Modernization of Manufacturing with Cybersecurity at the Forefront

by

Francesco E. Mangano

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
(Computer and Information Science)
in the University of Michigan-Dearborn
2018

Master's Thesis Committee:

Professor Di Ma, Chair
Assistant Professor Birhanu Eshete
Assistant Professor Feng Zhou

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMP	Advanced Manufacturing Partnership
APT	Advanced Persistent Threat
AV	Antivirus
BYOD	Bring Your Own Device
CC	Cognitive Computing
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System
CRM	Customer Relationship Management
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoS	Denial of Service
DRO	Digital Risk Officer
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GTAI	German Trade And Invest
HIP	Host Integrity Policy
HMI	Human Machine Interface
HTTP	HyperText Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICS	Industrial Control System
ICS-CERT	Industrial Control System-Cyber Emergency Response Team
IDC	International Data Corporation
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
LAPS	Local Administrator Password Solution
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MAPI	Manufacturers Alliance for Productivity and Innovation
MES	Manufacturing Execution System
MITM	Main-In-The-Middle
ML	Machine Learning
MPLS	Multiprotocol Label Switching
MTU	Master Terminal Unit
NAC	Network Access Control
NCCIC	National Cybersecurity & Communications Integration Center
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OT	Operational Technology
PC	Personal Computer
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controllers
PDM	Product Data Management
PLM	Product Lifecycle Management
RACI	Responsibility Accountability Matrix
RDBMS	Relational Database Management System
RDS	Remote Desktop Services
RTU	Remote Terminal Unit
SAM	Software Asset Management
SCADA	Supervisory Control and Data Acquisition
SCAP	Secure Content Automation Protocol
SCCM	System Center Configuration Manager
SCM	Supply Chain Management
SD	Software Defined
SFTP	Secure File Transfer Protocol

SIEM	Security Information and Event Management
SM	Smart Manufacturing
SMB	Server Message Block
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TELNET	Teletype Network
UBA	User Behavior Analytics
URL	Uniform Resource Locator
US	United States
USA	United States of America
USB	Universal Serial Bus
VACL	Virtual Access Control List
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firecall
WAN	Wide Area Network

Abstract

With the proliferation of Industrial Control Systems (ICSs), manufacturing processes have improved over the last 30 years, however, the organizational focus to securely exchange and process information to/from integrated systems has been consistently lacking. These environments continue to be susceptible to security vulnerabilities, despite history [15] showing that cybersecurity exposures in manufacturing have largely gone unaddressed and continue to rise [52]. This study evaluates cybersecurity challenges in the industry and proposes recommendations for practical and fiscally responsible defense-in-depth cybersecurity protections for manufacturing environments.

The business operating model, how ICSs became pervasive, as well as the major components that enable the operational technology (OT) were evaluated. With an understanding of the traditional network architecture for the industry [37], the rapidly evolving challenges facing the industry were examined. These challenges are impactful to the traditional and slow to change manufacturing operating model that has not focused on the necessary cyber protections for their OT environments. In addition, the industry is now facing game-changing technological concepts such as advanced manufacturing and Industry 4.0 that bring new complex challenges and cyber threats, unfamiliar to most in the industry. This is all underpinned by an organizational divide where the personnel most knowledgeable with the modern technology and cyber risks, in the majority of cases, are not responsible for the OT architecture and security. These headwinds impact an industry which spends the least on IT and cyber security than any other industry, globally [22].

The cyber risks and challenges in the industry are diverse, spanning technological and organizational competencies, stemming from purpose built components which operate in an ecosystem where cybersecurity is an afterthought. As a means to close the gap, practical and reasonable recommendations to address these problems are discussed; some specific and unique to the manufacturing industry while others are fundamental applications discussed with a manufacturing industry lens, which are commonly ignored due to perceived complexity, cost or simply lack of awareness. Lastly, a number of these recommendations were selected for further evaluation and implementation; challenges, approach, benefits and outcomes are shared showing measureable improvements to the cybersecurity posture of the organization.

Chapter 1: Introduction

Modern manufacturing has entered a digital renaissance where factories are requiring reinvention to address changes in customer demand, increased global competition, and organizational constraints. Companies are evolving, not only to expand and gain market share but in some cases, to simply maintain an existing customer base in a highly competitive global business climate. While the traditional manufacturing sector has characteristics similar to other evolving industries being revolutionized by "digital everything", there are significant complex and unique differences. These organizations historically focus on ways to drive continuous improvement and investment through what are considered traditional methods (e.g. process optimization, lean factory, etc.). Manufacturing companies are now being forced to invest in information technology (IT) and cybersecurity efforts in a manner that is new and unfamiliar to the manufacturing vertical; to address the digital divide as it expands in an industry that is slow to change and adapt.

I have focused my career in leading organizations to develop effective and efficient IT solutions across multiple different subject matter areas, with my primary focus on infrastructure services. For the last eight years, I have worked for a global five billion-dollar industrial manufacturing firm; at the onset of my tenure, I was amazed by the lack of attention that the operational technology (OT) environment received from an IT controls and cybersecurity perspective. As I began to address these issues, I was introduced to suppliers and customers who had similar issues, many of which were from smaller organizations. In learning about their difficulties regarding abilities to provide reasonable and prudent OT cybersecurity services, I conducted additional research about these problems within the industry. I came to realize that this is a systemic problem across the industrial manufacturing vertical that is not getting enough attention given the magnitude of short- and long-term potential impacts. Thus the focus of this research.

Recently, I attended an industry roundtable event hosted by the manufacturers alliance for productivity and innovation (MAPI) in conjunction with the Indiana University School of Public and Environmental Affairs. Approximately 40 senior leaders responsible for IT/OT strategy and operations within the manufacturing industry attended the roundtable. The purpose of this roundtable was to explore critical issues being faced by the manufacturing industry such as, artificial intelligence (AI), machine learning (ML), technical standards, cybersecurity, and privacy to determine if there was a path via a public policy initiative to improve and modernize the manufacturing vertical for these game-changing critical capabilities. Through this discussion, it became even more visible that cybersecurity in manufacturing is an area that lacks proper levels of awareness, attention, and degree of understanding to drive change and institute fundamental cyber protections. Surprisingly, the majority of the concerns surrounded the perception that in order to provide adequate cybersecurity protections, sophisticated and expensive tools, as well as third-party services, were by default a necessity. As I explored this topic further with the group, it became apparent that many firms are uninformed and unaware that reasonable protections can be instituted by performing basic, fundamental tasks aligned with traditional IT industry best-practices. Through this discussion, I was able to confirm the validity of my initial hypothesis for my thesis; with additional research and education, that there are material improvements that can be gained by defining a set of practical recommendations, focusing on improving OT cybersecurity in within the manufacturing industry.

The primary focus of this research examines how this industry is approaching these new business problems, namely cybersecurity for smart factories. IT-enabled factories are at the center of many of these innovations, where stakes are high and protection of people, systems, and information are of paramount importance. Beyond the inherent business need(s) that an organization must solve for, measures must be implemented to protect against nefarious individuals who want to gain access in order to exploit the organization in some manner. Ideally, OT organizations would implement the recommendations of the International Electrotechnical Commission Standard for Industrial Automation and Control Systems, IEC-62443 [18], as well as the NIST Cybersecurity Framework (CSF) [7], providing a well-rounded, yet aggressive stance to digital protections for any manufacturing organization. The reality is that most manufacturing companies cannot afford the initial and ongoing investment (people, time, and money) and downtime to implement the breadth and depth contained within IEC-62443 and the NIST CSF. The research and recommendations presented herein strive to provide a practical approach to assess and implement the measures that can address these modern risks, considering realistic constraints in a hyper-competitive and under-invested arena.

Chapter 2: Overview of Manufacturing and the Cybersecurity Landscape

Within the manufacturing sector, the convergence of OT and IT in real-time within the manufacturing industry is known as smart manufacturing. By comparing traditional manufacturing to SM, a better understanding of how manufacturing companies operate will be established. The new and pressing challenges, which will push modern manufacturing organizations into becoming digitally driven, will then be explored.

2.1. Traditional Manufacturing

In order to understand the unique cybersecurity challenges being faced by a modern manufacturing organization, it is important to understand traditional manufacturing principles. Traditional manufacturing is simply defined as transforming raw materials into finished goods by some chemical or mechanized process [54]. There are a handful of key factors that differentiate the traditional manufacturing industry, not only from other verticals, but also from advanced manufacturing characteristics. For the purposes of this research, these concepts are not explored in depth, only summarized below in order to provide a base level of understanding.

Raw Material – At the core of manufacturing is the raw material that is required for the creation of the product. Whether the products being manufactured are finished goods, ready for end user consumption/use or components downstream in a complex supply chain, investment in raw material is at the core of manufacturing. In modern manufacturing, retaining the correct amount of raw material is key so that enough is on hand to create the necessary product. However, the material should not be sourced too early, as that would deplete or lessen an organization's financial position. An efficient, accurate and responsive supply chain is key to this delicate balance.

Inventory Levels – Manufacturing organizations must maintain some degree of inventory or safety stock in order to ensure that customer demand can always be met, even in uncertain situations where supply chain issues may arise. Forecasts are created that depict demand and production planning personnel ensure that the necessary product is available whether it be just-in-time or long-lead time items. Retaining too much inventory hinders an organization's working capital, while not maintaining enough inventory can lead to delays in meeting customer demand and the potential for loss of business.

Customer Demands – Depending on the business in question, meeting customer demand for manufactured product can fall into one of two categories. Within the first category, variance in customer requirements is very low and mass production is acceptable, provided normal order volumes can quickly turn into realized sales. These are typically commodity products that are expected to be directly used with a known use profile and a clear understanding of the consumer's expectations. Products can be produced in mass and placed into inventory well in advance of committed orders. In the second category, manufactured components are purpose built or custom engineered for specific use and conform to a high degree of customer variability. In this category, products are manufactured to the requirements of a specific customer demand.

Labor – In a traditional manufacturing organization, labor is typically the number one variable cost component of the goods sold. In 2012 a study by Kronos Incorporated, conducted by International Data Corporation (IDC) Manufacturing Insights, it was noted that across most first and second world countries, the manufacturing industry was the single most important industry as a driver for economic health [41]. Additionally, labor productivity was the main driver for success. Firms within a manufacturing vertical traditionally focus on training and continuous improvement as methods to minimize waste and increase productivity.

Compute Interfaces and Data – The advent of the integrated circuit chip allowed for manufacturing efficiencies to be exploited through supervisory control and data acquisition (SCADA), as well as ICS technologies. SCADA and ICS allow hardware and software solutions to be interconnected and monitored. The resulting data can then be gathered for further analysis, instrumentation, processing and automation in a real-time manner within a manufacturing facility.

