challenge is that with the introduction of automated control and management, ICS security inherits the vulnerability challenges of remotely accessible software. Specifically, potential security exploits emerge across the so-called OT/IT interface that exists just beneath the highest layer in the Purdue model. It is this interface that connects traditional hackers with computers on IP networks and the OT-based devices in an ICS ecosystem.

> **WITH THE INTRODUCTION OF AUTOMATED CONTROL AND MANAGEMENT, ICS SECURITY INHERITS THE VULNERABILITY CHALLENGES OF REMOTELY ACCESSIBLE SOFTWARE.**

For this reason, most implementations of the Purdue model now include a separation function, expressed as a demilitarized zone or perimeter network, at this OT/IT interface. This separation includes firewall, intrusion detection, filtering, and other traditional network security functions. The implementation is usually generic, using addresses, ports, and protocols, but the control at least offers some opportunity to separate functions and enforce policy.

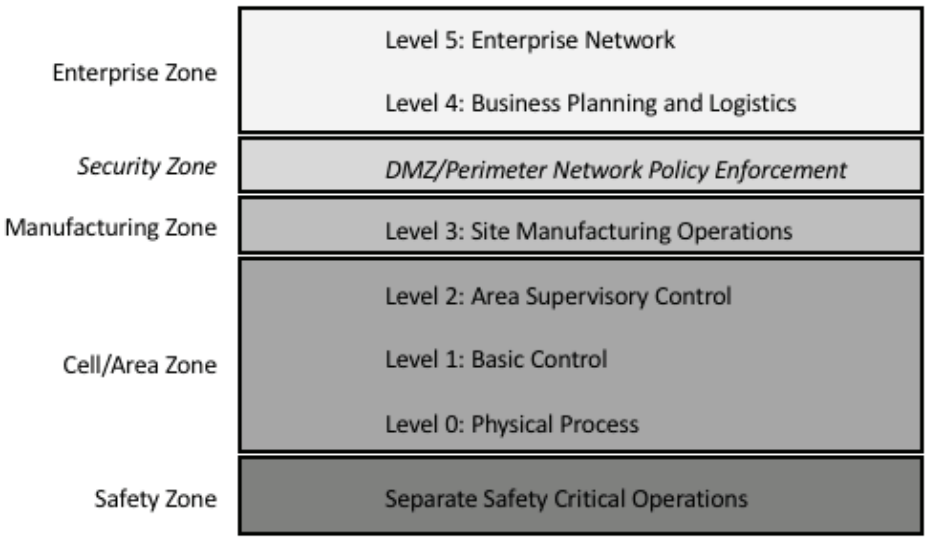


Figure 1-3. Purdue Enterprise Reference Architecture with DMZ

The challenge with this perimeter-based security zone – as you would expect – is that IT security experts have already determined that software-based perimeters don't work. Sadly, this conclusion extends to OT/ICS environments as well. Service exceptions, compromised insiders, and unavoidable traffic entry and exit make perimeter firewalls look more like network cross-connects than traffic cops. This is no longer a controversial claim; everyone agrees.

ADVANCED, MODERN CYBER SECURITY FOR OT/ICS

The challenge for modern cyber security engineers working in the OT/ICS area involves modernizing the weak or missing protection controls in existing infrastructure toward more advanced and effective solutions that will stop malicious actors. The good news is that many of these controls can be extended from mature IT security, but in the lower layers of the Purdue model, some new situations emerge that require new types of cyber risk management.

An important consideration in practical OT/ICS contexts is the practical belief by many industrial experts that traditional IT security – including patching, anti-virus software, and password management – is simply inadequate to the serious consequences associated with industrial systems. This is a promising balance to the often-cited shortcomings in OT/ICS staff in their expertise and training in modern cyber security.

> **IN THE LOWER LAYERS OF THE PURDUE MODEL, SOME NEW SITUATIONS EMERGE THAT REQUIRE NEW TYPES OF CYBER RISK MANAGEMENT.**

It helps to first partition OT/ICS into two categories – namely, (1) *OT infrastructure* consisting of non-traditional computing components such as analog signaling and electromechanical operation, and (2) *IT infrastructure* consisting of traditional computing components such as application software, physical and virtual servers, and packet networks running the TCP/IP protocol suite. OT/ICS threats exist within each of these domains, or across their boundary.

To ensure protection of these domains and the OT/IT interface, three basic security objectives provide optimal design guidance:

- **Strong Entity Authentication** – This involves strong validation of reported identities by OT devices in IoT or ICS settings. No security architecture can possibly work without such assurance and for IT-exposed systems, multi-factor usage is becoming more the norm than the exception.
- **Domain Separation** – This involves the creation of strongly separated architecture domains that can enforce desired policies. Unidirectional gateways are emerging as a useful technique to ensure provable separation between domains.

- **Activity Monitoring** – This involves gathering information about observable activity for threat analysis, compliance monitoring, and report generation. Nearly all compliance frameworks demand activity monitoring functionality, and this includes OT/ICS.

The achievement of these basic security objectives within OT is by far the greater challenge, simply because any change in OT must be analyzed and tested so very extensively, while IT security best practices evolve at a rapid pace to stay ahead of our attackers.

Two important caveats are worth mentioning with respect to these security objectives: First, in the presence of strong entity authentication, administrators might need workarounds to deal with emergency situations that require immediate unimpeded access to safety systems that can save lives. OT/ICS security design must therefore account for this important consideration, if only because of the unique role that safe, assured operation plays in industrial systems.

