wurldtech
A GE Company

Network Segmentation for Industrial Control Environments

A Wurldtech White Paper

Wurldtech, A GE Company | March 2016

Introduction

In 2015, there were 10 billion “connected” Internet of Things (IOT) devices. By 2020, the number is expected to skyrocket to 34 billion.[1]

For industrial “things,” this level of connectivity means an expanded use of advanced analytic techniques to boost productivity and efficiency, lower cost and downtime and, ultimately, increase profitability. Unfortunately, it also means an expanded attack surface and greater risk of successful cyber attacks within critical infrastructure environments.

No doubt, cybersecurity is a must. But where to start?

Network zone segmentation: It’s a foundational building block of any modern industrial cybersecurity practice. That is, so long as it’s applied in a manner that befits the specific needs of industrial control system (ICS) and operational technology (OT) environments. Otherwise, as connectivity continues to increase, the risk of successful attacks will continue to rise, while the efficiency and profitability advantages of digital industrial investments slowly wane.

Segmentation 101: Origins

The roots of network segmentation run deep in enterprise IT environments. What began as a way to improve network performance and bandwidth (through better management of the broadcast and collision domains of shared network devices and better containment of network traffic on respective sub-networks for each workgroup) has today evolved to significantly support a proactive network security practice.

This evolution is important because perimeter defense—which only accounts for traffic going in and out of the network—is no longer enough. Once an attacker or malware penetrates the perimeter and gains a foothold, consequent lateral movement within the network is usually a foregone conclusion.

The takeaway: More protection is needed *inside* the network, precisely where segmentation and its zone-specific policies play a crucial role; e.g., an accounting system zone might have one set of policies; an engineering zone, a different set.

According to ISACA, “A common technique to implement network security is to segment an organization’s network into separate zones that can be separately *controlled*, *monitored* and *protected*.”[2]

- Control—to limit the spread of an attack or mitigate the damage to a particular network segment.

- Monitor—to alert an IT team to the threat and specific anatomy of the attack.
- Protect—to stop attacks from spreading and further harming the broader network, critical assets, and the organization at large.

Proper segmentation enhances an organization's security posture and helps harden the controls network. Without it, or without enough of it, successful hacker attacks can result in tremendous loss of data as well as corporate reputation.

Now that OT networks are becoming increasingly connected, the attack surface is widening, and increased risk is likely. But unlike in IT, OT environments such as steel mills, power plants, pipelines, rail yards and hospitals have much more at stake: safety of people and multi-million dollar critical infrastructure, productivity and the environment, to name but a few.

Let's discuss OT segmentation in more depth.

Why OT Network Segmentation Is Different Than IT Network Segmentation

Unlike in IT environments, where a successful hack can result in data loss or damage to a corporate reputation, the stakes are higher in OT. When attackers target steel mills, power plants, pipelines, rail yards, or hospitals, defense is about multi-million-dollar critical infrastructures, critical assets, the environment and, most importantly, human safety.

Still, while we know network segmentation is a fundamental component of cyber security, the problem remains that it's difficult to implement in an industrial control environment.

Why? Three reasons:

1. Air gaps are fading.
2. Perimeter security is insufficient.
3. IT tools and techniques don't work in OT networks.

Air gaps are fading

In the past, when systems were completely isolated (both physically and virtually), there was air-gapping for security. Today, with the evolution of industrial systems, mobility, cloud technologies and multi-vendor environments, everything's changed; air-gapping is going the way of the bison.

In Wurldtech's 10+ years of experience conducting industrial and OT site assessments, we've found that nearly every site thought to be air-gapped was, in fact, connected to the Internet. In short, air gaps are a security-measure myth.

Another myth is that all insiders are trustworthy and competent. According to a SANS 2015 survey of industrial cyber security practitioners, insiders were the largest identified source of infiltration/infection, at 25 percent. Unidentified sources was the only higher grouping, at 44 percent.[3] A high insider threat and lack of visibility into other incident sources should lead any organization to question relying on an air gap that may or may not be intact.

Perimeter security is not enough

Industrial system devices must communicate with one another, as well as with other sub-system devices. As this creates multiple perimeters within OT environments, it shows how traditional perimeter security (one protective shell around the entire system) is insufficient. A better plan is to give each group of systems (each with its own unique set of security requirements) its own unique set of granular protections.

Figure 1 illustrates how each level can be a separate zone, and how a zone can include a subset of elements from multiple levels. It also depicts the information flows from level to level (or zone to zone) via conduits (i.e., connectivity between zones).

Step one is to establish the proper zones with clearly defined and enforced security policy; step two, to properly secure the conduits with granular network traffic inspection.