2.2 Brief History of Manufacturing Origins and Industrial Control Systems

Industrial control systems were first developed to automate and control the states of analog devices. The first known use case of an ICS system can be traced back to the ancient Egyptian inventor Ctesibius who created a water clock in 250 B.C. that was much more precise than other methods at the time [8]. This invention is an example of feedback control, which is a simple type of ICS. Ingenuity and innovation continued as advancements in science and mathematics in the 1600s and 1700s facilitated the concepts of feedback loops, closed loops and control systems. This led to the development of many items, such as thermostats, steam engines and other purpose-built devices [15]. Much of 1800s' advancements built on the ideas of the men and women before them, iterating to create improved analog solutions. In the 1800s, significant progress was made in electricity, electromagnetic theory and conduction. These advancements led to controlling temperature, pressures and liquid levels for industrialized needs, such as hydraulic, pneumatic, and steam systems. These systems drove further advancements that ultimately led to the creation the first relay logic-based systems that laid the foundation for the advent of modern ICS architecture.

2.3 Architecture

ICS can take on different forms depending on the design requirements and the approach of the system integrator who is designing and building the solution. While there may be different design approaches, the majority of ICSs have the same core components. In order to understand the opportunities for improvement related to cybersecurity, it is important to understand these core components.

2.3.1 Major Components of an ICS

Supervisory Control And Data Acquisition (SCADA) – SCADA systems allow for large distributed measurements of control systems, centralized at a larger scale. Manufacturing organizations are no longer relegated to individual, distributed PLCs. Instead, SCADA can now collect, communicate, report and control across a system of networked PLC functions at scale [20]. SCADA allows for hardware and software solutions to be interconnected so that data can be monitored and collected for further analysis, instrumentation, processing, and automation in real-time.

Remote Terminal Unit (RTU) – With the new capabilities enabled by SCADA systems, there was a need to aggregate all of the systems for oversight and management purposes. Thus, RTUs were purpose built as highly resilient architectures to prevent SCADA systems from being negatively impacted. RTUs are traditionally deployed in remote locations and are equipped with wireless radio interfaces (wireless LAN, microwave, etc.) to support situations where remote wired communications are unavailable [57].

Programmable Logic Computer (PLC) – PLCs are microchip devices that monitor and control instruments using the input/output of instruments, sensors, actuators, motors, etc. PLCs were first used in the manufacturing industry in the 1960s in order to automate the changing of switches, sensors and control relays required to swap out different types of sheet metal. The automotive industry was booming and drove this requirement as the potential for different body materials increased [15]. PLCs have since evolved into sophisticated devices with the capability of directing complex processes used largely in SCADA and distributed control systems (DCSs). In SCADA environments, PLCs are less inexpensive and more adaptable than special-purpose RTUs [15].

Distributed Control System (DCS) – A DCS is a set of computerized systems that consists of geographically distributed controls within a factory. A DCS differs from a SCADA system in that a SCADA is a single controller located centrally, but in a DCS environment, each process or machine is managed by a dedicated controller [60].

Intelligent Electronic Devices (IEDs) – The need for third party bolt-on components acting as makeshift RTUs across multiple disparate SCADA architectures resulted in the industry creating new a standard. The International Society of Electrical and Electronics Engineers (IEEE) introduced a designation for IEDs, which consisted of an independent power system, a microprocessor and a communications port [15]. The IED was developed as an intelligent sensor/actuator that could obtain data, communicate with other devices and perform local processing [21]. An IED combines multiple inputs, outputs, controls and communication mechanisms in one device.

Data Historian – A data historian is a utility application that acts as a central database for aggregating all the information from an ICS. Information can be accessed to support different needs, from statistical analysis to enterprise resource planning (ERP) functions [57].

Human Machine Interface (HMI) – The HMI is a combination of software and hardware that allows factory operators to monitor the manufacturing processes and override operations in an emergency. The HMI displays process status information as well as historical information and reports for operators, administrators and other authorized users. HMIs can take on many different forms based on the use case. For example, an HMI could be a dedicated PC in a control center, a laptop connected via a wireless network or a browser on any system connected to the network [21].

Sensor – A sensor is a component of a larger subsystem, which detects a change in state or condition based on the variables in its environment. Upon noting a change in state (e.g. temperature, vibration, direction, etc.), a sensor will send a signal to a control system, such as a PLC or an RTU, for further analysis and determination of the next action, if any.

Actuator – An actuator is a component of a machine that is responsible for moving and controlling another component, mechanism or system. Actuators generally require a control signal and a source of energy to facilitate mechanical motion.

Remote Station – A remote station is a collection of sensors, actuators and control systems (PLC or RTU), which are dedicated to a specific purpose or function. A typical manufacturing operation will have numerous remote stations across a single operation.

Control Server – The control server executes PLC supervisory control software that accesses downstream control modules over an ICS network.

SCADA Server or Master Terminal Unit (MTU) – The SCADA server is the component that acts as the master control server in a SCADA system. Remote stations, RTUs and PLC devices typically report status, conditions and other information to these systems. SCADA servers act as brokers or as interfaces between upstream and downstream components within the ICS, as shown in Figure 1 below.

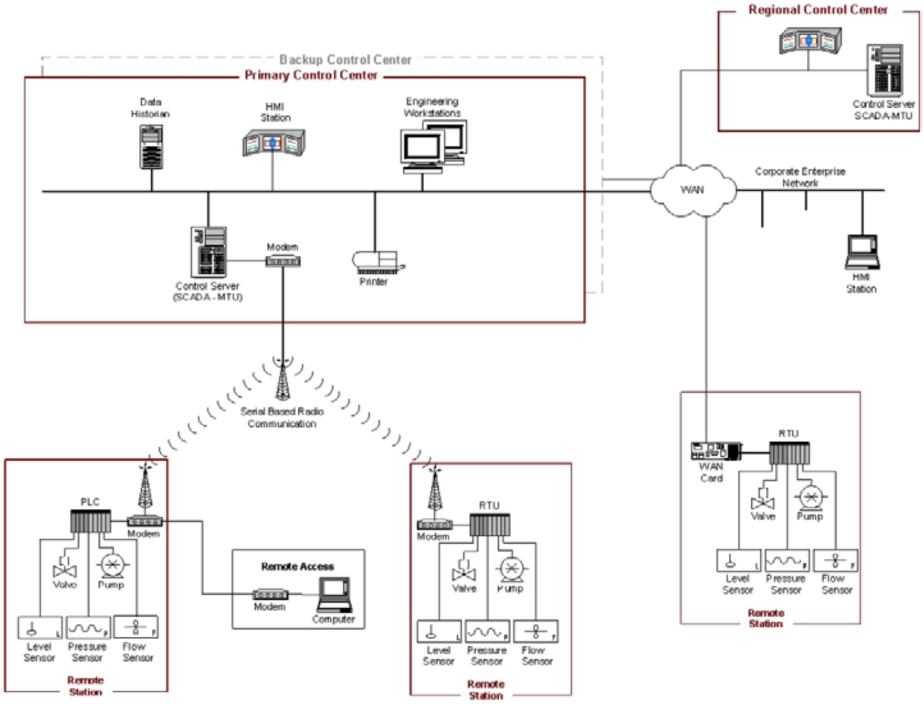


Figure 1: SCADA system implementation example [40]

Enterprise Resource Planning (ERP) System – An ERP system is a software application that leverages a database to manage and control important business processes as part of an operation. An ERP system traditionally covers multiple business functions, such as planning, purchasing, inventory, sales, finance and human resources.

Manufacturing Execution System (MES) – An MES is the wide-ranging platform that controls all the events within the manufacturing operation. Processing with an MES begins with orders from customers, planning and coordination of back office functions and the master schedule. From there the MES plans and drives the processes required in order to build the products in the most effective, low cost, practical and high-quality way. Functions that reside in most MES systems include, but are not limited to, scheduling, shop floor control, inventory tracking/management, material movement, maintenance management, time and attendance, costing, quality, document management, product lifecycle/data management, configurators, routings, engineering change control and supply chain management. MESs typically integrate into ERP systems for holistic management of the shop floor and business operations.

In a modern manufacturing environment, each of these components, as shown in Figure 2, are required to efficiently and effectively operate a manufacturing operation.

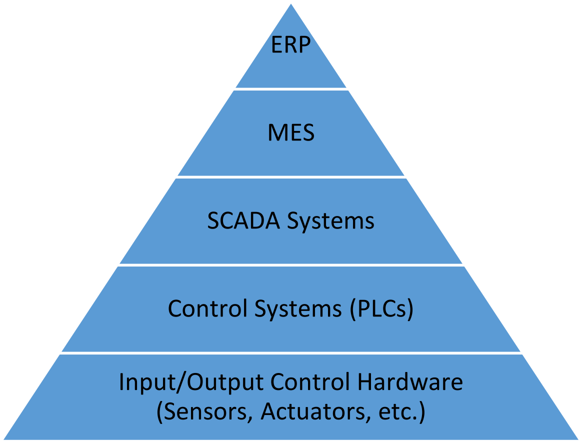


Figure 2: High-level architecture hierarchy of a manufacturing environment

2.3.2 Network Components

ICS environments can be architected with different components and connection mediums tailored to the specific needs of the engineered solution. Many traditional ICS environments use fieldbus networks to locally connect sensors/actuators to PLCs or RTUs, however, with IT influencing OT, modern connection methods have bridged these two ecosystems. While this has improved efficiency, lowered costs, and met customer needs, it has also caused a significant increase in security vulnerabilities exposed to the shop floor. Part of this study will discuss these attack vectors, the origins, and what can be done to protect manufacturing environments going forward without significantly impacting availability and efficiency. In order to discuss these topics, the major components of a typical ICS network must be understood.

Fieldbus Network - The fieldbus network interconnects sensors, actuators and other devices to a PLC, RTU or other microprocessor-based controller. Similar to traditional IT networks, fieldbus technologies eliminate the need for point-to-point cabling between the controller and each device. The devices communicate with the fieldbus controller using a variety of protocols, many of which are proprietary.

Control Network - The control network connects the higher-level components, such as the data historian, HMI and SCADA-MTUs to lower level control modules, such as remote stations, PLCs, sensors and actuators.

Remote Access Points - Remote access points are the entry/interface points of a control network for remotely accessing and configuring control systems on the Local Area Network (LAN). This can be in the form of laptops, mobile devices (tablets, mobile phones, etc.) or purpose-built terminals. The core trait is that access is granted remotely to the control system.

Router - A router is a communication device that sends packets (electronic data) between two networks. In a manufacturing environment, this includes, but is not limited to, LAN-to-WAN, MTU-to-RTU and long-distance communications across WANs for remote site SCADA communications.

Firewall - A firewall segments and protects devices on a network by filtering, monitoring and controlling packets using predefined policies based on source, destination, port/protocol, application/service and authenticated user

Modems - A modem is a communications device used to connect remotely to a computer or similar device over traditional telephone circuits. Modems are often used in SCADA systems to enable long-distance serial communications between MTUs and remote field devices, where high-speed WAN connections are not available or are too expensive. Modems are also used in SCADA systems, where gaining remote access for operational diagnostic and maintenance functions is necessary [50].

2.4 Traditional Network Segmentation Model for Manufacturing

Historically, manufacturing networks do not have the same architectural design and security-minded approach as enterprise or corporate networks. This is often a by-product of IT and OT being managed by entirely separate departments. For instance, manufacturing environments are built out of necessity by engineers looking to achieve a specific constraint-based outcome, rather than from an IT and cybersecurity best-practice perspective. Thus, it is not uncommon to find manufacturing networks with fundamental issues, such as unsegmented flat networks, a lack of firewalls implemented, and third-party equipment vendors with uncontrolled access to the manufacturing network.