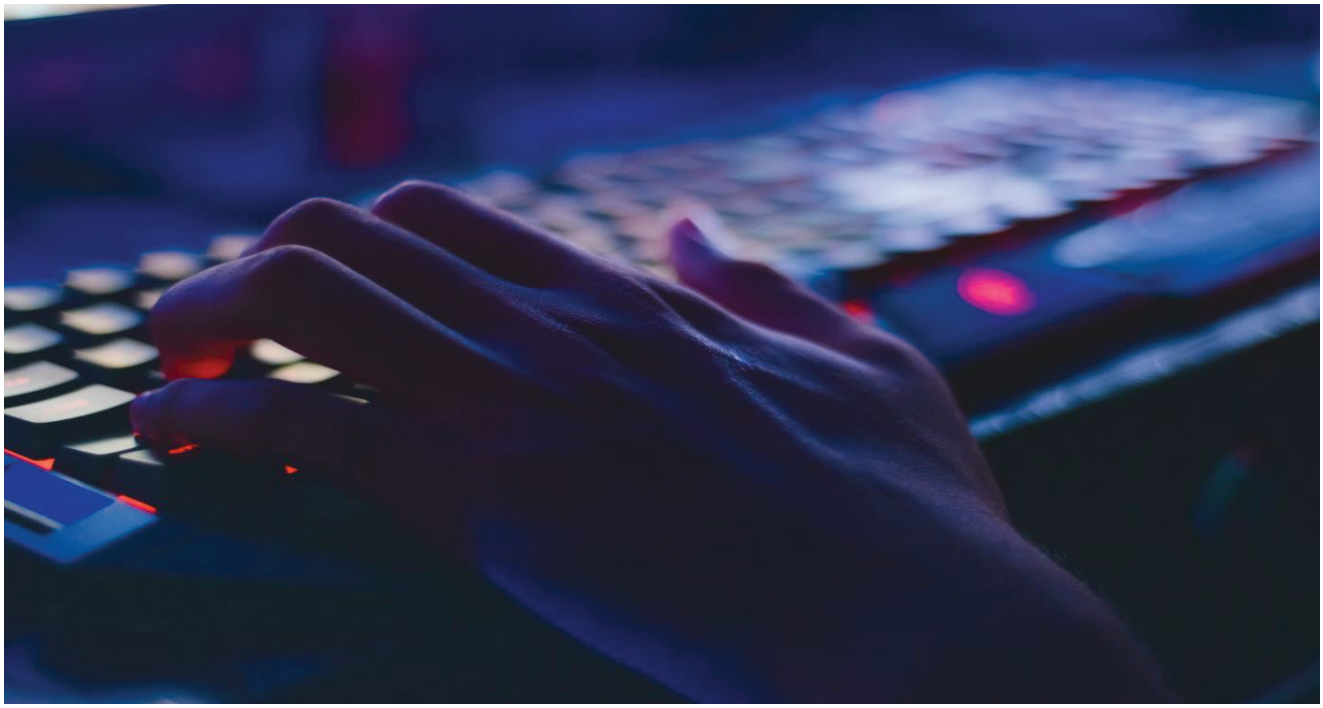
Second, it should be recognized that domain separation – and perimeters, in particular – play a much more vital role in OT/ICS security design than enterprise IT infrastructure. This follows the common specificity associated with the input and output command and traffic requirements for an OT/ICS domain. Unlike enterprise IT systems, these industrial requirements are more tractably supported by perimeter controls.

The prospect for achieving the three basic security objectives are much more promising within and across the IT/OT interface. Subsequent articles in this series will explore specifically how modern cyber security controls can be embedded in this aspect of the OT/ICS model to reduce cyber risk. Highlighted results of this application for the next four articles in the series are listed below:

> **THE PROSPECT FOR ACHIEVING THE THREE BASIC SECURITY OBJECTIVES ARE MUCH MORE PROMISING WITHIN AND ACROSS THE IT/OT INTERFACE.**

- *Article Two* offers an insight into how hackers have had success to date breaking into operational systems
- *Article Three* outlines the SCADA vulnerabilities associated with typical industrial control system architectures
- *Article Four* covers how innovations such as unidirectional gateways can be used to separate industrial networks from Internet-exposed IT networks
- *Article Five* provides a glimpse into the future of OT and SCADA systems in critical infrastructure.

The insights offered in these articles are intended to provide guidance for both traditional IT security experts, as well as OT engineers who might be new to cyber protection solutions. The optimal staff arrangement in any OT/ICS environment would optimize the OT experience and expertise of the engineers with the cyber security insights of the traditional enterprise IT security expert. These articles are intended to help both types of expert.



ARTICLE #2

HOW HACKERS EXPLOIT CRITICAL INFRASTRUCTURE

The traditional focus of most hackers has been on *software*, but the historical focus of crime is on anything of value. It should come as no surprise, therefore, that as operational technology (OT) and industrial control system (ICS) infrastructure have become much more prominent components of national critical infrastructure, that malicious hacking activity would be increasingly targeted in this direction.

It also stands to reason that the salient aspects of hacking – namely, remote access, automated tools, and weak attribution – would extend naturally to malicious targeting of critical OT/ICS infrastructure. These attributes are particularly attractive in this context, because criminals interested in disrupting factories, production systems, and other tangible infrastructure, *previously* had to establish physical presence or compromise some group with local access.

The new approach to OT/ICS hacking involves a combination of traditional techniques with domain expertise of the systems being targeted – although little expertise might be required to trigger damage to an ICS/OT system. The most powerful issue here is the ability for attackers to target tangible systems such as power plants and refineries, without having to step foot into the local facility. This is a major departure from historic norms.

> **THE MOST POWERFUL ISSUE HERE IS THE ABILITY FOR ATTACKERS TO TARGET TANGIBLE SYSTEMS SUCH AS POWER PLANTS AND REFINERIES, WITHOUT HAVING TO STEP FOOT INTO THE LOCAL FACILITY.**

It is instructive to review the details of some previous OT/ICS attacks with emphasis on how malicious actors adapted familiar hacking methods with the specifics of the targeted ICS system. In the sections below, we examine two of the more well-known example hacks that have occurred in the past few years – namely, the Stuxnet worm of 2010 and the Ukrainian Power attack of 2015.

STUXNET ATTACK

Stuxnet consisted of worm functionality operating in the upper layers of the Purdue Model that was designed to locate and attack OT resources in the lower layers. Specifically, the worm was propagated by unknowing humans with malware-infected USB sticks transported and used across critical infrastructure sites. Once resident on a Windows computer, the worm searched for the presence of Siemens control-system software used to control electromechanical devices.

If the Stuxnet search on a given Windows machine located the desired Siemens control software, the toolkit would propagate throughout all of the computers in the Siemens control system, through firewalls and across IP networks. When the Stuxnet malware found the responsible computers, then a powerful rootkit was downloaded into what is known as a *programmable logic controller (PLC)*, as found in Layer 1 of the Purdue Model. PLCs control many types of physical systems.

While many questions remain as to the origin of the attack, the security community generally agrees that Stuxnet was developed to target gas centrifuges in Iran's uranium enrichment facilities. The consensus opinion is that the worm used its rootkit payload to send special destructive commands to Iran's enrichment infrastructure as an alternative to conventional forms of attack. The attack forced changes in the rotor speed of the gas centrifuges to cause permanent damage to these devices – all done remotely.

Figure 2-1. Stuxnet Attack Progression

Understanding how Stuxnet might have been prevented offers useful hints about OT/ICS security. First, one would likely point fingers at the Microsoft and Siemens software, both of which provided a friendly environment for the USB worm. Four zero-day vulnerabilities in Microsoft Windows, for example, were used to infect target systems. So, it is reasonable to recognize the impact of platform vulnerabilities as a root cause in present and future OT/ICS attacks. This is not a problem that will ever go away – all software has defects, and some of those defects are vulnerabilities, known and unknown.

> **IT IS IMPORTANT TO RECOGNIZE THE IMPACT OF POOR OPERATING SYSTEM CODE QUALITY AS A ROOT CAUSE IN PRESENT AND FUTURE OT/ICS ATTACKS.**

Second, one would recognize the ease with which the worm was able to propagate from higher levels of the architecture to lower levels. This suggests that OT/IT interfaces require at least the same levels of gateway protection one finds in a typical enterprise gateway. This implies that the lower layers of the Purdue Model should not implicitly trust software operating at the higher levels.

