Optimizing Network and Endpoint Resilience: Manufacturer Cybersecurity in the Era of Digital Transformation

TXOne Networks Inc.
Steven Hsu
Max Farrell

Table of Contents

Introduction: The Bull's-Eye on ICS

2017 was a major turning point in the emergence of IT-focused ransomware such as WannaCry, NotPetya, and BadRabbit, which have since penetrated into many OT environments causing serious damage. Previously, most threats to industrial control and security were directed at organizations in critical infrastructure sectors, usually targeted for reasons related to politics or espionage. By 2018, the combined damages from ransomware incidents rose to over $8 billion USD.

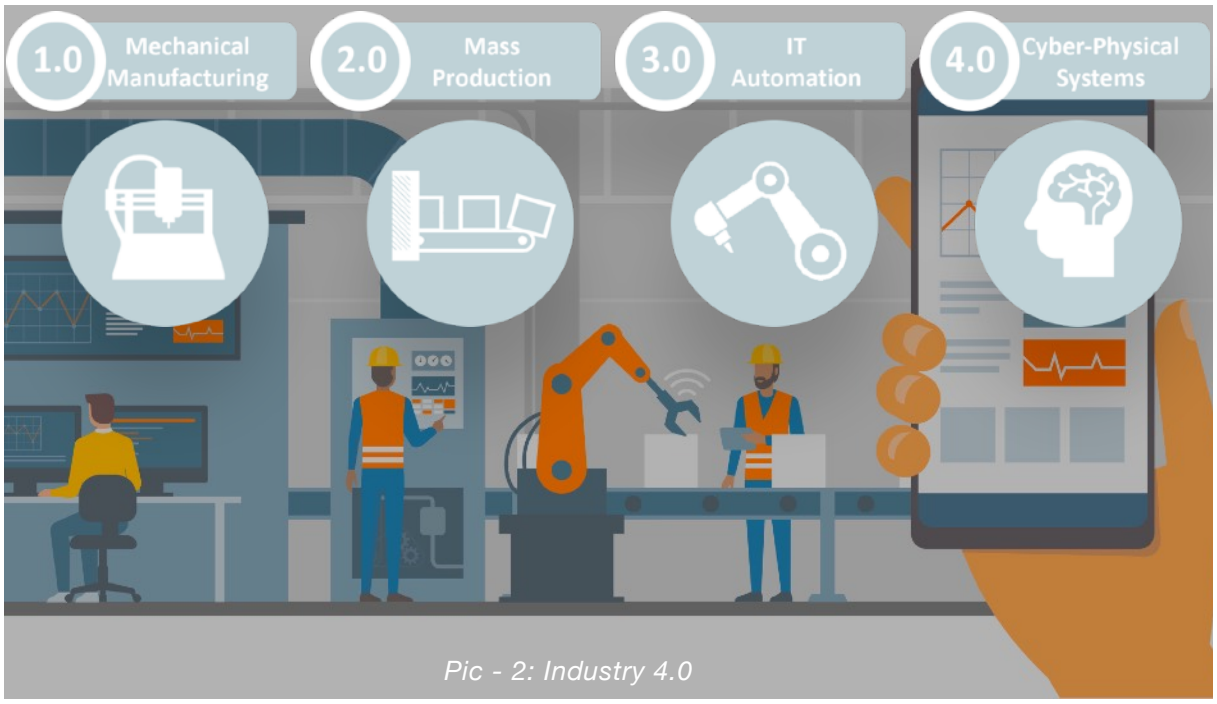
In the years that have followed, targeted ransomware attacks have been developed that are specialized for ICS disruption or takeover, which demand Bitcoin ransoms in exchange for encryption keys that allow files to be recovered – examples of this include Snake/EKANS and DoppelPaymer. One recent example of a totally modern ransomware attack took place in May 2020, when two major fuel suppliers in Taiwan were hacked. The intruder acquired admin privileges for each company's Active Directory, which they used to spread the ColdLock ransomware. All employees at headquarters were unable to access the company's online systems, and customers had to pay for gasoline by cash until the system could be restored.

From January of 2020 to October, 57% of ransomware attacks were in manufacturing or in healthcare, with a ransomware attack taking place somewhere on the internet roughly every 14 seconds[1] .

Pic - 1: Changes in the ICS Threat Landscape

The Fourth Industrial Revolution: The Age of ICS Targeted Attacks

One example of leveraging sensor data collected over the network to revolutionize performance is the ThyssenKrupp elevator company's move to link their elevators to IoT sensors and data aggregation. Microsoft provides them with an IoT service, called MAX. This service allows them to conduct predictive manufacturing, totally streamlining maintenance and repair, as well as "potentially reducing downtime by up to 50%"[2].