In the 1990s, Theodore Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing developed the Purdue enterprise reference architecture (PERA) model, as shown in Figure 3. PERA was assembled specifically for the manufacturing industry in order to address the human and organizational aspects of an enterprise, from planning to operations. PERA is unique, as it considers both facility engineering and IT in a comprehensive enterprise-wide model for discreet and process manufacturing [37].

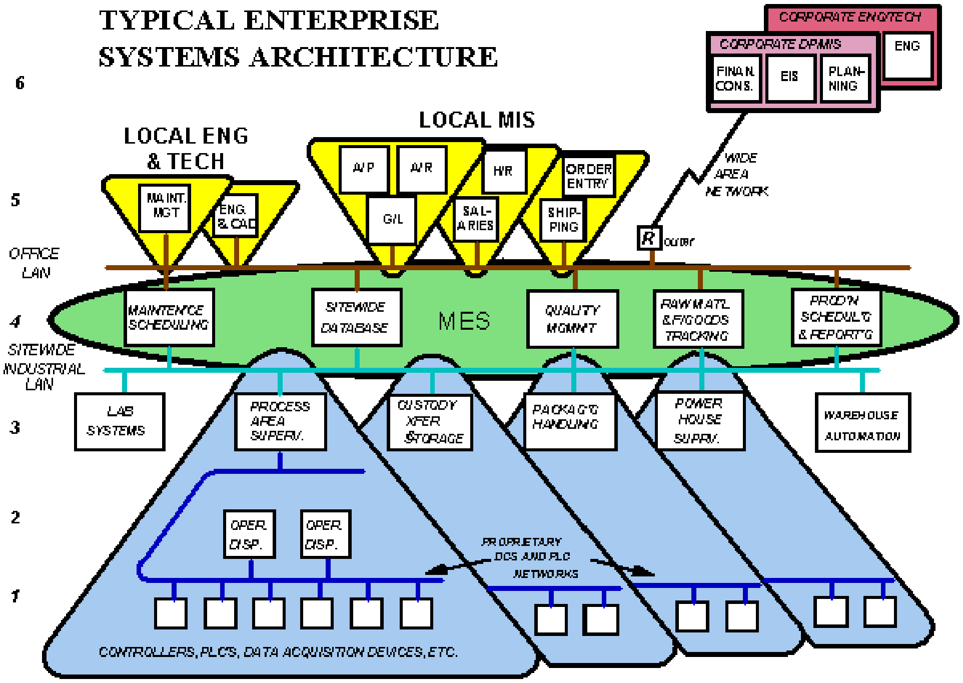
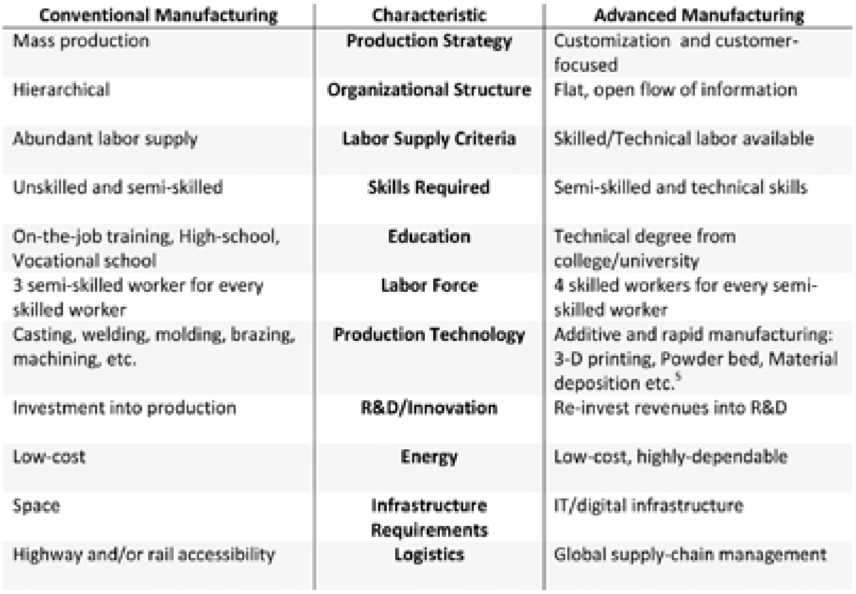


Figure 3: PERA sitewide network architecture [37]

As shown in Figure 3 above, levels 1 through 3 within the PERA model are comprised of components on the factory floor where the manufacturing process control functions reside. Level 1 consists of sensors and actuators, level 2 consists of PLCs and RTUs, which ingest the data from the sensors and level 3 consists of HMI devices, which control the processes being executed and measured. All components located on level 3 and below reside on a dedicated industrial/control network. Level 4 consists of the manufacturing management processes and related devices. Typically, the manufacturing execution system (MES) processes are located on level 4, including maintenance-scheduling, quality, raw material management, and reporting functions. Level 4 sits between the industrial network and the site's LAN for general back office functions. Level 5, within the site LAN, contains processes and related devices that perform functions such as engineering, finance, human resources, shipping and order processing. Level 6 is connected to the site LAN and represents all connectivity to other company offices, commonly via a WAN (MPLS, site-to-site VPN tunnels, etc.), where other upstream- or downstream-dependent functions reside as part of a larger distributed enterprise organization [37].

2.5 Advanced Manufacturing

Advanced manufacturing carries with it the foundation of traditional manufacturing concepts, however, it focuses on accelerating manufacturing practices through state-of-the-art applications of science, technology, processes, product design, and production [54]. A core belief in the advanced manufacturing world is that the competitive advantage will be held by those who innovate, adopt, and leverage technology at a continually increasing rate. Those who fail to embrace advanced manufacturing will be irrelevant, and thus will be relegated to niche products/markets, will succumb to an acquirer, or will simply go out of business. As shown in Figure 4 below, research conducted by Camoin Associates in a 2011 study compared key characteristics of conventional and advanced manufacturing [10]. While there were parallels affecting productivity between traditional and advanced manufacturing, every component in advanced manufacturing relied on technology.



Conventional Manufacturing	Characteristic	Advanced Manufacturing
Mass production	**Production Strategy**	Customization and customer-focused
Hierarchical	**Organizational Structure**	Flat, open flow of information
Abundant labor supply	**Labor Supply Criteria**	Skilled/Technical labor available
Unskilled and semi-skilled	**Skills Required**	Semi-skilled and technical skills
On-the-job training, High-school, Vocational school	**Education**	Technical degree from college/university
3 semi-skilled worker for every skilled worker	**Labor Force**	4 skilled workers for every semi-skilled worker
Casting, welding, molding, brazing, machining, etc.	**Production Technology**	Additive and rapid manufacturing: 3-D printing, Powder bed, Material deposition etc.[5]
Investment into production	**R&D/Innovation**	Re-invest revenues into R&D
Low-cost	**Energy**	Low-cost, highly-dependable
Space	**Infrastructure Requirements**	IT/digital infrastructure
Highway and/or rail accessibility	**Logistics**	Global supply-chain management

Figure 4: A comparison between conventional manufacturing and advanced manufacturing [10]

In a survey by IDC, the top three factors affecting the global manufacturing landscape were training, continuous improvement and investment in technology [41]. This investment in technology is not only a necessity in modern manufacturing, but it is the singular key enabler for relevance in a highly competitive space. Technology affects traditional manufacturing in immeasurable ways. Customers can now visualize 3D-printed scale models at the front end of a sales cycle. AI and ML can provide numerous real advanced insights such as visual quality inspection variances and predictive indicators regarding factory conditions. Advanced robotics can work alongside or in-lieu of human labor and augmented reality can be used to visualize designs or assist in numerous factory operations from stock room picking to advanced research and development. Technology is influencing how customers partner with firms to solve highly complex problems in every industry. It is also affecting how human capital evolves, for instance, from a utility-based model to a knowledge-based model on the shop floor. Manufacturing companies will continue to evolve at a new organizational pace as technology improves at a rapidly.

On June 24, 2011, President Barack Obama spoke at Carnegie Mellon University and initiated the Advanced Manufacturing Partnership (AMP). This was an industry-driven, national effort and a key component of the U.S. government's plan to further develop manufacturing opportunities and stave off the recent decline of manufacturing jobs in the country. This initiative involved the government, private industry and academia to identify the prevailing issues and the most impactful opportunities to improve technologies, processes and products across multiple manufacturing industries [42]. The focus on investing in advanced manufacturing has provided a renaissance of sorts to an aged and slowly evolving industry, which has been attempting to capitalize on a range of new opportunities. The opportunities all share a common constraint, which is the most important component of advanced manufacturing – the availability of a skilled, technology-enabled workforce. "The integration of technology and advanced machinery diminishes the need for 'unskilled' workers and increases the reliance on workers with the sophisticated skills required to operate the equipment. Advanced manufacturing training courses and programs in community colleges, technical schools, and even K-12 education systems are essential to supporting growth in the advanced manufacturing sector" [10].

Advanced manufacturing is an area receiving significant attention, especially outside of the United States. Germany is leading the charge with a federally-funded 2006 initiative, Industrie 4.0, where the aim is to lead industry-integrated solutions by 2020 with a target to increase productivity levels by 50% [12]. China is a close second with the Made in China 2025 initiative, which began in 2015. Its objective was to transform China into the global advanced manufacturing leader [27]. Both governments are heavily investing in this area, because of the value that digitally-enabled manufacturing will bring to local economies. In 2014, the United States followed suit and began the Manufacturing USA program to organize industry, university and government partners to grow U.S. manufacturing competitiveness and promote a sustainable national manufacturing research and development platform [28]. The U.S. program has been slow to evolve, as it aims to partner with private industry rather than push targets from the top-down, as it is done in other countries.

2.6 Industry 4.0

Advanced manufacturing is enabled and advanced by an ever-evolving world of interconnected objects. These interconnected objects interface with each other over a global footprint of technologies over traditional and modern mediums including LANs, WANs and cloud-based services. This manufacturing-based, automated information exchange is evolving, however, there are a few key components that make up such a system. Below is a sampling of the prevalent components receiving attention and being invested in today.

Internet of Things - At the core of Industry 4.0 is the IoT. IoT is the concept that every device, as basic or sophisticated as it may be in its normal, intended form, can be enhanced by technology to interface and communicate with other internetworked components. The advancements and additional innovations that can be made once these components are internetworked are seemingly endless. Within the manufacturing space, the industrial internet of things (IIoT) is a subset of the IoT, where large numbers of networked devices connect with each other to establish systems that can monitor, aggregate, share, analyze, and convey valuable information, which was previously unattainable or extremely complex and expensive to gather. At its peak, in a high functioning IIoT landscape, autonomous manufacturing becomes a reality, and robots either replace or supplement the labor traditionally handled by humans. IIoT is commonly associated with industries, such as oil and gas, power generation, and healthcare, where unintended interruptions can cause life-threatening or high-risk situations [9]. Conversely, the IoT tends to represent consumer-level, convenience-based devices, which do not carry life threatening or significant monetary repercussions.