This is easier said than done, but the way, because the worm demonstrated the functional ability to automatically jump through firewalls across encrypted, authenticated connections. Imposing new cyber security requirements such as two-factor authentication between processes communicating across the OT/IT interface would have done little to slow down Stuxnet.

UKRAINIAN POWER HACK

In December of 2015, hackers compromised electric power distribution to citizens of Ukraine. Three energy companies – all with names too long to repeat here – were targeted and the bottom line is frightening: Nearly a quarter of a million people had no electricity for several hours. The origin and motivation of the attack have been debated, but would seem less relevant than the question of how to prevent such a thing from occurring in the future.

Analysis of the attack reveals use of a multitude of different SCADA cyberattack methods including the following components:

- **Trojan Malware** – Advanced Windows-executable malware called BlackEnergy was identified, but was not implicated in the outage. Instead, standard hacktivist remote control methods were most likely used.
- **Spear Phishing** – Attackers used email spear phishing with spoofed sender identity (Ukrainian Parliament) and malicious attachments.
- **Remote Control** – The attack resulted in remote operation of power company substation equipment and systems.

- **Destructive Action** – The KillDisk utility delivered as part of the attack destroyed files on substation servers and devices.
- **Denial of Service** – Power company customer support centers experienced DDOS attacks to degrade their ability to provide service to affected customers.

This coordinated attack suggests that the IT/OT interface for these Ukrainian power companies was largely unprotected. Each of the components in the attack are well-known to the cyber defense community, and while no cyberattack risk can be reduced to zero in any case, the protections here seemed much too ineffective for users and systems in an electric power grid environment.

> **THIS COORDINATED ATTACK SUGGESTS THAT THE IT/OT INTERFACE FOR THESE UKRAINIAN POWER COMPANIES WAS LARGELY UNPROTECTED.**

Perhaps the greatest lesson from the Ukrainian attack is that critical infrastructure providers must develop and maintain higher cyber security standards than purveyors of more mundane systems and services. The idea that such an extensive collection of attacks might be successfully engaged with these companies should sound alarms across the entire industry segment – and this includes power companies in larger countries such as the United States.

A basic notion that such companies might consider involves separation enclaves around power substation or related functions. This might be best accomplished using separate physical communications infrastructures. These separate physical enclaves would also benefit from powerful gateway solutions implementing unidirectional communications flow. This would ensure that hacks to the IT portion of a power company would not cascade to OT substations.

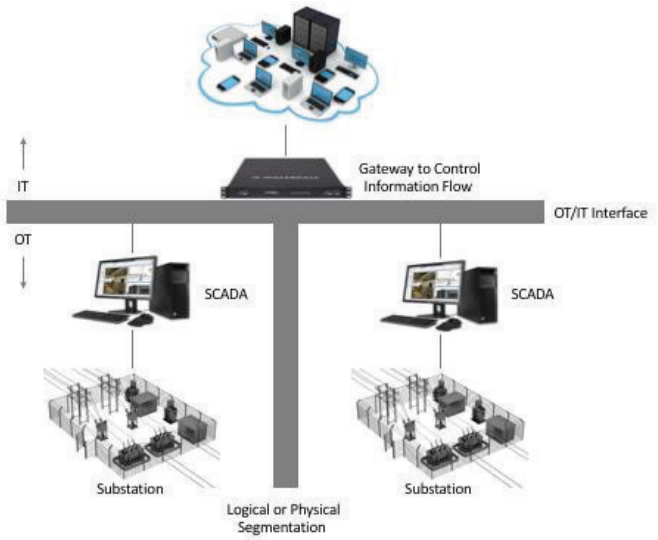


Figure 2-2. IT/OT Substation Protection Using Advanced Separation Technology

Regardless of the specific types of cyber security technologies being used, the idea that substations might be separated into physically discrete domains across power company infrastructure provides powerful protection against the types of cascading attacks so commonly found in advanced attacks, especially from nation-state actors.

LESSONS FOR OT/ICS SECURITY

Designers and operators of OT/ICS infrastructure should recognize that incidents such as the Stuxnet worm and the Ukrainian Power Company attack offer clear hints as to the best security solutions for the sector. First, it should be clear that standard IT-based cyberattacks can and will be launched at their OT systems. This suggests that a role will exist for traditional security vendors who can adapt their approaches to work across OT/IT interfaces.

> **IT SHOULD BE CLEAR THAT STANDARD IT-BASED CYBERATTACKS CAN AND WILL BE LAUNCHED AT THEIR OT SYSTEMS.**

Second, they must recognize that exploitable ICS vulnerabilities will always exist in OT infrastructure, and that malware is being designed to specifically target these weaknesses. It is no longer an acceptable security solution to simply presume that because technology differences might exist between IT and OT-based systems, that cyberattacks will not cross the boundary. Recent evidence clearly suggests the contrary.

Finally, these recent attacks suggest that this presumed technology gap between IT and OT systems is certainly shrinking. The idea that malware might seek, find, and destroy SCADA capabilities in a worm launched using conventional IT social engineering (e.g., dropping memory sticks in parking lots) should create chilling prospects for OT/ICS security engineers. Let's hope the community pays attention and takes protective action immediately.

ARTICLE #3

SCADA VULNERABILITIES IN ICS ARCHITECTURES

A major challenge in industrial control system architecture involves the dual nature of its underlying technologies. That is, a typical ICS component must have the capability to exchange information with both IT and OT systems across designated network or system interfaces. This is different from traditional industrial devices like heat pumps, actuators, and motors that were previously *only* accessed and controlled by OT systems, usually either analog or electro-mechanical.

So, today the existence of two access points for devices represents one of the primary vulnerabilities in OT/ICS infrastructure, and prompts the general strategy that malicious actors tend to follow. That is, conventional IT hacking tools and techniques would be typically used to first achieve sufficient proximity to the ICS component. Using this proximity, the attack would then attempt to either subvert OT control, or the device directly.