Pic - 2: Industry 4.0

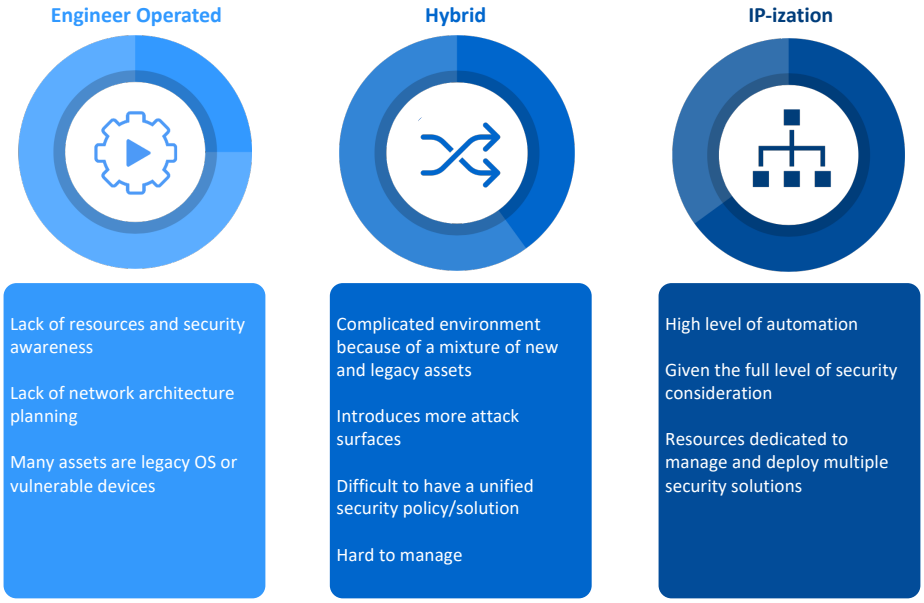
Within this fast-developing set of technologies, emergent concerns include closing the gap between Information Technology (IT) and Operational Technology (OT), strengthening the manufacturing process, and using data analysis and prediction results to create what has come to be known as a "smart factory". However, digital transformation is not a one-time process – it will continue to be a journey that requires long-term investment, with the promise of rich rewards at its end.

Careful consideration of defense is necessary because integrating an organization's record keeping and organizational IT infrastructure with its process-focused, operation-oriented OT is a standard practice at modern work sites. This integration increases convenience and availability while also creating a number of potential attack surfaces with potentially devastating vulnerabilities. The convenience created by running a factory HMI by smartphone can cut both ways, giving equal benefit to you or an intruder.

Hackers will use any path they can find to overtaking assets of any kind. After that, they can disrupt production, demand a high ransom for encrypted files, or blackmail stakeholders with stolen data. Such intrusions pose a threat to assets and facilities, as well as create safety concerns. In the near future, cyber attacks will be conducted with the specific goal of endangering human lives.

The Phases of Automation

The manufacturing industry can be divided into three different stages of digital transformation: engineer-operated, hybrid-operated, and computer-operated (sometimes called “IP-ization” because it gives an IP to every asset). Modernization and automation maturity are both based on the adoption of technologies or methods that are designed for computer operation. The adoption rate for asset owners is heavily affected by CAPEX and OPEX – and as automation increases efficiency and output, these are two very good reasons for long-term thinking.



Pic - 3: The three different stages of digital transformation

Examining these three stages from a cybersecurity perspective shows totally different security challenges, and totally different attitudes in response to cyber risk.

In the first phase, engineer-operated, the most common security issues for work sites are usually related to insufficient budget, resources, and experience to deal with cyber security issues, or that their existing network environment was deployed with flat network architecture. Factories in the second phase of transformation, hybrid-operated, have their own unique security concerns as well. Running a mixture of new and legacy assets creates new and sometimes startlingly vulnerable attack surfaces. Take, for example, the VPNFilter malware, which compromised (new) routers to target (legacy) SCADA systems.