Cyber-Physical Systems – A cyber-physical system (CPS) is a solution, where physical hardware and software are deeply intertwined. The unique, independent components with different behaviors interact with each other in multiple ways. CPS involves approaches from multiple disciplines, such as mechatronics, cybernetics and embedded systems. Examples of CPSs are autonomous automobiles, medical monitoring systems, advanced robotics, and autopilot systems. CPS is thought of a higher functioning architecture built on top of dependent IoT components [34].

Cognitive Computing – Cognitive computing (CC) incorporates the disciplines of artificial intelligence and signal processing. The technology mimics the functions of the human brain. It is adaptive, context aware, stateful, iterative, and interactive. CC traditionally contains components from machine learning, natural language processing, object recognition, reasoning, human-computer interaction, and narration [19].

Cloud Computing – Cloud computing is the concept that computing resources (compute, storage, memory, networking, etc.) can be provisioned and shared across multiple distinct entities. This provides economies of scale, which results in more readily accessible resources, quicker data processing (generally) and a reduction in the overhead to operate and maintain compute clusters. Rather than investing financial capital upfront, cloud computing uses an expense-based model where users can pay as the services are rendered. Most cloud services leverage a scale-out model, where smaller, denser servers are leveraged and can be easily added to as demand increases.

2.7 Information Technology vs. Operational Technology

The promise of smart manufacturing is considerable from an economic impact perspective. In a 2017 study by CapGemini Consulting, it was estimated that SM would add between $500 billion and $1.5 trillion in positive economic impact within the next five years [38]. While the potential of SM is tremendous, there are a significant number of issues, both technical and non-technical, that virtually all manufacturing organizations are facing. Specifically, the differences between IT and OT and how the related characteristics and organizational biases clash must be addressed for the benefits of SM to be realized. These factors in many cases have a direct impact on the organization's cybersecurity posture and exacerbate the problem, at times unnecessarily. Additionally, the business needs and approach are different enough to cause other downstream problems (skills, cost, process, etc.). As an example, in a 2012 interview of decision makers at 39 different North American utility companies, improving the IT/OT integration was a higher priority than planning for smart grid initiatives [14]. While there are parallels in IT and OT security, having a mature OT security posture is typically more critical, as the practices are used to protect people and assets involved in monitoring and controlling devices, processes and actions rather than simply data and information. In order to understand how to establish a set of recommendations to close the cybersecurity gaps within an OT setting, the differences between IT and OT must first be defined; see Table 1.

Table 1: IT vs. OT

	IT	OT
Purpose	Manage information, automate business processes	Manage (physical) assets and events, control plant processes
Culture	Adapts to frequent change, anticipates newer technology	Accustomed to long useful life, change requires significant testing
Focus	User experience, data and services, confidentiality, integrity, availability	Safety, reliability; people, environments
Success Targets	User satisfaction, budget compliance, on time delivery	Consistent solutions, longevity of solutions, deterministic outcomes, high fault tolerance
Architecture	Transactional, relational database management system (RDBMS), publishing or collaboration	Event-driven, real-time, embedded software, rule engines
Solutioning Approach	Assess requirements, develop standards, buy/build at lowest cost, plan for upgrades and support	Leverage vendor solutions / previous examples, optimize for performance and use
Interfaces	Web browser, PC, keyboard/mouse	Sensors, coded displays
Custodians	Chief Information Officer (CIO), infrastructure, application professionals	Engineers, technicians, plant managers
Connectivity	Corporate network, IP-based, web-based, mobile, wireless, cloud-enabled	Control networks —increasingly IP-based, wireless
Security Compliance	Imperative at all levels as part of a defense-in-depth strategy, harden everything inside the network and on the edge	Seen as an interference to manufacturing processes, leave the manufacturing network alone, however, secure the edge
Examples	ERP, supply chain management (SCM), CRM, email, online banking, collaboration, etc.	SCADA systems, PLCs, HMIs, control systems, monitoring tools

When assessing the cybersecurity impact on core technology characteristics, there are also key differences further emphasizing how OT must be treated differently. Table 2 below has been assembled to map OT characteristics and their related impacts on cybersecurity. The impact that the OT characteristics have on cybersecurity planning and design will enable business operations, yet protect the data and devices involved in the OT processes.

Table 2: OT characteristics and impact on cybersecurity

	OT Characteristic	Impact on Security
Default System Parameters	OT devices ship from OEMs with default configurations, which allow the device to operate in most environments without specialized configuration customization.	Default settings are typically not hardened or secured. There is a lack of hardening configurations, which can lead to access to default credentials, unnecessary open services, etc.
System Monitoring	OT systems are often monitored externally by specialized vendors and OEMs in order to maintain and certify tight control parameters.	The security perimeter needs to be designed and controlled with OT equipment vendors. External client VPN, persistent access to OT devices, etc. are all potential access methods required for manufacturing environments.
Latency	"Real-time" latency in the OT world refers to sub-millisecond responses compared to milliseconds in the IT world.	Controls intended to protect the environment, such as firewalls, virus-scanning products, etc. typically increase latency, thus potentially affecting OT operations.
Availability	In a manufacturing environment, it is not uncommon for an organization to run multiple shifts, even 24x7x365 (outside of any preventative maintenance cycles).	The requirements for high availability creates challenges in the timing of patches, updates, vulnerability scanning, etc. A high level of coordination and planning is required to meet the business's needs.
Asset Lifecycle	Within a manufacturing setting, it is not uncommon to have machinery and its related specialized computing equipment used for upwards of 15 to 20 years.	Software/firmware are often out of date well beyond a reasonable level. IT/OT teams need to implement a regular maintenance procedure in order to maintain a reasonable security posture.
Incompatibility With Security Software	In many cases, OT related devices are designed in a closed architecture, due to concerns with regulations, human safety and intellectual or proprietary property.	Additional security agents, clients or tools (e.g. anti-virus software, client firewall) cannot be used to protect the devices. IT/OT organization should look to implement compensating controls, where possible.

As shown in Figure 5 below, in a 2017 survey by Gartner, 350 executives were asked to rank the top three challenges that organizations faced when aligning IT with OT systems. The top challenge was *Division between IT and Operations,* followed by *Fear of security implications* and *Risk to processes/equipment integrity* [58].

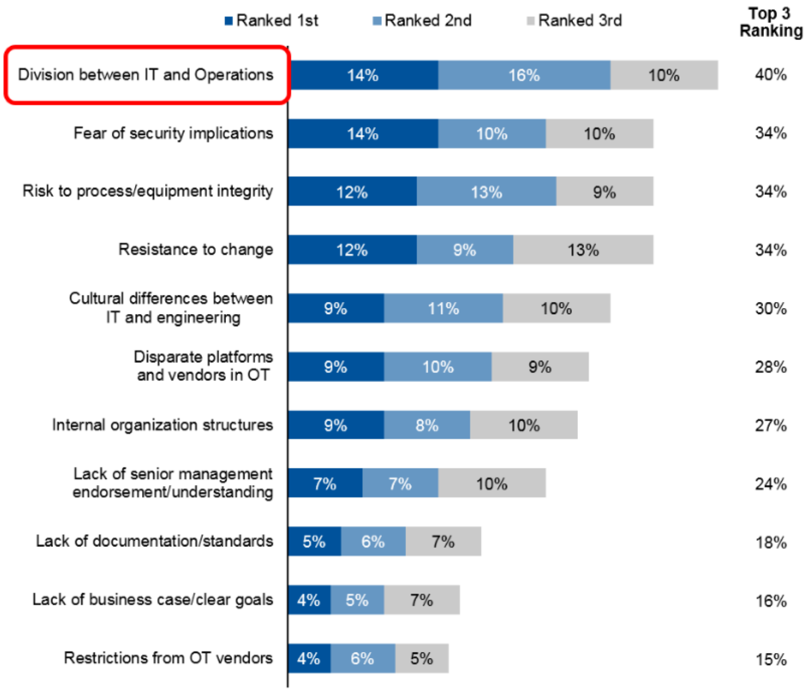


Figure 5: Top challenges executives faced when aligning IT with OT systems [58]

Understanding these different paradigms allows focus to be placed on the actions necessary to optimize both IT and OT in order to develop a model to improve the overall cybersecurity posture of the organization.

2.8 IT Spend for Manufacturing Organizations

Financial investment is a key driver for any organizational capability. IT and cybersecurity are no different, especially with technology evolving as frequently as every 12-18 months. In a 2016 study conducted jointly between Deloitte and the manufacturers alliance for productivity and innovation [62], 225 executives were interviewed regarding cyber-risk in advanced manufacturing. From the responses, it was determined that only 52 percent were confident that the proper protections had been put in place against external threats. Appropriate funding and talent readiness were cited as the key reasons for the lack of confidence. Furthermore, as shown in Figure 6 below, 48 percent of the respondents noted that funding was not adequate for the necessary cyber initiatives and 27 percent detailed that there was a lack of senior level support [62].

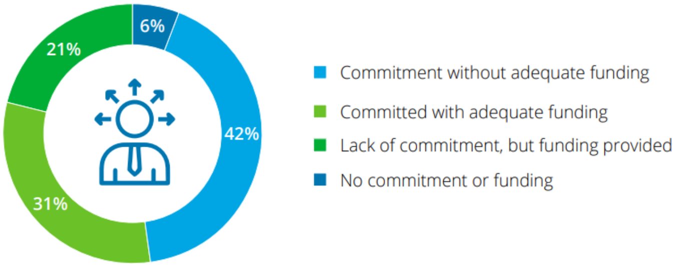


Figure 6: Senior support and funding for cyber initiatives [62].

Every industry is different as it relates to the amount of money invested in cybersecurity; some industries like high-tech and banking are on the high end and others like industrial manufacturing and retail/wholesale on the low end. While the level of financial investment does not provide a direct correlation to the level of cybersecurity readiness, it does provide a leading indicator of the level of commitment and senior executive acceptance of the realities of a digitally enabled workforce. Annually, Gartner releases their IT Key Metrics Data that tracks numerous various data points relating to technology trends and investment. As shown in Figure 7 below, industrial manufacturing is at the bottom with only 4.3 percent of IT spend dedicated to IT security, with all industries averaging out at 6.2 percent [22]. At the time of this research, there was no data available to measure OT security spend; this is currently viewed as a small subset of IT security bucket.

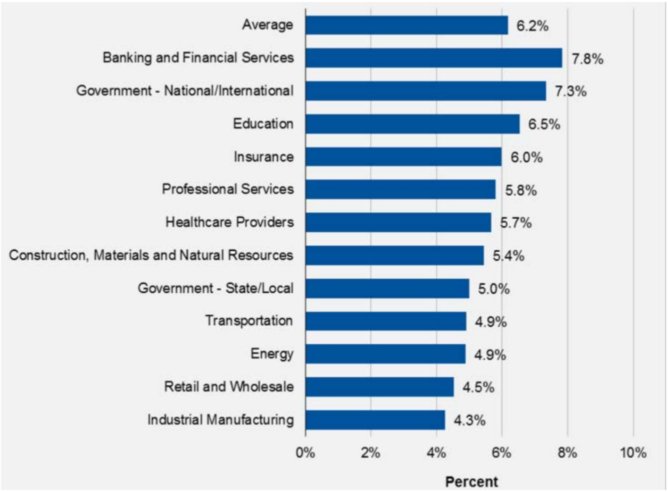


Figure 7: IT security spending as a percent of IT spending by industry [22]

Another thought-provoking metric relates to the amount of spend per employee. According to a 2017 Gartner survey, as shown in Figure 8, the average spend on IT security per employee was $1,171 across all industries; for the industrial manufacturing industry, the average spend was $190 [22].