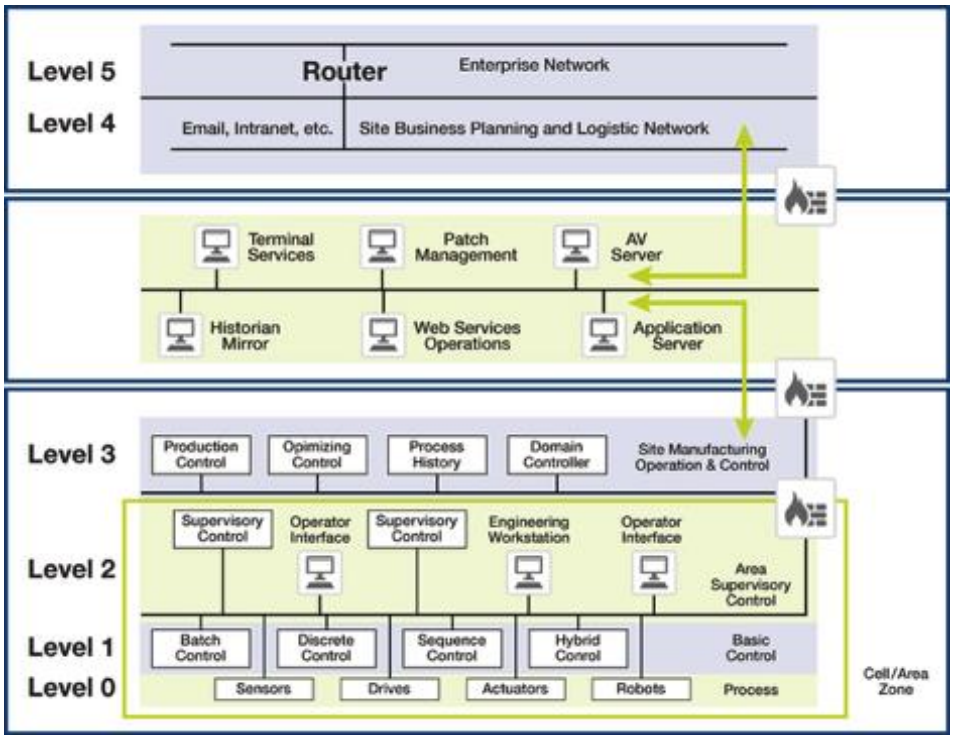

Figure 1. Purdue Reference Model for Computer Integrated Manufacturing (CIM)

IT segmentation technologies do not fit OT environments

Whether an entire level or a collection of cross-level elements, each zone has its own perimeter. While this might, at first blush, make typical IT segmentation seem like a good strategy, we know it's not. Why? Because we also know IT technologies simply weren't built to work in OT environments.

VLANs and Routing

Traditional segmentation mechanisms using VLANs or routing can become very complex, very fast. To start, in order to configure new IP addresses and ports that accommodate VLANs and IP subnetting, an OT environment must be brought down, or scheduled during a maintenance window. From a cost perspective, the required downtime and/or equipment reorganization makes this an impractical option. What's more, the complexity increases the risk of misconfiguration and employee error while the necessary overhead could overwhelm an operations team already strapped for OT security skills and resources.

If these issues weren't enough, it's also important to consider how automation vendors may dictate specific layer-2 and layer-3 designs. Any new network segmentation can fall outside the supported reference architecture and, thus, be disallowed. Bottom line: Traditional IT-style segmentation is not feasible for deep zoning of industrial systems.

Even if VLANs and routing were to work in OT environments, they still fall short in terms of security efficacy. While effective in directing network traffic and containing it within designated zones, these technologies do not provide insight or enforce security policy for network traffic. Specifically, they can't answer:

- Does the traffic contain malware?
- Does the network traffic use a legitimate command for an unauthorized, malicious, or otherwise dangerous purpose?
- Is a command issued to leverage a device vulnerability to launch an attack?

IT Firewalls

To secure and segment network traffic, many would recommend IT firewalls. However, though IT firewalls may offer network security and segmentation capabilities, they've been designed to inspect IT protocols, not OT protocols. Essentially, this means IT firewalls cannot "see" what's happening on an OT network and can neither enact on commands or payloads nor interpret context to understand whether a packet or set of packets is authorized.

At best, a limited number of next-generation firewalls might be able to identify a few OT protocols associated with a data flow, but that's about it. This level of visibility cannot detect wrongful commands or harmful payloads. Simply detecting

that there *is* an OT protocol doesn't make anything actionable from a security perspective.

Ideal Segmentation for ICS Environments

The basic goal for segmentation is simple: Create boundaries or zones around groups of assets and/or data, so that specific policies can enact on those zones based on business requirements. Unfortunately, available segmentation options (e.g., VLANs, routing, IT firewalls) fall short of OT security requirements.

For successful security, a new zoning approach is needed, one that focuses on the specific characteristics and challenges of OT environments.

Easy virtual zoning without OT network reengineering

For OT environments, a network segmentation solution must enable easy zone-level separation in a centralized manner. Any requirement to physically move equipment for proper segmentation is not only impractical, but out of the question. Critical devices are bulky and/or remotely located. A solution must, instead, be able to segment a network virtually or logically, even in instances where equipment resides at different sites.