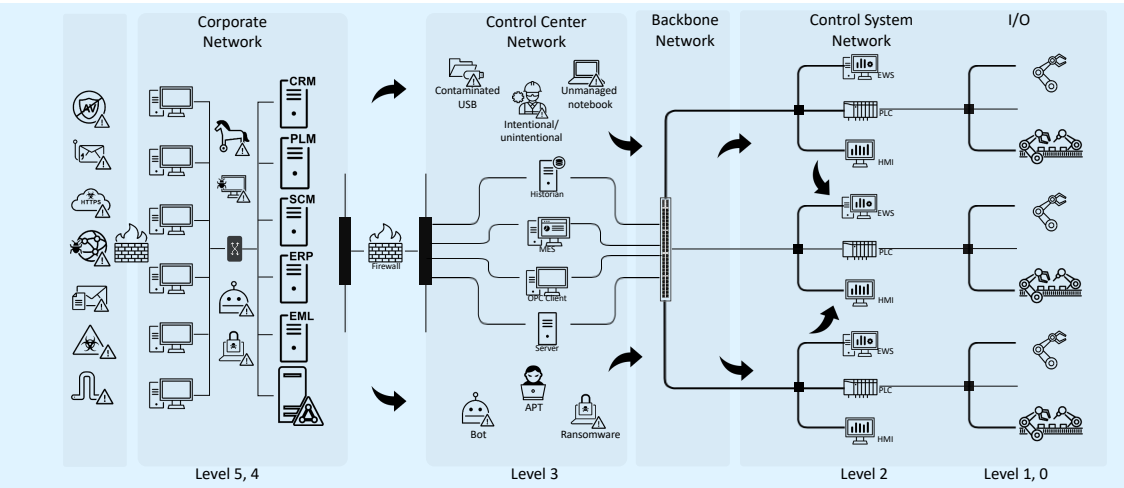
As a work site transitions into the third and most up-to-date phase of automation maturity, computer-operated, two main issues need to be resolved: network architecture and the management of endpoints. Typically, computer-operated factories will be running fully realized and planned cybersecurity, which will include multi-layered protection, detection, and response (since they highly depend on sensors), as well as data and network connectivity for the purpose of decision and prediction. Computer-operated, highly-automated work sites have a unique, particularly serious potential weakness: any single point of failure is going to severely impact the automation cycle. With one process locked up or otherwise unable to be completed, the plant’s entire operation comes to a grinding halt. For this reason, it’s necessary to prepare failsafety and redundancy to pursue total availability.

Threat Exposure: Open Season on ICS

One of the most common supposed foundations of ICS defense is reliance on an air gap. Assumptions about the effectiveness of an air gap lead to less-developed planning and deployment of security countermeasures. Many security risks are found in every ICS environment without exception (personnel, for example). An air gap is primarily at risk if it's either run using unsophisticated management strategies or faces sophisticated APT attacks.

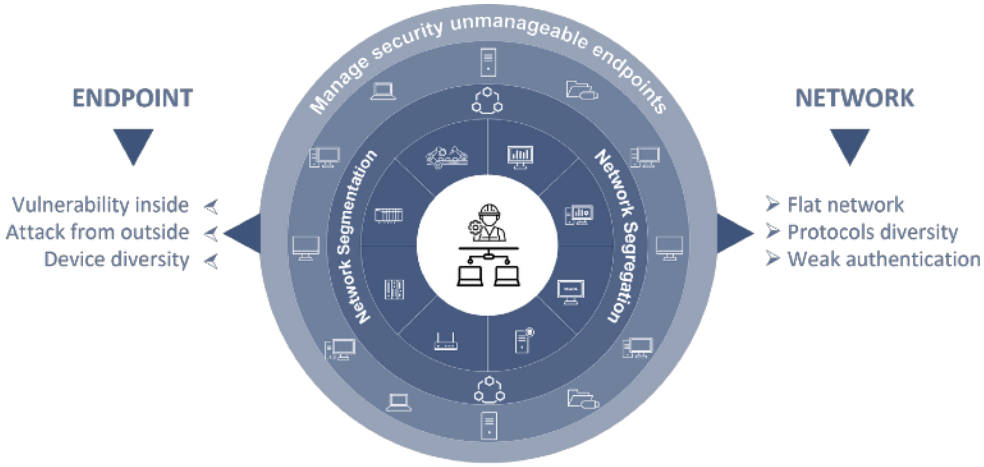
Among other things, unsophisticated management strategies allow workers unnecessary opportunities to damage the ICS environment (intentionally or unintentionally) or to steal sensitive information. Mobile devices which move between air-gapped environments such as USB sticks for data transfer and laptops for maintenance, require excellent management. Either of the two can be a perfect vector for malware transmission.

Dealing with sophisticated APT attacks is very challenging, especially when legitimate credentials have been hijacked or stolen. The threat actor will be doing everything they can to get enough time to accomplish their goals, which, in order, are to conduct necessary reconnaissance, to access the ICS network, and then to deploy a bot or ransomware to finish the job.