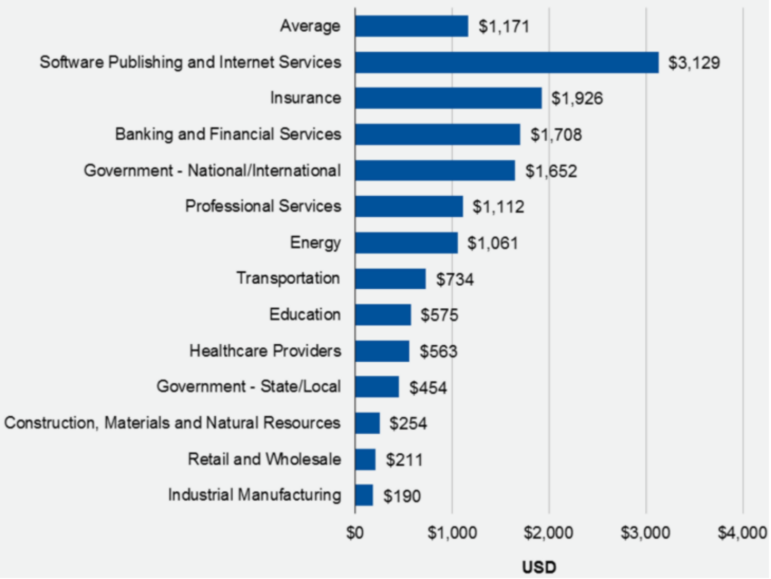


Figure 8: IT security spending per employee by industry [22]

As you can see through these metrics, the industrial manufacturing industry is on the low end of investment pertaining to IT security. This default position places additional hurdles in the way of providing a prudent defense-in-depth security posture.

Chapter 3: Review of Cyber Risks and Challenges Posed to Manufacturing Organizations

3.1 Introduction

Prior to the 21st century, the consensus was that malicious activity and cybersecurity would not affect manufacturing operations. This false perception was built upon the belief that OT systems were generally unimportant to those with nefarious intent. It was also based on denying that modern advancements had made OT environments vulnerable to IT threats. In this chapter, the risks and challenges affecting OT environments and organizations are assessed and evaluated.

3.2 A Sampling of Previous Cybersecurity Exploitations in Manufacturing Operations

Due to the long lifecycle of SCADA environments, most ICSs have little or no fundamental security protections built in. Until recently, security controls and related protections were not a consideration when manufacturing plants were designed and built. The related ICS systems lacked protections, such as authentication and authorization requirements. The systems did not require validation of code or commands downloaded to controllers that monitor and direct physical, and now cyber-physical, system operation. These systems used unencrypted protocols and often operated over networks that were not segmented. Attacks on OT and digital technology outside the IT space are real, prevalent and here to stay. Below is a small sampling of high-profile examples, which provide a real-life cross-section of IT issues in an OT setting.

- Turkish Oil Pipeline (2008) – A Turkish oil pipeline ignited without producing any warnings, sensor alerts or alarms. Those investigating the event found that malicious entities had hacked a security camera system's software to laterally move across the network and gain access to the pipeline's ICS network. Once access was gained, pressure within the pipeline was increased to a point where explosions were set off causing millions of dollars in damage. The attack was believed to be caused by the Russian government who opposed the Turkish pipeline [1].

- Stuxnet (2010) – Stuxnet was a targeted, specialized piece of malware introduced to Siemens PLC devices via a USB flash drive, thereby bifurcating any devices that were air gapped for security purposes. Stuxnet was the first malware to specifically target an industrial process [3], most notably impacting Iranian nuclear control systems. Manufacturing operations in Indonesia, India, Azerbaijan, the United States and Pakistan as well as a host of other countries were infected [45]. While no official credit has been taken for Stuxnet, it is believed to have been developed by the federal intelligence agencies of the United States and Israel within a classified program called "Operation Olympic Games," specifically targeted to affect Iran's uranium enrichment processes. Liam O'Murchu, the Director of the Security Technology and Response group at Symantec noted that Stuxnet was "by far the most complex piece of code that we've looked at — in a completely different league from anything we'd ever seen before" [11].
- German Steel Mill Cyber Attack (2014) – The German Federal Office for Information Security provided a report noting that a nefarious entity had penetrated a domestic steel facility. The malicious entity used a spear phishing email to infiltrate the enterprise network, laterally move into the ICS plant network and implement an advanced persistent threat (APT). The infiltrator caused various system components to fail, including critical processes, which resulted in significant physical damage to the plant [23]. No specific perpetrator(s) or motive have been identified to date.
- Power Blackouts in Ukraine (2016) – Portions of the Ukraine were without power due to a cyber-attack on one of the country's power systems via power supplier, Ukrenergo. Malicious entities gained access to the power company's IT network at least six months prior to the attack. The hackers worked to gain privileged access to the SCADA environment(s), scouring the landscape for ways to execute the attack. The infiltrators could have attacked a larger surface area of the environment, but were not entirely successful. It is worth noting that this is not the first hack of the Ukraine power grid. In 2015, a similar attack was conducted; both attacks were believed to be a direct result of Russian-led efforts [33].
- Honda and WannaCry (2017) – Honda halted production of multiple vehicles in a Japanese plant due to the WannaCry trojan. WannaCry is a trojan-based worm that spreads by manipulating weaknesses in the Windows operating system. Once installed, the

Ransomware payload encrypts files and demands a payment for decryption. Furthermore, WannaCry is self-propagating so once it is within a network it will attempt to use the file sharing protocol, server message block (SMB), to infect vulnerable hosts [36]. Operations at the Japanese plant were significantly impacted. Global operations in North America, Europe and China were not impacted, however, all reported to be infected [53].

3.3 Evaluation of Security Issues, Challenges and Risks Related to Operational Technology

In this section, several topics will be evaluated that affect the manufacturing industry. Each area of interest's problem or perception is discussed, as well as the correlating reality, to understand the impact of the problem or perception continuing onward.

3.3.1 OT Denial of Relevance Regarding Security Threats

Perception / Problem – There is a common denial that malicious parties have little or no interest in OT. This misconception is in part based on a sense of under appreciation for the value and importance of the OT processes, as well as the data/information generated by OT.

Reality – To a malicious entity, it makes no difference whether the system(s) being compromised are IT or OT based. It only really matters if it is a targeted attack, at which point the level of expected sophistication and potential impact are raised considerably. The parties with an interest in attacking OT cover a wide range of players with an even wider range of motives, from recreational hackers and political activists to resentful employees and organized criminal organizations.

There have been a number of presentations delivered by reputable parties bringing light to and explaining the threat vectors by which operational technology is vulnerable and relatively easily exploitable. CERT, the United States Computer Emergency Readiness Team, regularly discloses vulnerabilities directed at OT. Due to the continued rise in ICS-based attacks, in 2012 the Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT) was established to reduce risks across critical infrastructure sectors by collaborating with law enforcement agencies at every level (intelligence, control systems owners, operators and vendors). As of 2017, the ICS-CERT operates under the National Cybersecurity and Communications Integration Center (NCCIC) to collaborate with public and private sector CERTs in order to share control systems-related security incidents and mitigation measures [17]. In a 2016 Booz Allen Hamilton Industrial Cybersecurity Threat Briefing, and as shown in Figure 9 below, a 20 percent increase in ICS critical manufacturing related incidents was reported compared to the year prior, with expectations for the trend to continue to rise [52].

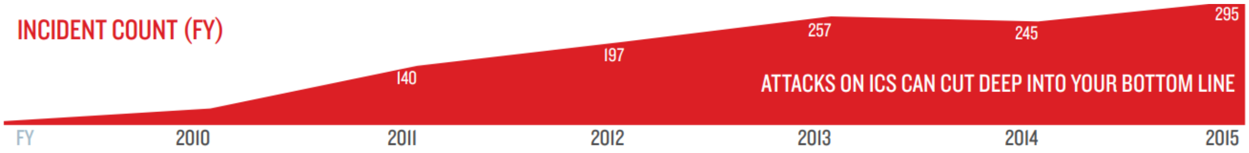


Figure 9: Critical cyber related incidents affecting ICS devices [52]

3.3.2 OT Protocols and Systems Are Secure By Obscurity

Perception / Problem – A perception that has been perpetuated is that OT networks, systems and protocols have been developed over the years from largely proprietary, standalone (e.g. Fieldbus, Modbus) technology, which has in some cases been insulated from the back-office enterprise networks. Furthermore, the notion that ICS-based solutions do not overlap with IT based architecture and solution design created a false pretense, which too many IT staff operate under [31]. These principles of an OT environment lead to a false sense of security, where IT professionals and the like believe that these systems and ICS solutions are obscure from attackers, and thus protected from malicious actions.

Reality - While there are examples of extreme isolation (e.g. air gap, no cross connectivity between IT and OT), it is not an accurate representation of most OT networks. This separation approach has led to the independent development of IT and OT networks, with interconnections between the environments, in some cases, connections managed by third party shadow-IT based vendors or plant managers. As noted in a study by Verizon Labs, "there is a varying amount of interconnection between OT and IT network environments with interdependencies between the two influencing the level of interconnection. While some organizations continue to maintain strict separation, most have begun to allow interconnectivity to occur in a much broader fashion" [31]. Plant managers and engineers are embracing this interconnectivity at a rapid rate as these advancements come with increased visibility to operations and accessibility to ICS systems across an enterprise. The challenges are that security weaknesses are more widely known, and exploitation of the systems is often easier, even on a larger scale [13]. These advancements make security a major concern, because many systems and devices in the OT domain were never designed, developed or envisioned to operate on an open standards–based infrastructure with a large degree of built-in security capabilities. Lastly, as the IT and OT models merge, historically OT protocols can be reverse engineered relatively easily [47]. The proprietary protocols are legacy and due to age, are widely understood and distributed as publicly available content. As OT protocols are compromised this would allow an attacker to dissect the control messages within the ICS architecture, as well as gain visibility to data being generated by the system.

Gone are the days of proprietary protocols and networks transmitting ICS data for a manufacturing operation. Standards based transmission protocols, such as Ethernet, TCP/IP, 802.11 wireless and Bluetooth are now the norm due to the seamless interoperability between IT and OT. As it relates to the applications that operate the manufacturing operations, COTS components, such as Microsoft Windows and Linux (various flavors) are pervasive and can be easily embedded within most components (PLC, etc.) of an ICS architecture. These mainstream adoptions, and in some cases adaptations, of traditional IT platforms within the OT space provide numerous benefits. However, the same also extend a new range of problems into a space where human safety and operational reliability are put at increasing risk.