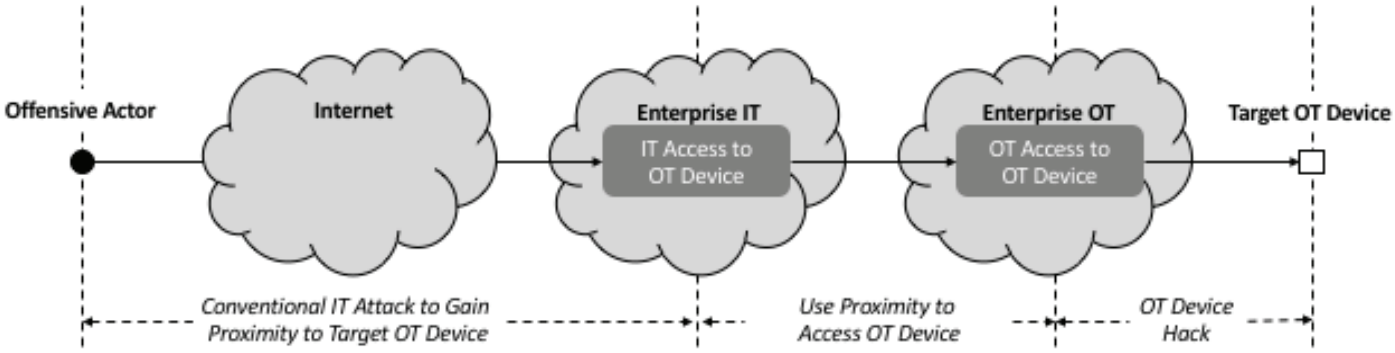


Figure 3-1. IT Attack Paths to Gain Proximity to OT/ICS Target

The term SCADA refers to the supervisory control and data acquisition functions that exist at Level 2 of the Purdue model, and that are the essence of this IT/OT interface. Because of this attack path vulnerability, cyber security experts have increasing focused on demanding improved security features SCADA software, which is much easier for new control functions, than for legacy SCADA systems that might have been in place for many years. These experts recognize though, that no matter how many security features are built into OT software, all software has bugs and other residual vulnerabilities.

The reason SCADA security is so controversial stems primarily from the intense consequences that come from a compromise in this area. Unlike some purely technical debates where issues of cost, functionality, or standards might be considered, when SCADA systems are hacked the consequences can include the following types of *potential* types of severe impact:

- **Industrial Control System Hijacking** – The remote-control safety-critical or reliability-critical OT system in an industrial control setting could be hijacked by criminals, terrorists, or aggressive military groups.
- **Vital Telemetry Interference** – Important information beaconed from an OT system regarding possible safety or equipment-damaging conditions in an industrial control system might be blocked or interfered with.
- **Critical OT System Unavailability** – The accessibility and availability of OT systems might be blocked or degraded, which could have real-time consequences if that target system is required for essential control of physical operations.

In many environments, the primary functional control separating IT and OT systems is the physical bus on some computing element. Using only software to drive such security separation is never recommended for any critical infrastructure component. For example, an automobile should never connect IT services such as WiFi and entertainment to the same physical bus as control services such as engine diagnostics and safety management.

Carrying this vulnerability further, the more general requirement is that IT and OT systems would be best configured to never share any functionality that can be remotely accessed. This creates that lifeline path hackers seek to gain access via routine, conventional means, and to then use this access to cross that

shared path to the targeted OT device or system. This strategy is both effective and clearly demonstrated in practice.

> **THE MORE GENERAL REQUIREMENT IS THAT IT AND OT SYSTEMS WOULD BE BEST CONFIGURED TO NEVER SHARE ANY FUNCTIONALITY THAT CAN BE REMOTELY ACCESSED.**

In 2015, two security investigators from the University of San Diego demonstrated malicious remote control of the brakes in a Corvette vehicle by accessing the on-board diagnostic dongle located under the driver's side dashboard. The use-case they cited was that someone might be sitting in your car, could plug into the diagnostic dongle, and then use that remote access later to perform the hack on other systems – including brakes.

Perhaps more shockingly, two well-known researchers, Charlie Miller and Chris Valasek, demonstrated, also in 2015, the ability to exploit a zero-day software vulnerability to access a moving Jeep on a live highway from their laptop, without ever having physical access to the target vehicle. The attackers used this remote access to send commands through the vehicle's entertainment system to its dashboard capabilities, which included the brakes, steering, windshield wipers, air conditioning, and other functions.

In each case – and this is clearly not limited to automobiles, the primary vulnerability involves shared access between remotely accessible features and mission-critical functions. This is a fatal problem in OT/ICS infrastructure, because hacks can often occur in the presence of proper network security controls. By connecting critical and non-critical components across shared mechanisms such as the well-known CANbus on many OT systems, hackers are given a path to remote control.

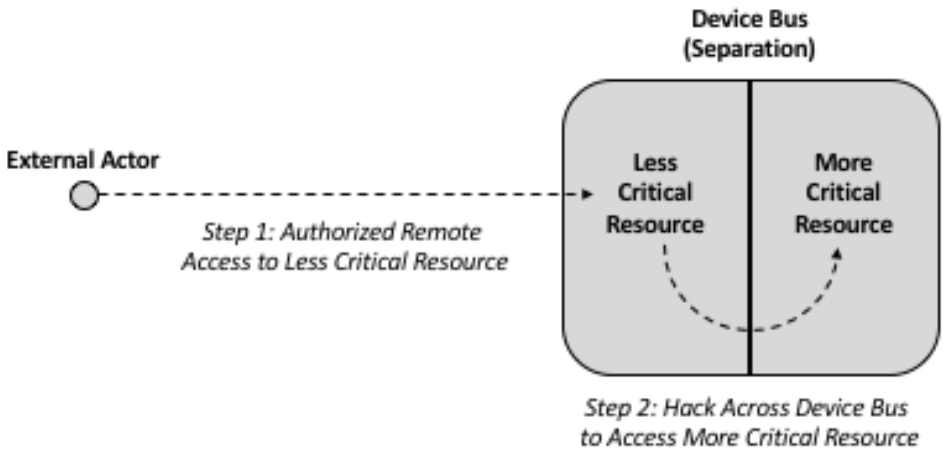
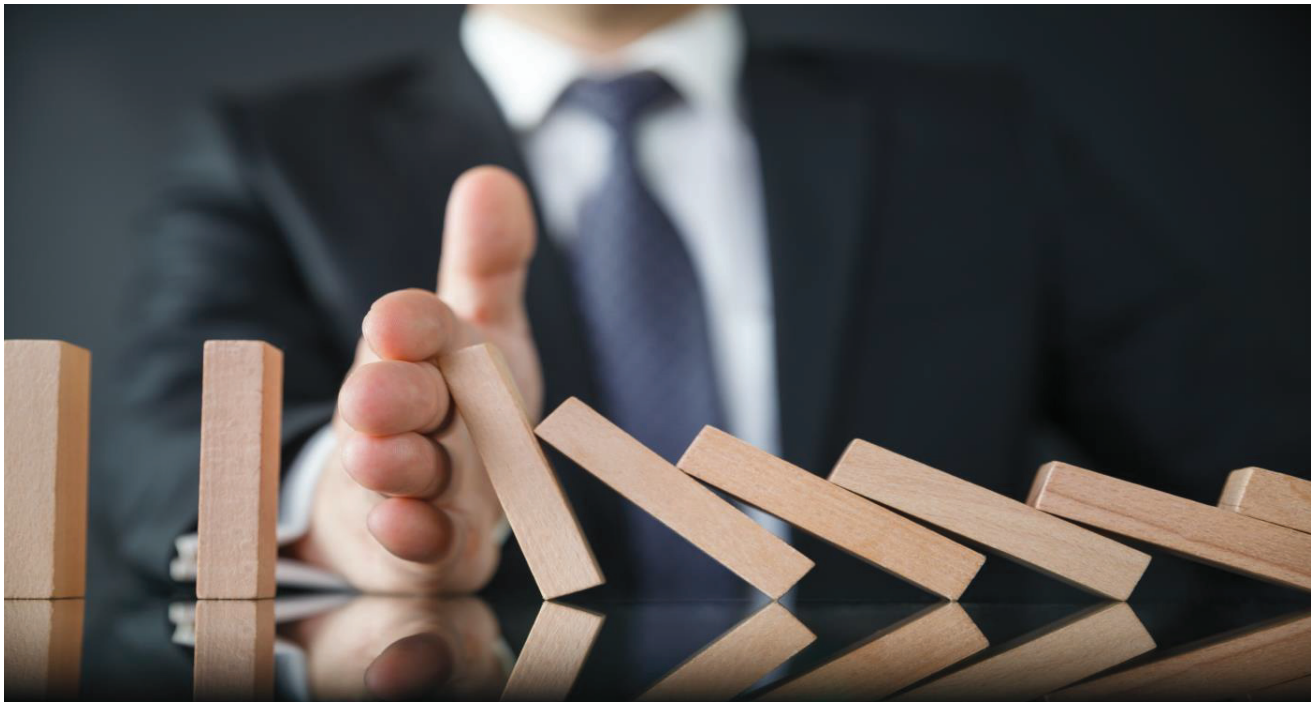