Pic - 4: The air gap myth

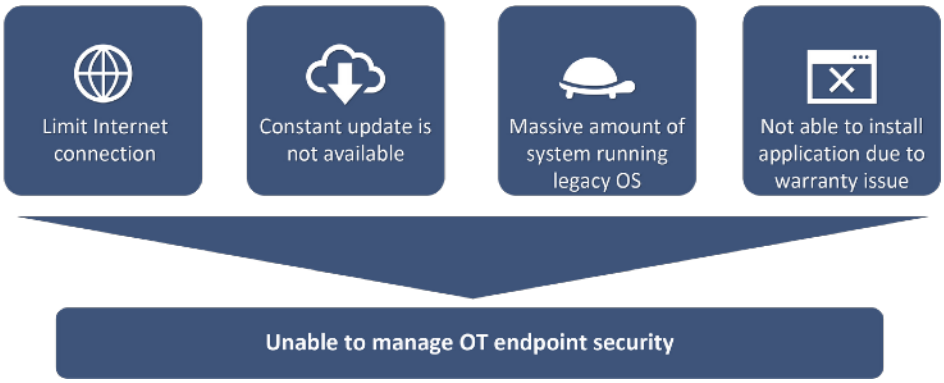
Many diverse industries require OT networks at their work sites. Though they might vary widely due to their differing needs, there are at least two things that they consistently have in common: endpoints and networks, both of which must be protected while still maximizing productivity.



Pic - 5: Common ICS weaknesses

Commonly, ICS endpoints are the weakest link in ICS network security, because there are many outdated ICS endpoints in the environment performing critical operations or functioning at decision points in the production line. Operating systems well past their End of Service date, such as Windows XP or Windows 7, can be seen in the ICS environment. On these legacy systems, updates and patches are no longer released, meaning newly-discovered vulnerabilities are no longer repaired. Every legacy system is a sitting duck.

Processes that are life-critical or otherwise could lead to endangerment create another unavoidable constraints for engaged ICS endpoints. These endpoints are subject to special warranties or regulations, and installing additional applications would void the warranty or break the law. The pharmaceutical industry, for example, has many such assets. A cyber incident on such a device is very serious – but, because of the device's delicate nature, it's not possible to install antivirus applications. A special solution is necessary to maintain and safeguard such systems.



Pic - 6: ICS endpoint security issues

The essence of ICS network architecture is based on availability rather than security – productivity is the main consideration in most decision-making processes. As a result, industrial control network architecture is rarely designed with defense in mind, and is often flat. Previously, organizations could run their ICS this way and rely on 'security through obscurity' – attentive readers will know that reliance on security through obscurity is now a relic of the distant past. In order to improve performance and availability, ICS network protocols tend to avoid encryption or skip authentication. On the other hand, the diversity of proprietary ICS network protocols can severely complicate network segmentation or trust listing.

(1) Industrial control network architecture does not consider information security for zone management or even detailed level isolation.
(2) The software and firmware of critical assets running legacy systems are no longer updated, meaning newly-discovered vulnerabilities will not be patched.
(3) Many industrial control communication protocols are not encrypted, which also makes it easy for hackers to manipulate factory operations and disrupt production.
(4) For a variety of reasons, traditional IT security solutions are unsuitable for industrial control environments.

Presently, the security risks that IT and OT networks can encounter when integrated are clear. According to our threat researchers at TXOne Networks, industrial security solutions must be constructed with the requirements of OT as their foundation so they can be integrated into the operational process. Instead of IT solutions which can complicate the OT environment, OT solutions must be tailored to the ICS environment from the ground up.

Purpose-Built OT Cyber Fortifications

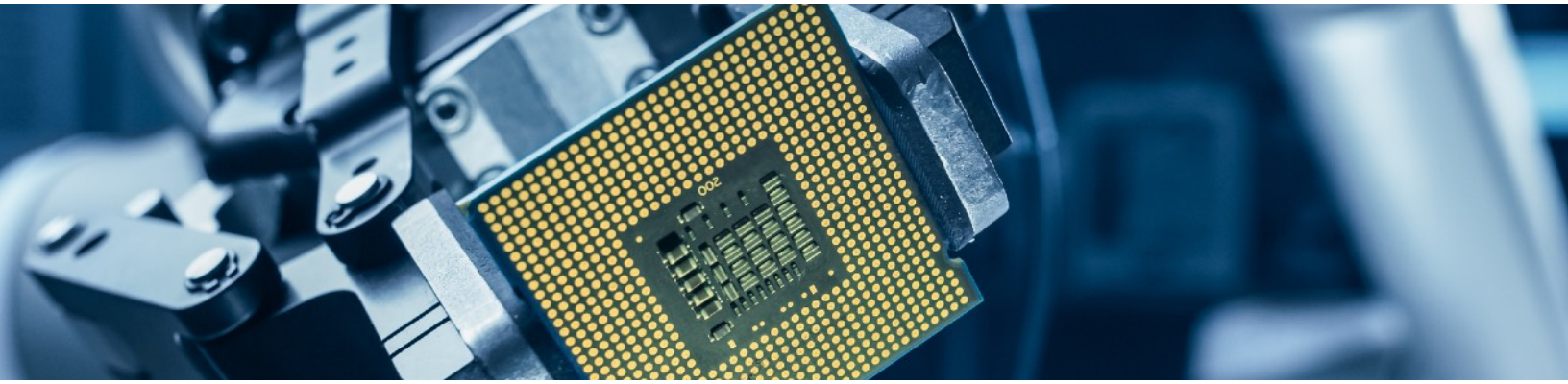
Work site stakeholders are extremely familiar with their own needs and processes, and more often than not have total mastery of their operations. Similarly, cybersecurity experts bring in familiarity and awareness that is essentially necessary to warding off modern cyber attacks. A dedicated in-house team can provide equally good support if given the necessary resources and preparations, however since 2017 (maybe even since 2010), it will always be necessary to consult the most current and up-to-date cyber threat knowledge both for building a secure operational foundation and keeping it secure while it's put into use.