3.3.3 Vulnerability Management and Patching Are Useless for OT

Perception / Problem - Within ICS networks many issues combine to make traditional vulnerability and patch management approaches very difficult and seemingly useless. The issues include, but are not limited to:

- ICS networks cannot be scanned for vulnerabilities, as active scanning may negatively affect sensitive instrumentation or components.
- ICS networks cannot be patched at all or as frequently as traditional enterprise networks.
- SCADA systems and related components are shipped by vendors with outdated or end-of-life operating systems.
- ICS environments are significantly outdated because of the extended asset life-cycles on which these plants operate — often 20 or more years between major overhauls.
- In many cases, ICS systems are purpose built and coded to perform specific functions, often for a specific client. It is not uncommon for customers to run on COTS platforms or custom software, which run on long unsupported operating systems or have software operating in critical processes from OEMs that are no longer in business.

Reality - Within any OT environment there is a real business need for both vulnerability and patch management capabilities. There is no doubt that there are real roadblocks and detractors, which make instituting these capabilities a difficult task to accomplish, both technically and organizationally. However, cyber threats to ICS environments are real and becoming more prevalent. Researchers from the Georgia Institute of Technology have created a ransomware strain named LogicLocker that can alter PLC parameters [5]. While LogicLocker is only a proof-of-concept, it shows the level of intelligence possible, such that the ransomware can dynamically identify when it is running on computers with PLC software, it can lock the device and it can alter the PLC parameters under the hood. Researchers agree that it is only a matter of time until PLC-based ransomware becomes an unfortunate trend amongst malicious threat actors.

Since the late 1990s, ICS manufacturers are beginning to include security in new systems, with engineering firms prioritizing cybersecurity in the design of new plants [2]. More prominent OEMs of ICS solutions, such as Siemens and Rockwell Automation, maintain databases of security advisories affecting the products [46] with a common vulnerability scoring system (CVSS). The method is used industry wide to capture the characteristics of a vulnerability and produce a numerical score reflecting its severity, to give customers a risk-adjusted approach to ensuring the most critical and impactful vulnerabilities can be evaluated and mitigated.

3.3.4 Social Engineering is Not An OT Issue

Perception / Problem - Social engineering is a phrase used to denote a wide spectrum of nefarious activities conducted by manipulating humans via various social interactions. Social engineering uses psychological manipulation to trick people into making decisions that compromise personal and usually sensitive information. There exists a perception that because the OT components of an environment do not directly interface with social media or communication tools, the components are immune from the attack by social engineering.

Reality - Most social engineering attacks occur via a multiple step process. A malicious entity first investigates the targeted prey (individual or organization) to assemble reference information, such as potentially weak security protocols in order to proceed with the attack. Next, the attacker works to gain the target's trust and provides a provocation for downstream activities that go against organizational security policies, such as unknowingly sharing sensitive information or allowing access to key resources. These downstream actions do not need to have direct access to the OT networks, as various social engineering attack techniques will sit dormant on the initiating network and perform reconnaissance actions in order to spread and ultimately reach the intended goal. Given that many OT networks are not segmented and firewalled from the corporate network, the spreading and infiltration can occur via a multitude of methods, such as spreading via SMB, removable media (refer to StuxNet) and port/application scanning. Some threats are multi-threaded, where once a condition is met (e.g. a specific PLC device is found on the network), different, new actions are taken to specifically target those device types.

3.3.5 Misplaced Trust In Firewalls

Perception / Problem - Within any defense-in-depth oriented security architecture, well placed and properly configured firewalls provide an adequate level of protection. Some organizations, especially those with a lack of maturity when it comes to network security, look at firewalls as the all-purpose device to protect the environment, regardless of design, configuration accuracy, strength of rule base, etc.

Reality - While firewalls are a pivotal component protecting against unauthorized access and malicious activity, there are a number of factors that can prevent the necessary protections from being effective, including:

- Misconfiguration – Modern firewalls are complex devices and require subject matter expertise to provide a hardened device configuration, as well as a well-defined ruleset to process the traffic passing through it. Studies have shown that improperly configured rulesets can create conflicts in the intended results and thus decrease the effectiveness of the firewall [6, 56].
- Insider Threats – If an attacker has already gained access to an environment or if someone with legitimate access knowingly (actively participating in malicious behavior) or unknowingly introduces an attack (e.g. via a compromised USB stick), firewalls are generally useless unless placed between multiple layers of the organization to section off or quarantine a subset of the environment.
- Filtering Encrypted Traffic – Traditional host-based or network-based firewalls are unable to investigate and assess traffic across an encrypted connection. This lack of visibility can create a significant blind spot for both authorized and unauthorized traffic.
- Shadow IT Introduced Connectivity – Due to a historical lack of collaboration between IT and OT departments, manufacturing engineering teams and/or factory operations staff commonly will work with suppliers, customers and other third parties to provision direct access to the factory network through various methods (point-to-point circuits, site-to-site VPN connections, etc.). The untrusted parties are placed directly on the factory operations network without a clear understanding of the network security consequences.
- Lack of Peer Reviews – Generally, firewall rulesets of an organization are highly protected, due to inherent sensitivity. As such, the number of personnel who have access to those configurations/rulesets are typically restricted to those who need to know in order to support the organization. Because of the closely guarded nature of firewalls, organizations rarely perform internal peer reviews or externally conducted audits, which could help identify potential issues and prevent downstream negative impacts.

3.3.6 One-way Communication Appliances Offer 100% Protection

Perception / Problem - In the last decade, unidirectional firewall gateways have been heavily marketed in high security use cases with a large push in the manufacturing sector, due to the human safety concerns that are inherent in SCADA environments. This is a non-routable hardware-enforced, one-way communication product that provides efficient, unidirectional information transfer [48]. This technology was designed to intercept and block attempts to transmit data in the opposite direction, thereby protecting the information being transmitted. The manufacturing use case serves well where ICS systems in a defined network segment transmit data to systems outside the ICS space; for example, in corporate IT networks.

Reality - With proper configuration and continuous oversight, this technology does elevate the protection scheme of any IT/OT landscape. With that said, there are caveats and limitations on solely relying on this technology for SCADA environment security.

- Some unidirectional gateway technologies act as interpreters, analyzing the permutations of metadata as traffic attempts to traverse the network. As this interpretation occurs, there is the potential to inject malicious code via TCP, a two-way protocol by design.
- A study conducted from 2013 to 2014 by the ARC Advisory group found that many organizations could not accept (in practice or by policy) the perceived limitations of one-way communications, despite the recognized security benefits [55]. In these cases, one approach was to implement a unidirectional solution for each direction. While this technically provides the necessary protections, it is not practical from a fiduciary, technical complexity and operational overhead perspective. There are other methods to allow for pre-approved bi-directional traffic, but the solution begins to degrade and appears similar to a traditional firewall with the added complexity of specialized devices.
- Within the TCP/IP stack, the "three-way" handshake built into TCP/IP will prevent any TCP/IP-based protocol from passing through a unidirectional gateway; most user datagram protocol (UDP) protocols require two-way communication for proper operation. In order to get around this issue, modern unidirectional security gateways implement custom software to proxy the traffic. While the technical constraints can be overcome, most

products on the market today have not been validated and certified for use by SCADA vendors, which limits application [43].

3.3.7 Endpoint Protection Is Sufficient

Perception / Problem - There exists a perception that purpose-built ICS devices with proprietary operating systems are inherently protected from worms or viruses, since a significant portion of vulnerabilities are targeted at the Windows operating systems maintained by the IT team with the proper endpoint protections applied.

Reality - It is true that IT and OT environments are very different, but the reality is that the endpoints in an OT environment are increasingly connected to the rest of the enterprise and must be treated and maintained just as IT environments are more than ever before. As these worlds converge, there is also greater risk to the OT environment. In order to mitigate potential attacks on OT, endpoints in the OT environment need to be protected and organizations need to ensure that IT endpoints are protected to avoid attacks that laterally traverse to the OT environment. An overarching endpoint security strategy needs to be in place for OT and IT environments to address endpoint management, including but not limited to:

- Due to the traditional separation between IT and OT, the members of the IT support organization who traditionally have the skills and knowledge in properly protecting the endpoint technology may not be the same people who administer and support the OT environment. This can result in improperly configured technology, thus providing a false sense of security and a potential attack vector.
- Worms and viruses, which traditionally deliver exploits to Windows-based devices, constitute only a portion of the overall threat landscape [29]. There are other attack vectors that are technology agnostic; these include but are not limited to account hijacking, information leakage and malware.
- Endpoint protection cannot prevent all types of attacks. For example, a targeted attack will specialize in how to gain entry and compromise a target, whereas some attackers will attempt to use obscure malware to proceed undetected. This is true for specialized attacks

against OT, as specialized hardware and software can be difficult to identity by traditional IT endpoint protection defenses.

- Without proper oversight, planning and diligence, endpoint devices can be left in a state that is easy to disable by attackers. This stems from potential scenarios, such as unconfigured devices/software (e.g. default factory credentials, settings, etc.), improper configuration and unnecessary services not disabled. It would not be uncommon for an attacker to gain access through one of these methods or worse yet via another method and then laterally move across the endpoints through a consistent opening in the device's security configuration.

3.3.8 PLCs and RTUs Do Not Need To Be Hardened

Perception / Problem – PLCs and RTUs do not need to be hardened as they are specialized devices incapable of being compromised.

Reality – Modern SCADA technology and related solutions are sophisticated and complex. These modern platforms operate in a distributed, multi-component architecture and for these reasons, the threat to SCADA systems is rising dramatically. PLCs and RTUs have built-in network interfaces and are controlled via the LAN. Additionally, due to the need for acknowledgement of executed actions (due to safety requirements), PLCs and RTUs communicate via TCP/IP. Some of these devices were designed to be holistic self-serving units to the extent that many will run services (e.g. telnet, file transfer protocol (FTP), dynamic host configuration protocol (DHCP), web services, etc.) in order to self-operate the ecosystem. This allows the device to fully participate in manufacturing operations, as well as provide capabilities for remote management. PLCs and RTUs are also commonly configured and maintained by third party suppliers who specialize in the devices. In order to perform common administration and maintenance tasks, the devices need to be accessible via client VPN connectivity, so the third-party supplier can provide effective and efficient support remotely.

Chapter 4: Recommendations to Improve Cyber-Security Posture for Manufacturing Organizations

4.1 Recommendations

The major components of a manufacturing environment have been reviewed, as well as the challenges and cyber risks posed to manufacturing organizations. In this chapter, recommendations will be presented to improve the cybersecurity posture for these same environments. All too often, organizations aim too high and set goals for security compliance that are unachievable without the addition of numerous external resources and/or significant increases in OT budgets. The recommendations presented within this chapter aim to be practical, prudent, and foundational to any manufacturing organization where reasonable investments can be made, aligned with the financial and operational expectations of the organization.