Figure 3-2. Remote Exploit Across Shared Device Bus

The solution to this problem lies first in establishing proper security separation requirements for industrial control system devices, as well as any other Internet of Things (IoT) component that might produce unwanted consequences if hacked. Separation needs to become a mandatory functional requirement embedded in the design process, enforced during development, and consistently audited before and after deployment.

> **SEPARATION NEEDS TO BECOME A MANDATORY FUNCTIONAL REQUIREMENT EMBEDDED IN THE DESIGN PROCESS.**

Separation is best achieved using flow control mechanisms that can ensure complete avoidance of malware transferal from untrusted systems to critical infrastructure. This can be implemented using gateways that implement physical separation and one-way communication mechanisms. This technique, known as a unidirectional gateway, will be highlighted investigated further in a subsequent article.



ARTICLE #4

UNIDIRECTIONAL GATEWAYS

A powerful technique for protecting OT from IT, or to enforce whatever separation is required to ensure the integrity of industrial control infrastructure, involves controlling the direction of traffic into or out of an ICS enclave. At first glance, it might seem counterintuitive to restrict bidirectional traffic between OT devices and management systems, but closer inspection reveals that across IT/OT interfaces, almost all data flows are from OT to IT systems, and hardware unidirectional flow assurance provides strong risk reduction for OT.

Most information flow in OT/ICS environments involves communications from control systems to IT systems. This enables continuous and effective monitoring of critical industrial control functions and equipment status. Modern industrial enterprises have long since learned to profit from real-time access to operations data, through programs ranging from predictive maintenance to comparing details of operation across facilities to enable enterprise-wide optimization and operations best practices.

A primary cyber security OT risk involves malware or remote attackers finding their way into the ICS infrastructure to degrade operations, block telemetry flow, or alter configuration settings. Assuming the devices are manufactured correctly (i.e., no malware inserted by developers), this risk can only be realized only in the presence of an information flow channel into ICS devices from the network infrastructure hosting the IT systems.

This information flow channel may be physical, for example a USB drive carried past physical security, or via online IP or other messaging. Modern industrial sites generally eliminate as much as possible physical information flows, by banning removable media and transient devices such as vendor laptops, and implementing security controls that make it impossible to mount such media on control equipment, or connect unauthorized devices to control networks. What remains is to control the online attack channel.

> **A PRIMARY CYBER SECURITY OT RISK INVOLVES MALWARE OR REMOTE ATTACKERS FINDING THEIR WAY INTO THE ICS INFRASTRUCTURE.**

A paradigm thus emerges for data flow management through designated *unidirectional gateways* that can assure such control in all cases. The operational objective is that upon deployment, telemetry *from* ICS devices *to* the external network is permitted to support industrial control monitoring, but that reverse flow *from* the external network *to* the ICS devices would be prevented to prevent malware infections.

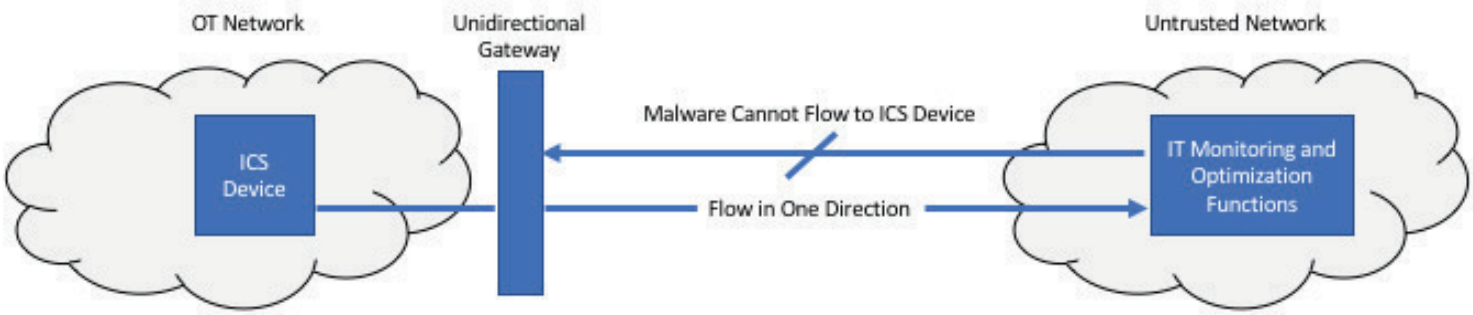


Figure 4-1. Unidirectional Gateway Protection of ICS Devices from Malware

The implication of such flow management is profound, because if the underlying unidirectional device design is sound, then one can make the physical argument that malware cannot flow toward the control system network. For many years, air gap arguments were weakened by end-around paths in complex networks because IT monitoring of OT systems had so much value. Unidirectional Gateways enable this very valuable monitoring function, while physically preventing any potentially compromising information from reaching the protected ICS system.

The physics of unidirectional gateway design supports transmit and receive flows using the optical characteristics of light. Without getting too much into the physics, security experts can take comfort in the fact that a so-called TX (transmit) laser sends data across a gap medium to an RX (receiver) in a manner that ensures that information can physically flow in only one direction, but not in the reverse.

THE PHYSICS OF UNIDIRECTIONAL GATEWAY DESIGN SUPPORTS TRANSMIT AND RECEIVE FLOWS USING THE OPTICAL CHARACTERISTICS OF LIGHT.