The NIST Cybersecurity Framework version 1.1 was made publicly available on April 16, 2018. This framework provides an excellent reference model for categorizing the functions of cybersecurity activities: Identify, Protect, Detect, Respond and Recover. For ICS-specific cybersecurity, the NIST 800-82 v2 Guide to Industrial Control System Security was published in May 2015.

These comprehensive security guidelines are defined into 5 major sections:

(1) Overview of the Industrial Control System
(2) CS Risk Management and Assessment
(3) ICS Security Program Development and Deployment
(4) ICS Security Architecture
(5) Applying Security Controls to ICS

Setup and deployment are based on two guiding principles: 'Build It Secure' and 'Keep It Secure'. When we 'Build It Secure', the current ICS security posture must be identified, allowing discovery of weaknesses and development of both a system and a framework to address a firm's cybersecurity needs. It's vital to start with a solid foundation before building or deploying security countermeasures. The best way to 'Build It Secure' is to form a dedicated team and seek the expertise of an external



consultation service. 'Risk Assessment & Security Management' and 'Security Architecture' are both categories under the umbrella of the Build It Secure approach.

We can think of 'Build It Secure' as creating a defensible, rock-solid foundation for our ICS security framework. When the OT environment goes into full operation, though, and can be exposed to versatile and adaptive threats and threat actors, 'Keep It Secure' takes over as the day-to-day priority. TXOne Networks' team of research specialists see securing both networks and endpoints in ICS as the lynchpin of practices developed to 'Keep It Secure'.

As is well-known by now, cybersecurity requires operational continuity to deal with constantly-evolving attacks – this is where Keep It Secure comes into play. To Keep It Secure, it's necessary to have a well-established foundation and a well-planned framework for developing and deploying solutions. One commonly-recommended practice is seeking the guidance of experts in selecting and deploying solutions.

Build It Secure		Keep It Secure	
Risk Assessment and Security Management	Security Architecture	Security Program Development	Security Control

• Risk management process
• Consider the impacts of ICS incident and process in Safety System and Connected Systems for covering 1.) Safety, 2.) Physical and 3.) Non-digital aspects.
	• Management
	  • Establish business cases and cross functional team
	  • Define charter and scope for the expectation
	  • Define security Policies and Procedures
	• Engineering
	  • Security Risk Management Framework implementation
		• Networking
		• Defense-in-Depth Architecture
		• Firewall policies
		• High Availability
		• Security, Privilege and Resilient
			• Applying Risk Assessment Framework to ICS
			  • Categorize, Selection, Implementation, Assessment, Authorization and Monitoring
			• Guidance on Application of Security Control on ICS
			  • 18 Control families and privacy control

Pic - 7: Build It Secure and Keep It Secure

Throughout the journey of digital transformation, organizations will be facing similar challenges as they work to secure both networks and endpoints. For this reason, organizations that aggregate cybersecurity knowledge by looking at multiple environments, situations, and vulnerabilities provide some of the most reliable resources to defense strategies. TXOne Networks has developed solutions based on three key technologies to safeguard ICS networks and endpoints: Network Segmentation, Virtual Patching and Trust Lists.