4.1.1 Education About and Inclusion of OT in IT Practices

As with any denial of risk, the first step is proper education on the problem. At multiple levels of the organization - IT professionals, engineers, executives and many roles in between, need to be aware of the reality that OT is just as important and as much of a cyber-target as IT is. All the traditional problems that plague IT from a cybersecurity perspective also apply to OT and should not be taken lightly. Beyond education, an organization's computer incident response plan should be extended to address the OT. In order to make the plan truly effective across all facets of the organization, it should be viewed as a digital systems incident response plan with coverage across all digital platforms on the premises, in the cloud and everywhere in between. The incident response plan should include all tasks related to a security incident, including but not limited to detection, analysis, reporting, communication, ownership, escalation procedures, containment options, formal investigation practices, root cause resolution/mitigation, and close out. Accountability for all aspects of the plan must span not only traditional IT personnel (administrators, developers, CIO), but also plant operation engineers, plant managers, etc.

Once the hurdle of acknowledging the cybersecurity risk to OT has been surpassed, an organization can then move to become further aware of OT/IT related risks in a time sensitive, ongoing manner. Specific to the manufacturing industry, IT personnel need to adopt and understand the OT cultural and technology differences and be able to truly understand the different outcomes when compared to traditional IT; there are different imperatives in manufacturing that must be at the forefront (described in Table 1 and Table 2 above). Differences can be understood by conducting a number of different activities from walking the manufacturing shop floor in conjunction with seasoned plant personnel to evaluating ICS-CERT bulletins and common vulnerability and exposure (CVE) announcements through a lens of OT risks and related impacts. Performing these activities result in a more comprehensive understanding of the manufacturing processes, problems and constraints. In order to be successful, organizations must become informed about threats to manufacturing operations but also the inherent characteristics specific to the manufacturing vertical.

4.1.2 Asset Inventory

Within any IT/OT environment, a core cybersecurity principle is *that which is not visible cannot be protected*. Visibility is a fundamental cybersecurity necessity to protect assets and information. In order to ensure that clear visibility of the OT network is in place, a set of tools, processes and controls must be established. This includes enumerating all devices that have been authorized to participate on the network, as well as dynamically identifying unauthorized devices that have connected to the network. This asset inventory should provide the necessary information to address all aspects of the asset's lifecycle, from initial implementation to administration, patching/upgrades, vendor support, configuration and connectivity (internet access or internet accessible). Doing so will allow an organization to take advantage of the business benefits that connected devices provide, while minimizing security risks.

Organizations should also invest in deep packet inspection technologies, which provide advanced methods of examining network packets in order to identify, classify, evaluate and reroute/drop packets with malicious or potentially malicious payloads. In conjunction with deep packet inspection, another practice that organizations should take on is whitelisting of OT traffic. Organizations should create a traffic map denoting all paths and traffic types under normal conditions. This map can be referenced in order to determine anomalies within the network, and when responding to a cyber-threat, remove a device from the network, as needed. Furthermore, this map can be used to help build virtual local area network (VLAN) and firewall access control lists (ACLs) for additional protections in layer 2 and layer 3.

Another control that should be evaluated relates to the use of client certificates on company-managed devices, where possible. By having a process in place to install unique device-based certificates within a device's operating system, this can act as another mechanism to identify and authorize the device. Additionally, this could also authorize access to data/applications, the ability to connect to company wireless services, and the ability to connect to the network via an external client VPN, amongst many other opportunities. Within the manufacturing industry, and in any OT environment, many devices on the shop floor will not allow for the installation of certificates. In these cases, organizations should revert to DHCP IP and media access control (MAC) switch port reservations for static management and access to resources. While MACs can be spoofed, it at least provides another layer of defense against those trying to gain access.

Due to the specialized nature of ICS equipment, identifying and fingerprinting these devices cannot be performed with traditional IT tools. There are two key considerations specific to manufacturing which must be taken into account. First, some asset inventory solutions have the potential to disrupt normal functions of critical ICS devices as the inventory processes are executed; this cannot occur under any circumstances due to the critical nature of the ICS processes. Secondarily, ICS device fingerprints vary widely and a vendor which has the capabilities to accurately map and represent the potentially vast array of assessed inventory, is a key capability. There are a number of solutions that can assist organizations to glean detailed information about their OT architecture stack across the factory floor. Solutions that succeed in this space for manufacturing companies provide real-time visibility to the industrial networks, by passively monitoring network traffic across OT network segments and modeling the usage patterns for every user, device and controller in the environment. They are able to fingerprint and define asset information for OT devices specifically which can be used as a source for asset management decisions and practices going forward. Notable players in this space include Darktrace Industrial, SCADAfence, Zingbox and Security Matters.

While physical or hardware asset management is important, so are the tools and processes for software asset management (SAM). By investing in tools and processes to establish SAM capabilities, organizations can gain a wealth of information, including but not limited to:

- Understanding the authorized software present in the environment. This makes identifying unauthorized or potentially malicious software possible.
- Implement software whitelisting as a mechanism to harden a device and prevent unauthorized software from being installed and executed. Having a software inventory of the environment will further that capability and provide the necessary insights. This is also a mechanism used to identify application libraries and scripts to ensure that the IT/OT staff place additional protections (e.g. signed certificates) on these, which would be harmful tools if accessed and leveraged by malicious entities.
- Providing a level of understanding as to the versions and editions of software leveraged across the environment in order to understand what packages may be unsupported by the publisher. This will facilitate discussions, especially surrounding critical OT related packages, in order to ensure third party support can be provided.
- Segregation of systems and related software, which are particularly high risk, such as packages that control devices having an impact on human safety or housing the company's most critical intellectual property or secrets.

Lastly, assets that are less tangible must also be considered; for instance, credentials for highly protected accounts, such as service accounts, default built-in accounts, root accounts, etc. Maintaining these credentials in an encrypted format, preferably in a privileged access management (PAM) tool will allow for delegation of authority, only accessible by those who are authorized to use these sensitive assets.

These recommendations will allow an organization to evaluate the level of risk associated with each endpoint and take steps to minimize that risk. In modern operations, there challenges that create roadblocks for achieving the necessary level of visibility. For completeness, it is important to understand the potential roadblocks, which include but are not limited to:

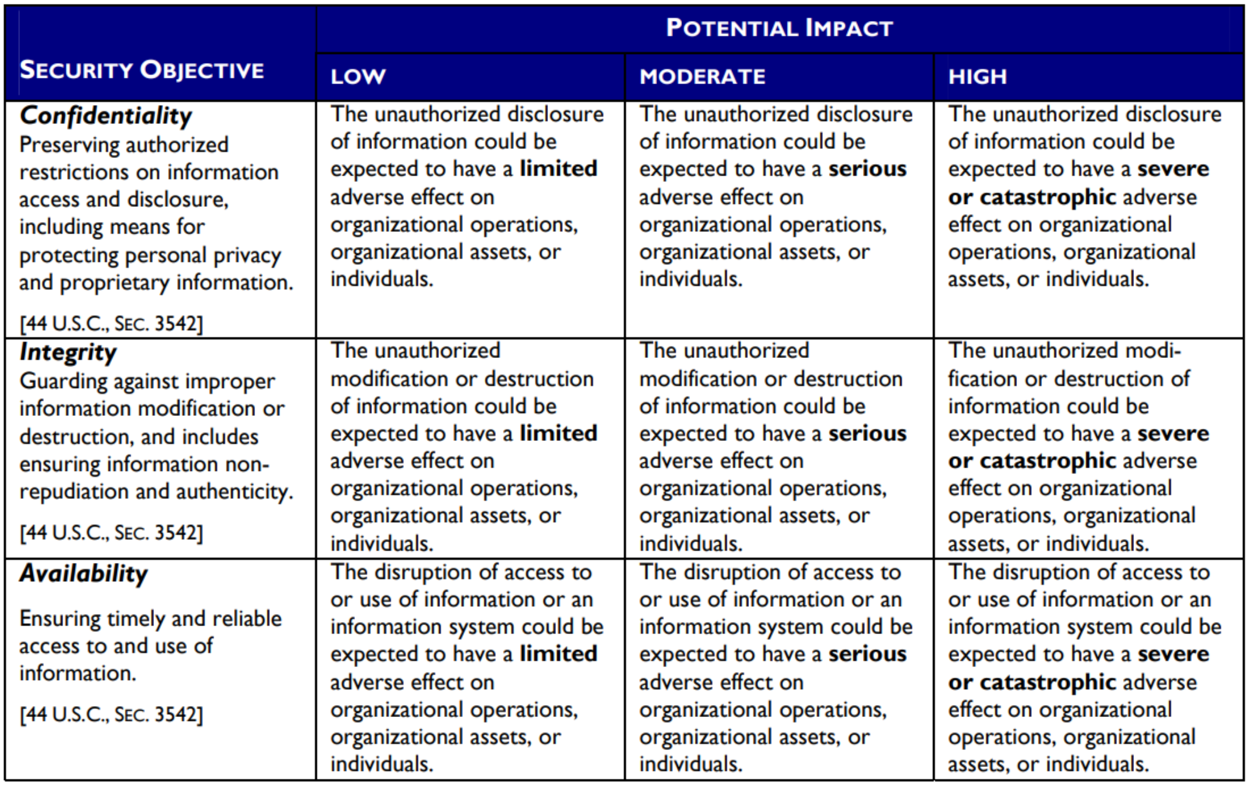
- Lack of IT Ownership – Many devices connecting to an ICS network lack ownership and are commonly not considered official corporate assets. Because traditional IT teams do not own these devices nor have visibility to them in many cases, assessing, monitoring or administering the same cannot be done easily which results in no accountability for the assets' life-cycle.
- Device Mobility – Factory floors are continually driving improvements in order to increase the efficiency of the manufacturing processes. This is commonly performed under a lean or Six Sigma umbrella. ICS devices are often moved as part of the manufacturing flow optimization.
- Shadow IT – Depending on the organization and segregation between IT and OT, it is not uncommon for engineers, or more generally, non-IT staff, to implement, configure, deploy, and maintain systems outside the purview of IT. Without planning, coordination and collaboration, devices will be provisioned, deprovisioned, and have their configurations changed outside the view of IT, thus making asset management and administration very difficult. This topic will be further addressed in a later section.
- Isolated Solutions – Where air gapped environments or network segments that are unreachable by IT's tools exist, this creates a native blind spot, which can be mitigated if acknowledged and disclosed to IT/OT admins up-front.

4.1.3 Documentation

Once a complete and reliable OT asset inventory has been established, it is important that a system architecture diagram be created, which captures all inputs and outputs under a normal controlled solution architecture. Many of the same tools identified in section 4.1.2 (Asset Inventory), can assist in mapping the OT environment landscape as part of their passive listening approach to understand traffic flows between devices. This system architecture diagram will allow the organization, IT staff and manufacturing engineers to understand and agree upon what the normal characteristics of sanctioned traffic flows should look like. By having these artifacts properly documented and understood, a cybersecurity organization can properly whitelist those traffic characteristics in firewalls, intrusion detection system (IDS) and intrusion prevention system (IPS) devices, thus making detection of malicious activity that much easier, in advance of a potential breach.