This type of strong flow direction management allows for security policies to be written and enforced on OT/ICS infrastructure regarding malware. For example, an OT infrastructure could have the following operational requirement imposed on its operation in the presence of a unidirectional gateway: "*The organization shall ensure that malware cannot flow into the OT/ICS infrastructure.*" This is a powerful cyber security requirement for SCADA protection.

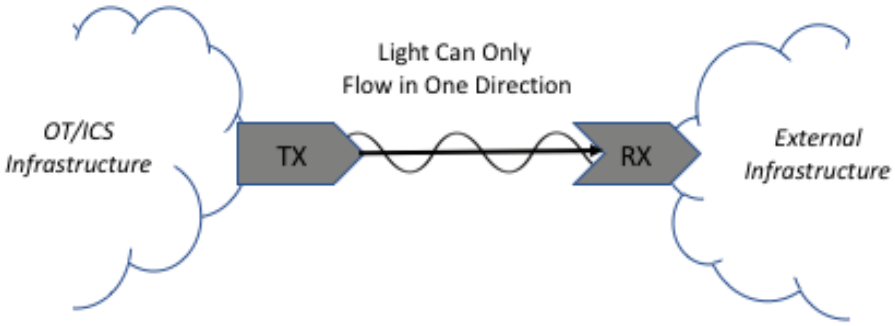


Figure 4-2. Unidirectional Gateway Design

An apparent challenge in the presence of a unidirectional gateway is modern communications protocols – almost all such protocols are query/response. How can response data reach IT consumers who can profit so much from the data, if no queries can reach the ICS data sources? The solution lies in the unidirectional gateway software, which replicates database servers and other servers. The software in the control-system source network queries control servers, sends data and updates through the unidirectional hardware, and on the receiving network, inserts the data into identical / replica servers. IT users and applications send their queries to the IT replicas, and get the same answer from the replicas as the live ICS servers would have given.

Another challenge is the apparent requirement for commands to flow from the external environment to the ICS devices. Reconfigurations, patching, updates, and other control commands, for example, might need to be issued from IT servers to the deployed OT/ICS servers and devices. Unidirectional gateways would disallow such functionality.

Most often, this need is an illusion. For example, automatic security updates might seem to warrant an inbound communications channel, but the engineering change control discipline demands extensive testing of such updates over a long period of time. An automatic inbound channel makes sense when security updates enter a network daily – such a channel reduces manual labor, errors and omissions in copying updates daily to removable media and carrying them across the perimeter. But in a system where security updates cross the perimeter in batches, only every 3-6 months, an automatic inbound channel introduces more risk than it alleviates.

A more common requirement is for anti-virus updates to enter protected control systems reasonably regularly, and batch instructions in the form of XML production orders to enter frequently as well.

These information transfers are more disciplined than the arbitrary “access” connections, and can be inspected in much more detail to determine that the transfers are safe.

> **INFORMATION TRANSFERS ARE MORE DISCIPLINED THAN THE ARBITRARY “ACCESS” CONNECTIONS, AND CAN BE INSPECTED IN MUCH MORE DETAIL TO DETERMINE THAT THE TRANSFERS ARE SAFE.**

This need can be met by replicating servers, or subsets of servers, from untrusted IT networks into control networks. This can be accomplished by deploying a reversible “FLIP” device – a unidirectional gateway whose orientation reverses on a schedule.

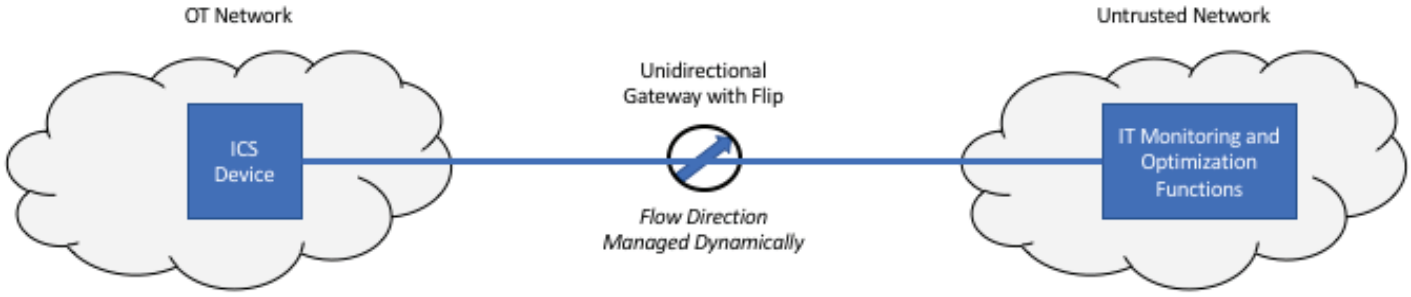


Figure 4-3. Unidirectional Gateway FLIP

The FLIP provides a disciplined method for inspecting and periodically permitting select content into unidirectionally-protected networks, in the rare cases where such content is deemed desirable. Given the unidirectional and scheduled nature of the FLIP, it is impossible to sustain an interactive TCP-like session through the device, even the most cleverly, stego-graphically hidden session.

For environments where the OT/ICS devices exist in a tangled web of local network infrastructure, perhaps with information flowing in many different directions from a variety of IT and OT devices, the security engineer might find a unidirectional gateway to be an awkward solution. It might be viewed as adding a motion sensor into the middle of a busy cocktail party, where the detection would trip constantly.

In such cases, it might be wise to rethink the overall OT/ICS architectural set-up. The decision to segregate SCADA controlled devices from IT support infrastructure such as DNS, Active Directory and anti-virus servers is a reasonable one, and would be recommended for any industrial network the enterprise deems important enough to protect thoroughly. One might say that the degree to which a unidirectional gateway, perhaps with flip capability, can be supported, is directly proportional to the segregation properties of that OT/ICS infrastructure.

Another apparent challenge to any unidirectional gateway integration involves existing or new ICS devices and management systems with intensely-bidirectional interfaces that cannot be interrupted by unidirectional flow. Most of the ICS ecosystems one can imagine would certainly have this requirement. The device might, for example, send telemetry to a system that is designed to provide back an expected heartbeat. This would seem fatal to the unidirectional concept.

> **THE DEGREE TO WHICH A UNIDIRECTIONAL GATEWAY, PERHAPS WITH FLIP CAPABILITY, CAN BE SUPPORTED, IS DIRECTLY PROPORTIONAL TO THE SEGREGATION PROPERTIES OF THAT OT/ICS INFRASTRUCTURE.**

A clever solution, however – one that greatly reduces the challenge of inserting unidirectional flow management devices into the existing device-to-control ecosystem involves functions resident on either end of the gateway, serving essentially like proxy capabilities, to emulate the function of the corresponding remote participant. Local devices, for example, would communicate with a local system proxy, and vice versa, so that the bi-directional protocol is properly supported on each network.