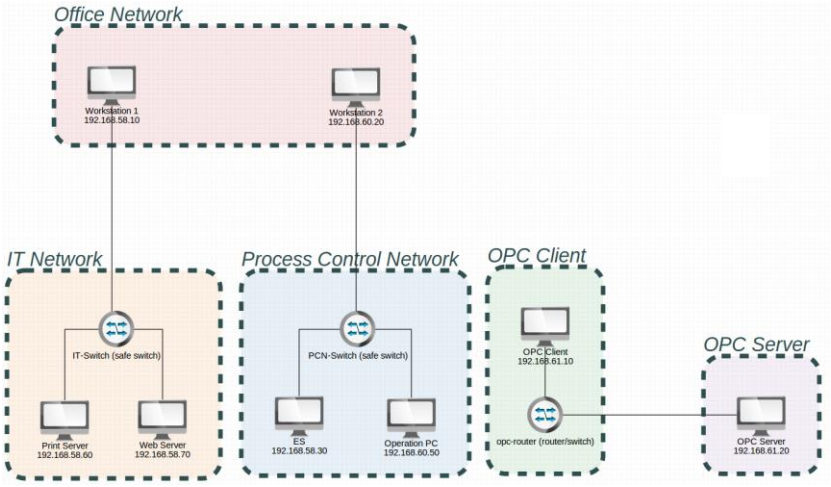

Figure 2: Zoning example

Additionally, a solution needs to feature an intuitive graphical user interface (UI) such that segmentation can be completed, as necessary, remotely. The UI should include an easy drag-and-drop feature that easily enables OT personnel of any skill level—and without extensive IT security training—to accomplish zoning objectives.

Lastly, the segmentation process cannot require OT network re-engineering or re-configuration. Any changes that would take the network offline or cause

disruptions to production are unacceptable.

Zoning with deep OT protocol inspection

To properly filter and inspect network traffic across zones, a solution must understand the communication languages of industrial environments, namely the relevant OT protocols (e.g., Modbus, DNP3, OPC and others). That's step one: protocol recognition.

The next step is deep protocol inspection. It's critical to consider the fact that legitimate protocol commands can be used for illegitimate purposes. Indeed, whether a network-based exploit, denial of service attack or an insider assault, each uses legitimate traffic in illegitimate ways. Deeper scrutiny into the full context of each data flow is what can help give a glimpse into malicious intent or accidental misconfiguration; and must consequently extend to each packet bit (every "0" and "1") to include the header (e.g., source and destination addresses) and the payload (e.g., commands such as read, write, reset, power on, power off, etc.).

Purposeful or not, incorrect execution of control commands can lead to dire consequences and cause physical damage to a network's critical assets. Therefore, a solution must be able to make decisions to allow, alert or block OT network traffic based on the full context of the packet—including the protocol, industrial application, command, addressing, sessions, normal vs. anomalous or malicious traffic and more.

Zone-specific OT security policies

Zones must enforce policy specifically created for a particular OT environment. Each network has its own unique combination of standard and proprietary protocols, multi-vendor industrial control systems, and various locales around the world. Security policy must conform to the network, and not the other way around. In other words, you can't afford to make changes to the network for the sake of zoning when policy should be transparent and seamless to deploy.

To build security policy tailored for your OT environment, look for a solution which includes a baselining capability that records all OT network traffic and can determine what normal traffic should look like so that each zone can be protected from malicious or even anomalous behavior (as represented by employee error or device misconfiguration). In addition, choose a solution that can automatically create security policy from the baseline.

Ideally, the solution needs to understand the full context of OT protocols, be able to complete virtual zoning remotely and centrally, and enforce security policy that's easily customized for each unique OT environment.

Take the First Step Towards ICS Network Resilience

Network segmentation is a core building block of a mature cybersecurity profile. In fact, it will do more for reliability and safety than almost any other available security measure.

With Wurldtech technology, system operators and integrators can define and implement segmentation that is specific to OT environments. They will be able to isolate systems into functional groups with similar security requirements and establish proper zones and conduits. This type of isolation not only makes unauthorized access and exploitation of critical devices much more difficult, but, should a breach occur, can help minimize its impact.

Contact Wurldtech for an evaluation of your operational technology environment, and learn how to best segment your network to enhance your security posture and promote safer networking.

End Notes

[1] http://www.businessinsider.com/34-billion-devices-will-be-connected-to-the-internet-by-2020-2016-1

[2] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf

[3] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf

About Wurldtech Security Technologies

Wurldtech, a GE company, works with both device manufacturers and system operators to provide protection for industrial and operational assets, process control networks, and critical infrastructure against persistent and dynamic cyber threats. Customers across oil and gas, power, transportation and healthcare use Wurldtech's operational technology (OT) cyber security products and services to reduce the risks and costs of a cyber attack, maximize system uptime and meet compliance mandates.

For additional information please visit our website at **wurldtech.com**.

Wurldtech Security Technologies
PO Box 49133
Suite 2000, Four Bentall Centre
1055 Dunsmuir Street
Vancouver, BC V6E 3V7

Tel 1 877 369 6674
info@wurldtech.com

wurldtech
A GE Company