Network Segmentation

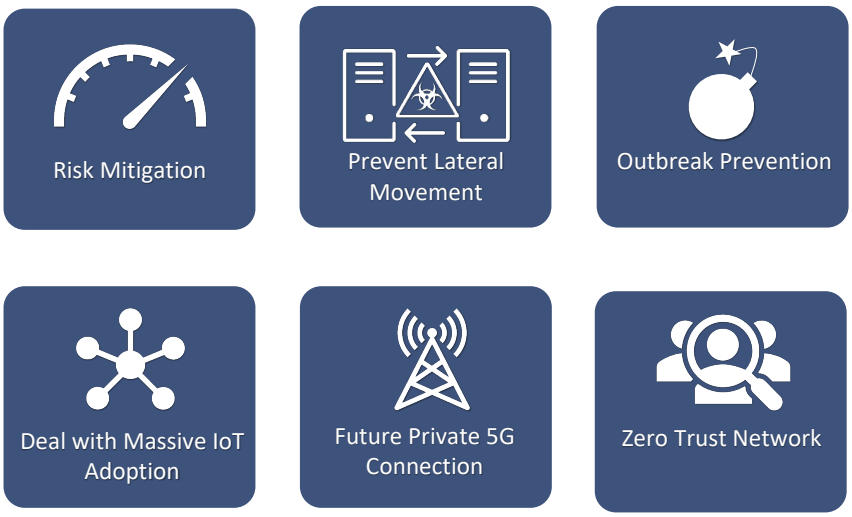
The ‘Network Segmentation’ mentality of network architecture is similar to building a bank building with its purpose in mind. An ideal bank building is set up with visibility, clear and practical routines, and defensive countermeasures in mind at all times. Elevators, stairs, hallways, and entrances are placed and organized with the knowledge that any point in the facility can either help or harm an attempted attack, raising the bar on defense across the board by delivering a much more easily defensible foundation. This way, during an attempted robbery, both employee safety and bank resources are protected. Similarly, to the modern cyber attacker, an OT network built without Network Segmentation in mind is like a bank without properly-placed windows, without well-placed and attentive security staff, and with more entrances than strictly necessary.

Having proper network segmentation in place within an ICS environment reduces threat impact and significantly increases ease of management. From a security point of view, network segmentation mitigates risk while preventing malware outbreaks or lateral movement by threat actors. Imagine being able to maintain factory production line continuity even when one part of the system has encountered a security incident. Compare this to traditional security countermeasures which are highly dependent on block lists, and which have a lot of difficulty repelling unknown attacks without constant signature or pattern updates. With network segmentation, even unknown attacks have limited impact potential.

In addition to security, network segmentation offers a significant improvement to availability management for factory environments with large-scale IIoT adoption. Network segmentation is also used to separate the control path (which is two-way) and the data path (which is one-way). This mitigates the risk from the uncertain security of newly-purchased IoT devices while maximizing their ability to collect data without potential interference in case of compromised nodes. This arrangement is designed to limit potential functionality available to intruders.

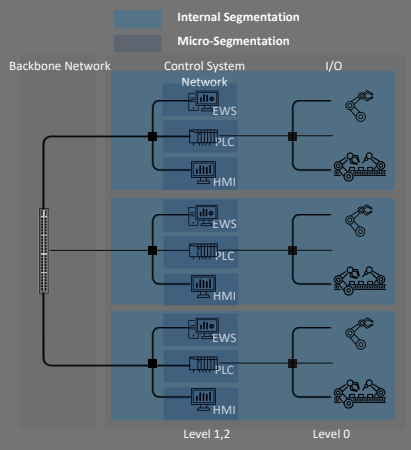
Another change in the landscape in the near future will be the price drop of private 5G. This is another incentive for asset owners to cost down operations that require long distance network connectivity. Conducting network segmentation to accommodate mobile edge computing is an effective way to make it much more difficult for intruders to gather intel and plan an attack.

The tremendous security potential of zero trust methodology is another reason why network segmentation is so important to mention. Asset owners should limit and minimize access privileges for any device, endpoint, user, or network with the assumption that other security countermeasures will fail. With that in mind, preparation should be made well in advance of a threat situation. When managing access privileges on a work site, keys are provided to employees on the basis of need. Cybersecurity must be run with the same concept in mind – open privileges, which were once common in network environments, must become a thing of the past.



Pic - 8: Why network segmentation?

Network segmentation has two complimentary levels: Internal Segmentation and Micro-Segmentation. Internal Segmentation is for large-scale areas or zones, and will depend on the available technology, bandwidth, and protocols in use to define the scope. Similarly, micro-segmentation is when technological solutions allow you to narrow down the area or zone that will be protected to a smaller scale or even down to a single asset.