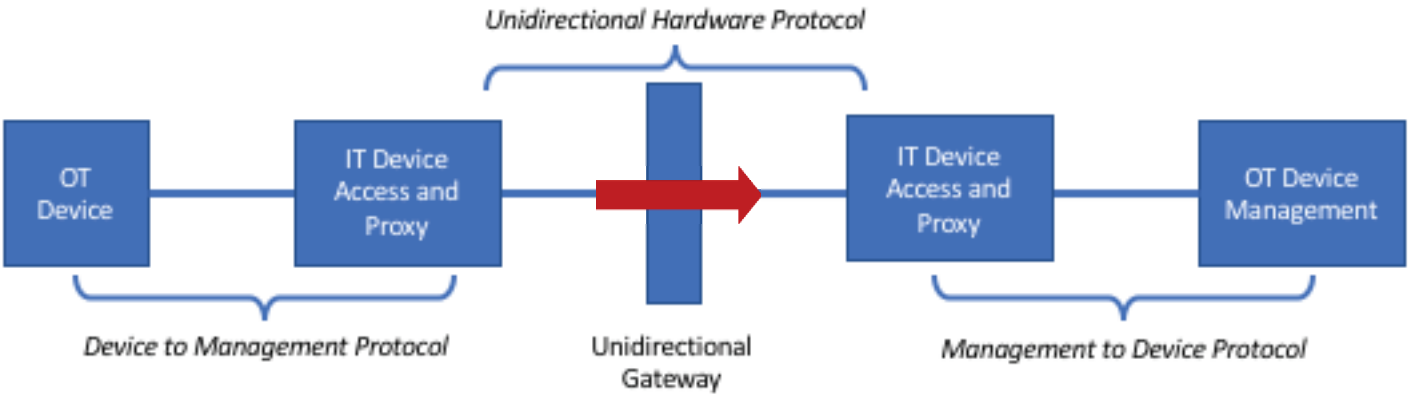


Figure 4-4. Support for ICS and Control System Bidirectional Protocol

Solutions such as from Waterfall Security offer all these and other clever capabilities, which create impression that information producers are communicating bidirectionally with the corresponding information consumers, but with the Waterfall gateway communicating across the unidirectional connection. This set-up provides the malware flow protection advantages of a unidirectional gateway while still satisfying integration requirements for existing protocols and servers.

Interested readers should contact Waterfall Security directly to better understand the various configuration options. In most cases, the platform involves what amounts to a client on both sides of the IT/OT gateway. Specific configuration requirements will vary between different OT/ICS environments, and the cyber security experts at Waterfall Security can help match the platform to the local OT/ICS requirements.

ARTICLE #5

FUTURE OF OT SECURITY IN CRITICAL INFRASTRUCTURE

Both the likelihood and consequences of cyberattacks to OT/ICS components continue to grow for modern industrial operations. While current advances in OT/ICS cyber security are impressive, new approaches are needed to gain defensive advantage over already-capable cyber adversaries, to keep up with new OT/ICS technologies, and to serve business risk management needs in increasingly-demanding, competitive environments.

In all these cases, progress only comes when both IT and OT stakeholders can (1) correctly assess current and emerging risks to industrial operations, (2) correctly assess the strength and benefits of candidate threat mitigation measures, and (3) convince business decision-makers of the correctness of these assessments to commit funds to business process and security modernization initiatives. All three of these cases are essential, but also have their corresponding pitfalls to avoid.

In practice, IT stakeholders often underestimate cyber threats to industrial operations, and overestimate the effectiveness of software-based security measures. OT stakeholders are often less predictable, sometimes underestimating threats and resisting investment in improved security posture, while other times overestimating threats and raising safety concerns that impair modernization efforts. In all cases, communicating threats, defensive postures, and the need for change to business decision-makers can be difficult.

To address these challenges, we discuss below three specific areas in the context of both improved enterprise operational effectiveness, and enhanced security for industrial control systems:

- **Industrial Internet of Things (IIoT)** – Internet-based cloud services for industrial automation promise significant benefits to industrial enterprises, while dramatically increasing industrial attack surfaces.
- **Universal Security Monitoring** – Modern enterprises rely on Security Operations Centers (SOCs) and Security Information and Event Management Systems (SIEMs) with limited visibility into their industrial operations.
- **Tamper-Proof Forensics** – Since no defensive posture can ever be perfect, strong support for incident response and recovery is a high priority, especially for industrial networks that may be targeted by sophisticated threat actors.

These three cases highlight the types of considerations that many OT/ICS security engineers are working on today. Each is discussed in more depth below.

INDUSTRIAL INTERNET OF THINGS

The emerging Industrial Internet of Things (IIoT) consists of edge industrial devices connected directly to cloud systems on the Internet. Significant advantages stem from aggregating and analyzing large amounts of data from many sites and/or clients. Many industrial vendors are investing significant resources in new product offerings in this realm. The security result though, is a significantly expanded attack surface where threats can use known and zero-day vulnerabilities to pivot from one customer, through cloud sites, to sensitive industrial networks at other sites and enterprises. This, and related risks, are impeding the adoption of IIoT technology at many sites.

Waterfall's Unidirectional CloudConnect is a solution that preserves the benefits of cloud-based big data analytics in the IIoT without the increased attack surface for industrial control networks. Unidirectional CloudConnect is an industrial control device having a local unidirectional gateway through which it can gather data from a wide variety of industrial data sources. Translation capabilities are included so that data can be exchanged between the OT and cloud domains. This allows direct connections from sensitive OT networks to the Internet.

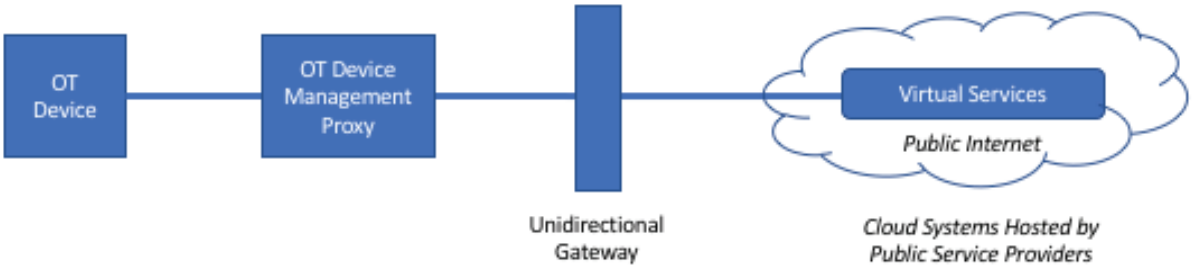


Figure 5-1. OT Devices Connected Directly to Cloud Systems on the Internet

> THE EMERGING INDUSTRIAL INTERNET OF THINGS (IIOT) CONSISTS OF EDGE INDUSTRIAL DEVICES CONNECTED DIRECTLY TO CLOUD SYSTEMS ON THE INTERNET.

This general issue of reducing risk in the IIoT will be one of the most important areas of cyber security in the coming years, especially as more ICS devices are integrated with IT-based or Internet-based cloud services – often for cost reduction. Unless these risks are properly addressed, the consequence implications for OT/ICS infrastructure can be significant.

UNIVERSAL SECURITY MONITORING

The Waterfall Security team has observed that while intrusion detection and security monitoring disciplines are mature on IT networks in most enterprises, the discipline tends to stop at the IT/OT gateway in industrial enterprises. In part, this is because few SOCs are equipped to properly gather and interpret telemetry and logs from OT/ICS networks.

> WHILE INTRUSION DETECTION AND SECURITY MONITORING DISCIPLINES ARE MATURE ON IT NETWORKS IN MOST ENTERPRISES, THE DISCIPLINE TENDS TO STOP AT THE IT/OT GATEWAY IN INDUSTRIAL ENTERPRISES.

An additional issue, however – and this might seem ironic, is that deep monitoring of certain OT/ICS devices is often seen as too sensitive to be installed into a given operational environment. That is, where OT devices are critical to correct and continued operation of important industrial processes, a management decision might be made to avoid installing intrusion detection probes and security monitoring systems for fear that new security risks might be introduced through connectivity with IT-based or Internet/cloud-based SOCs.

This is an unacceptable situation because security engineers can only secure what they can observe and measure. To address this need, intrusion detection and security monitoring engines are starting to support a much wider variety and depth of industrial systems than was historically the case. To address the security concerns stemming from connectivity with these engines, industrial sites are again deploying Unidirectional CloudConnect or other unidirectional monitoring capabilities.

In a sense, progress here mirrors the problem and progress in the IIoT realm. Both are examples of both risks and benefits stemming from increased connectivity between industrial networks and central IT-based or cloud-based systems. Unlike the emerging field of IIoT big-data analytics though, safe, increased coverage for central security monitoring systems is seen by most industrial sites as a current and urgent problem.

TAMPER-PROOF FORENSICS

With widespread adoption of the NIST Framework by industrial enterprises, many enterprises are seeking to develop robust industrial cyber incident response capabilities. One challenge with industrial incident response is access to reliable forensics. Industrial enterprises increasingly seek to defend their industrial networks against even the most sophisticated attacks. Sophisticated attacks though, frequently involve the intruder modifying, deleting, and erasing evidence of their attacks. This might even include accessing distantly hosted SIEMs and log analyzers if they can be located. Sadly, many of these systems share mutual trust across laterally traversed LANs, which is consistent with most APT methods.

The Waterfall Security team supports this challenge with its BlackBox solution, which includes a unidirectional gateway, and which gathers forensic data from a wide variety of industrial and IT device sources. The collected data is pushed through the one-way hardware into an encrypted and otherwise isolated storage system. The result is a securely stored, protected forensic log that cannot be tampered with by an adversary.

> **THE WATERFALL SECURITY TEAM SUPPORTS THIS CHALLENGE WITH ITS BLACKBOX SOLUTION, WHICH INCLUDES A UNIDIRECTIONAL GATEWAY, AND WHICH GATHERS FORENSIC DATA**

Waterfall Security has also developed a transportable version that response teams can carry to a given site if necessary. The device can be quickly configured to gather reliable forensics, in case the attackers are still active in the compromised network, and might be trying to actively interfere with the investigation. When the team has collected sufficient forensic evidence, analysis can be performed off-line.

CONCLUDING THOUGHTS

There are far fewer industrial control system networks in the world than there are IT networks, and far fewer ICS security practitioners. Historically, this has meant that many well-meaning practitioners take inspiration from IT networks, and apply IT-centric solutions universally to both IT and OT networks.

Fortunately, this is changing. A recent whitepaper by the Gartner Group for example - *Demystify Seven Cybersecurity Myths of Operational Technology and the Industrial Internet of Things* – points out clearly that IT methodologies are not appropriate to calculating risks and assessing threats on OT networks, and that IT cybersecurity designs are not adequate to OT security needs.

Unidirectional Gateways and related products are one of the OT-centric security technologies that Gartner and other experts and authorities are recommending be evaluated for OT security needs, and become part of many OT security solutions.

ABOUT

THE AUTHORS

EDWARD AMOROSO

Dr. Ed Amoroso is currently Chief Executive Officer of TAG Cyber LLC, a global cyber security advisory, training, consulting, and media services company supporting hundreds of companies across the world. Ed recently retired from AT&T after thirty-one years of service, beginning in Unix security R&D at Bell Labs and culminating as Senior Vice President and Chief Security Officer of AT&T from 2004 to 2016.

Ed has been Adjunct Professor of Computer Science at the Stevens Institute of Technology for the past twenty-seven years, where he has introduced nearly two thousand graduate students to the topic of information security. He is also affiliated with the Tandon School of Engineering at NYU as a Research Professor, and the Applied Physics Laboratory at Johns Hopkins University as a senior advisor. He is author of six books on cyber security and dozens of major research and technical papers and articles in peer-reviewed and major publications.

Ed holds the BS degree in physics from Dickinson College, the MS/PhD degrees in Computer Science from the Stevens Institute of Technology, and is a graduate of the Columbia Business School. He holds ten patents in the area of cyber security and media technology and he has served as a Member of the Board of Directors for M&T Bank, as well as on the NSA Advisory Board (NSAAB). Ed's work has been highlighted on CNN, the New York Times, and the Wall Street Journal. He has worked directly with four Presidential administrations on issues related to national security, critical infrastructure protection, and cyber policy.

https://www.tag-cyber.com/people/eamoroso

ANDREW GINTER

Andrew Ginter is the VP Industrial Security at Waterfall Security Solutions and an Assistant Professor at Michigan Technological University. At Waterfall, Andrew leads a team responsible for industrial cyber-security research, contributions to standards and regulations, as well as security architecture recommendations for industrial sites. Before Waterfall, Andrew led the development of commercial products for SCADA systems, IT/OT middleware, and ICS cyber security. He holds patents in the fields of IT/OT integration and ICS cyber security, is a co-author of the Industrial Internet Consortium Security Framework, the author of SCADA Security - What's broken and how to fix it and the author of The Top 20 Cyberattacks on Industrial Control Systems. He is the co-chair of the ISA SP-99 working group updating the ICS Security Technologies report, and a frequent contributor to ICS cyber-security standards and post-secondary curricula.

At MTU Andrew teaches EE 5451 - Cyber Risk Assessment for Critical Infrastructure Protection. Andrew holds a B.Sc.AMAT and an M.Sc. CPSC from the University of Calgary.

https://www.linkedin.com/in/andrewginter/

WATERFALL SECURITY SOLUTIONS

Waterfall Security Solutions is the global leader in industrial cybersecurity technology. Waterfall products, based on its innovative unidirectional security gateway technology, represent an evolutionary alternative to firewalls. The company's expanding portfolio of customers includes national infrastructures, power plants, nuclear plants, offshore oil and gas facilities, rail transport, 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.

Please contact us at https://waterfall-security.com/contact