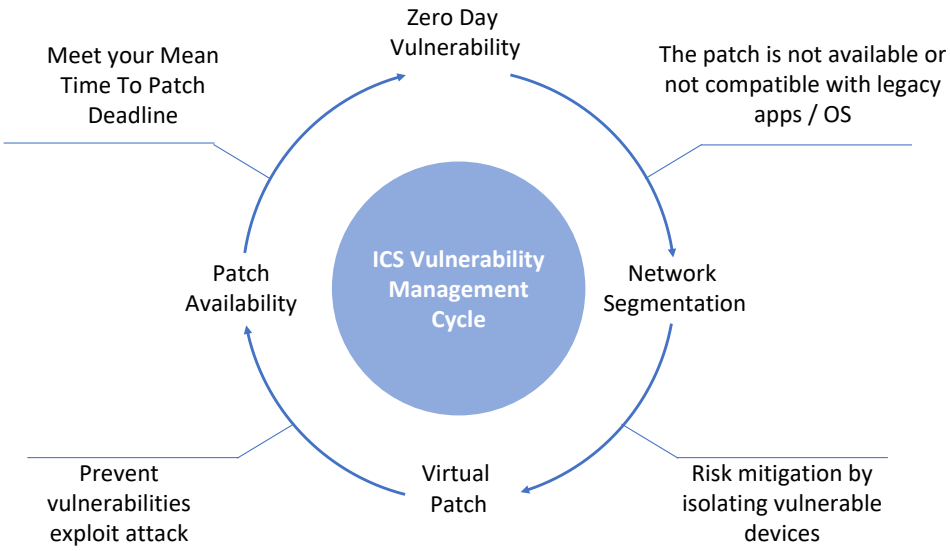


Virtual Patch

According to Trend Micro's Zero Day Initiative, the average mean time to provide a patch (MTTP) is 60 to 150 days[3]. This allows threat actors a window within which to launch an attack based on such exploits. This is just one of several complications to conducting agile patch management in an ICS environment. Additional concerns include what to patch, how to patch it, and when to patch it. Constantly decisions must be made to balance confidentiality and availability.

Through virtual patch technology, one can secure assets regardless of when their creator is able to release updates, making MTTP much less of a concern and making it possible to prioritize both productivity and security at the same time. Virtual patching can be implemented for endpoints by host-based IPS or network IPS. Such appliances have rule sets specifically designed to repel attacks leveraging known vulnerabilities without forcing endpoints to conduct a system update, meaning no system reboots and no production downtime.

Virtual patching reduces the impact from unknown attacks both by limiting their impact and allowing for signature updates as soon as our threat researchers learn of the vulnerability – usually a matter of days.



Pic - 9: ICS Vulnerability Management Cycle

Network segmentation and virtual patching establish well-rounded defenses against attackers seeking to exploit ICS vulnerabilities. They also reduce the impact from unknown attacks both by limiting their impact and allowing for signature updates as soon as our threat researchers learn of the vulnerability – usually a matter of days.

The ICS vulnerability management cycle illustrates the process of handling ICS vulnerabilities. The zero-day vulnerability is no stranger to most cybersecurity specialists, and handling these kinds of vulnerabilities demands a fast response, well-planned process, and a procedure for conducting patch deployment.

There are several dependencies to consider before patch deployment, especially when dealing with a zero-day vulnerability:

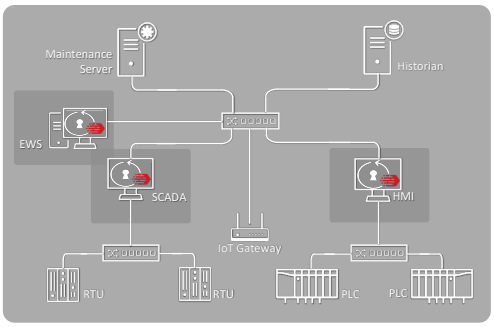
(1) Is a patch available?
(2) If a patch is available, is it compatible?
(3) Does the environment allow for the patching process to be conducted?

Any of these dependencies can become an obstacle to the patching process. This is another situation where adopting network segmentation has an immediate benefit – it allows for isolating or aggregating vulnerable assets into a safe zone that is more easily kept away from zero day attacks.

In some cases, such assets play an important role in the production line, so taking them off the grid is not allowed even when there is risk exposure. In such situations, virtual patch allows those assets to be secure and productive at the same time. When the patch package is available, both network segmentation and virtual patch can extend preparation time to patch while engineers conduct testing, and after that an organization's patch management plan can be used to deploy the patch.

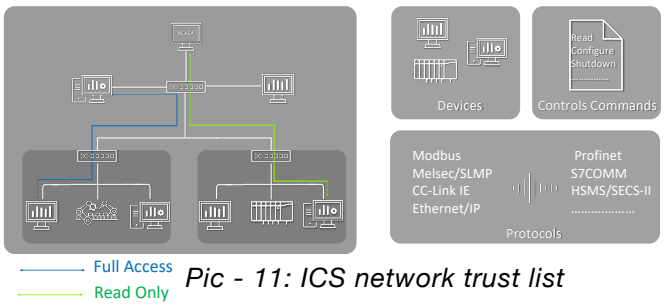
Trust List

Finally, setting up trust list control on both networks and endpoints will be the ultimate countermeasure to maintain both cybersecurity and productivity for an ICS environment. One cybersecurity challenge endpoints often face is that limited network access makes regular updates impractical. In such cases, traditional anti-virus is little help. A trust list is an expedient alternative solution, with no updates necessary to lock down the endpoint and limit the applications, processes, and configurations. In general, if we compare ICS endpoints with generic multi-purpose endpoints, it is much easier to conduct a lockdown procedure on single-purpose or "fixed-use" endpoints. This countermeasure avoids increasing computational strain on the endpoints, as well as not requiring constant anti-virus signature or pattern updates.



Pic - 10: ICS endpoint trust list

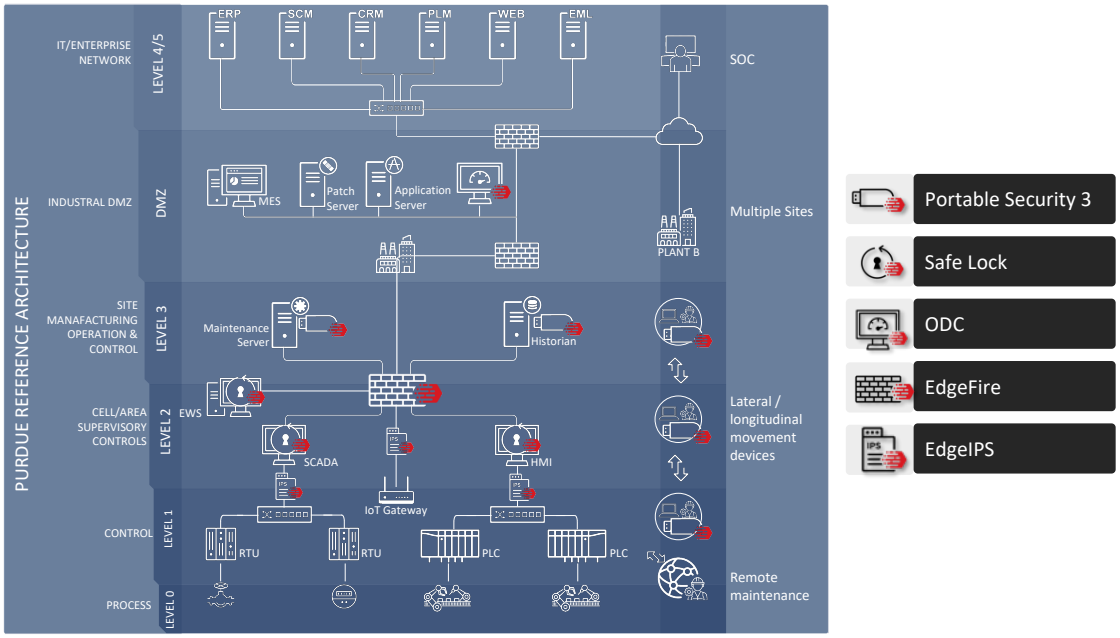
For the network, trust lists are similar in concept but making use of different elements: devices, protocols and commands within the protocols. For example, a technician can set up the network trust list so that HMI A can only use the Modbus protocol to communicate with PLC B, as well as applying read-only or otherwise customized privileges.



Pic - 11: ICS network trust list

Solution Deployment

Based on the Purdue reference architecture, these solutions can be fully deployed on Level 3 and below to protect the network and endpoints of the shop floor environment.



Pic - 12: Solution deployment

Conclusion: Building Resilient Networks and Endpoints from the Ground Up

The most important issue for cyber security leaders to understand and respond to is the need for defenses adapted to the unique requirements of each work site ICS. It should also be kept in mind that stakeholders do not need to “reinvent the wheel” – there are many organizations that work around the clock to aggregate and deeply understand the facts of cutting-edge cybersecurity. The digital transformation of high-tech manufacturing can improve efficiency and provide economic advantages, but cyber threats loom menacingly throughout the transformation process. The damage left in the wake of a successful attack goes far beyond the cost of protection. Disruption of production, theft of intellectual property, and leakage of sensitive information are all on the line.

Reference

1. Jacquelyn Bulao, *"How Many Cyber Attacks Happen Per Day in 2020?,"* techjury, July 28, 2020.

2. thyssenkrupp, *"thyssenkrupp and Microsoft turbo-boost digitalization of global elevator industry,"* thyssenkrupp Elevator, April 10, 2018.

3. Trend Micro, *""Zerologon" Understanding the Issues and Applying Solutions*," Trend Micro, September 16, 2020.

Created by
The TXOne Networks Technical Marketing

TXOne Networks Inc.

TXOne Networks is a joint-venture company of Trend Micro and Moxa. TXOne Networks is mainly offering cybersecurity solutions to protect industrial control systems. Trend Micro has more than 30+ years of cybersecurity threats intelligent and MOXA has more than 30+ years of OT network expertise, which makes TXOne Networks have both IT and OT technology to provide the comprehensive adaptive ICS cybersecurity solution. TXOne Networks leverage those advantages to develop the ICS cybersecurity products including endpoint security and network security, both Trend Micro and Moxa are not just providing the technology and knowledge, they are also taking care the go-to market channel for both sales and support service in IT and OT

txOne networks

Keep the Operation Running

www.txone-networks.com