4.1.4 Data Classification

Applications and the networks should be classified in order to define the level of control required. Data classification is based on the data's level of sensitivity and the impact to the organization if it is disclosed, altered or destroyed without authorization. The classification of data helps to determine what level of controls are prudent and necessary for protecting that data. As defined in the NIST guide for mapping types of information and information systems to security categories [49], all institutional data should be classified by assessing a data type's security objective (confidentiality, integrity and availability) against the potential impact (low, moderate, high) of unauthorized disclosure [49]. Doing so will provide a view into the level of security protections that should be implemented in order to prevent such an occurrence. For example, multi-tiered application servers with different security levels should be segregated by network security zones and VLANs according to the data present in the application.



Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Figure 10: Categorization of federal information and information systems [49].

Furthermore, once classified, organizations should take the time to assemble an inventory of all previously classified data and related systems that pose an above average risk if disclosed or compromised. Once understood, and as part of the established governance processes, organizations should discuss and consider what additional protections should be placed on these systems/data to ensure that the applied protections are acceptable considering the risk tolerance assessed by the organization.

Within a manufacturing organization, data classification requirements can vary and are a bit different from other back office functions due to the specialized nature of the information and personnel needed to maintain this content in an evergreen manner. As such, specific niche products are needed in order to address the specific needs of the organization. As an example of the differences, the specific requirements and potential solutions in a manufacturing organization, we'll address a unique need core to the manufacturing process, engineering data. As part of any produced good there are engineering drawings, bills of materials, routings which detail how the product is created as well as additional reference material necessary to both create and maintain the lifecycle of a product. Specific to the manufacturing industry, these requirements are commonly met with Product Data Lifecycle (PLM) / Product Data Management (PDM) tools. These tools manage the entire lifecycle of a product from original idea generation, engineering design and manufacture, to servicing and aftermarket needs.

Engineering data is just one example of specific industry data which needs to be considered within a data classification effort. Just like engineering data, there are other tools which are specific for other manufacturing functions (e.g. quality management) and as such the data classification strategy and approach needs to take into account these specific requirements and either determine if the data can be classified natively within those tools or if there is a different approach required in order to accomplish the task at hand in order to properly classify the data.

4.1.5 Patching and Vulnerability Management

Given the breadth and depth of potential threat vectors that any enterprise ICS environment may contain, it is important that organizations looking to mitigate the most impactful threats take a risk-adjusted approach to patching and validating base configurations for the most critical devices within the ICS network. These devices by-in-large utilize a set of unique and disparate technologies to execute as designed. Unlike the IT world, there is no common Operating System (e.g. Windows) or common patch management tools (e.g. Microsoft System Center Configuration Manager) for the OT side of the house. This makes patch management for OT a unique, ad-hoc process across the factory landscape for each individual device or group of devices. Plant engineers commonly work with vendors of key equipment to ensure that they are maintained adequately at proper software and firmware levels. Due to this fragmented landscape and lack of tools to cohesively patch/update these dissimilar devices and in some cases proprietary operating systems, we must turn our focus to vulnerability management so that we can at minimum identify vulnerable devices needing attention.

From a vulnerability management perspective, it is important that organizations leverage a secure content automation protocol (SCAP) compliant toolset in order to leverage a referencable common framework for assessing vulnerability compliance [44]. Standardized expression and reporting allow for vulnerability assessments to be automated, which is hugely beneficial when attempting to identify new variances and measuring against a baseline for continuous improvement purposes month-over-month. It is important to note that traditional vulnerability scanning tools used for IT environments are not suitable for ICS environments. If a traditional active vulnerability scanner is used within the OT realm, issues such as increased latency, communication channel disruption and in some cases causing a device to cease operation can arise. Luckily, over the last 12-18 months a few of security firms have come to market with specialized passive vulnerability solutions specifically to be used for ICS environments. Most notably are firms like Tenable and CyberX that have entered this space with solutions designed to passively monitor traffic and leverage their respective proprietary analysis and threat intelligence databases to determine if an ICS device is vulnerable based on how it is communicating on the network. Once identified, these solutions can alert personnel for further investigation and provide detailed reporting as to what has been observed.

In conjunction with vulnerability scans, organizations should conduct regular port scans against environments, looking for unauthorized ports/services (e.g. Telnet, FTP, etc.) present on the network. These unauthorized instances should be investigated to understand if there is a true business need or if it is a result of an oversight or misconfiguration. In environments that are well documented, port scans can be very powerful tools to understand variances at a deeper level, which may go unnoticed otherwise. This is a practice that requires a mature approach to managing the environment as well as available personnel to execute, as it can be a tedious and time consuming process if not automated.

Additionally, organizations should consider performing authenticated vulnerability scanning. Authenticated scanning, of both elevated and non-elevated accounts, is important as it allows an organization to simulate what vulnerabilities are exposed assuming a malicious entity has been able to harvest user credentials through previously executed malicious actions. Having this level of visibility through an attacker's lens can provide insights, which may determine how data and applications are exposed and can be further protected across the organization.

Since traditional approaches to vulnerability and patch management cannot be extended as-is within an OT environment, it is important to leverage existing enterprise-wide tools, policies and procedures where possible. It is key that IT staff partner with plant engineers and managers to adapt existing policies so that all parties can support and enhance the operational security practices specific to the OT portion of the digital footprint. It is also important to check with equipment manufacturers that the intended updates have been tested and qualified/validated to work properly, especially as it relates to the technology where human safety is a concerns. Once these policy updates have been agreed upon, for the OT devices that can accept updates, a defined and mutually agreed upon downtime schedule should be created for patching, testing and any other required maintenance activities.

ICS component manufacturers have taken a more security conscious approach, ensuring that the IT organization in conjunction with the plant engineers and managers work with the OEMs to establish formal relationships with contractual terms. This governs what the OEMs are responsible for relating to product support, patch management, zero-day vulnerability response, etc. Establishing these formal relationships and oversight mechanisms will ensure that the IT staff is tightly coupled with the OEMs, such that the organization receives the support it needs in order prevent or respond to a security incident.

4.1.6 Network Segmentation

The goal of network segmentation is to divide the network according to business requirements, address compliance and regulatory concerns, while enforcing security controls between zones. Network segmentation utilizes security policies that act as layers of security providing defense from internal threats and remote users with access to the internal network (via authorized client VPNs.

A segmented network architecture is based on the concept of network security zones. Zones may be further segmented into smaller virtual networks to minimize operational or information protection risks. Security zones are logical groups of virtual networks, which in turn represent physical network segments that group network resources with similar security levels based on level of importance to the organization. In a segmented network infrastructure, VLANs and other controls (that are presented later in this analysis) are used to segregate devices with different security levels. In order to filter communications between the segments, ACLs or firewalls are used.

Network segmentation is fundamental for a healthy and secured network design; however, many firms do not segment properly or at all for various reasons (e.g. complexity, additional overhead, lack of understanding and perceived value). Lack of internal network segmentation, especially between IT and OT data and services, is a contributor to quickly spreading security threats and attacks in SCADA networks [4]. IT/OT organizations need to work under the assumption of a breach, such that the attack needs to be compartmentalized with no ability to laterally move within the network to further compromise or exfiltrate data. It is common sense that most malicious entities (outside of nation states or highly targeted attackers) will not be persistent in an attack. If too much time or effort is wasted, the malicious entity will go somewhere else, again, unless the attack is highly targeted. Prevention is always better than having to potentially detect (if skilled or lucky enough) a breach.

Proper network segmentation is a large part of the prevention puzzle. Benefits that network segmentation can provide to an organization include but are not limited to:

- Consolidation of like devices within a defined broadcast domain can reduce unnecessary traffic across a broader segment, thus providing better performance, visibility (monitoring, detection, logging, etc.), simplified administration, and better forensic capabilities.
- Obscurity of network segments (when properly segmented with firewalls) to malicious entities deters their ability to laterally move in the environment. Leveraging the premise of least privilege and a global deny ruleset allows only explicitly understood and sanctioned traffic to pass from one segment (trust profile) to another.

- Separation of different applications/data into zones, which classify different data sensitivity levels so that additional protections and restrictions (via ACLs) can be placed upon the most sensitive zones within an organization.
- Reduced surface area for an attacker to compromise devices within a defined segment. Traditional segmentation practices as well as more modern micro-segmentation (traffic between any two endpoints can be analyzed and filtered based on a defined policy) techniques allow organizations to categorize or sub-categorize sensitive or highly critical portions of the network. Assuming a position that the organization has been breached, if properly segmented and protected with advanced security controls (such as multi-factor authentication), the attacker will not have a diverse inventory of network devices to work with.

4.1.6.1 Improvements to the Traditional Model

While the PERA model provides a solid foundation from which to segment an enterprise manufacturing network, it leaves much to be desired in a modern IT/OT landscape where security threats are complex and pervasive. There are several controls and protections that are practical and fiscally responsible and provide tremendous in-depth defense improvements; examples are explored below.

4.1.6.1.1 VLAN Access Control Lists (VACLs)

VALCs provide access control for packets that are spanned within a VLAN or that are routed into or out of a VLAN for VACL evaluation. VACLs apply to all packets and can be applied to any VLAN, are processed in the hardware and can apply to both IP and MAC-based traffic. If a VACL is set up for a packet type, and there is a miss-match, the default action is to deny the packet. VACLs can also be used to filter traffic between devices in the same VLAN. VACLs can be used in conjunction with the other segmentation technologies but can be largely redundant and add operational overhead, if not implemented properly.

4.1.6.1.2 Private VLANs

Further isolation of IT/OT resources can be achieved using private VLANs. A private VLAN is a secondary, or subset type of a VLAN. The benefits of private VLANs are additional network segmentation and isolation, if needed. Highly sensitive information can be insulated from other VLANs with restricted access if further isolation is warranted.

There are two types of private VLANs, community and isolated. A community VLAN is a secondary VLAN that transmits packets from the community ports to the upstream promiscuous port as well as to other ports within the same community. Multiple community VLANs can be configured in a private VLAN domain. The ports within one community can communicate with each other, but these ports cannot exchange data with ports in any other community. An isolated VLAN is the other type of private VLAN, which carries traffic from the host directly to the promiscuous port alone. Only one isolated VLAN can be configured in a private VLAN domain. An isolated VLAN can have numerous isolated ports, however, all traffic from each isolated port remains separate. Promiscuous ports can forward traffic from every secondary VLAN, as well as the primary VLAN. Figure 11 and Figure 12, shown below, provide views of how community and isolated VLANs operate.

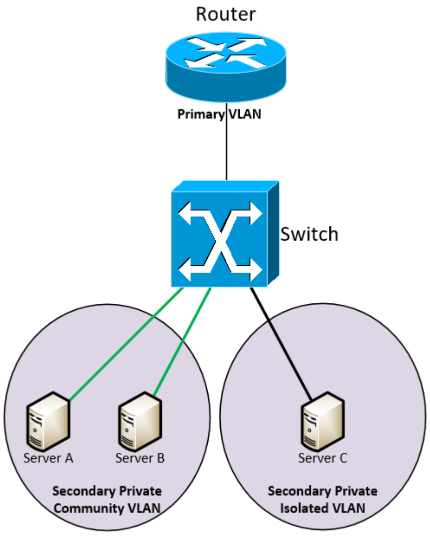

Router
Primary VLAN
Switch
Server A
Server B
Server C
Secondary Private Community VLAN
Secondary Private Isolated VLAN

Figure 11: Private VLAN example

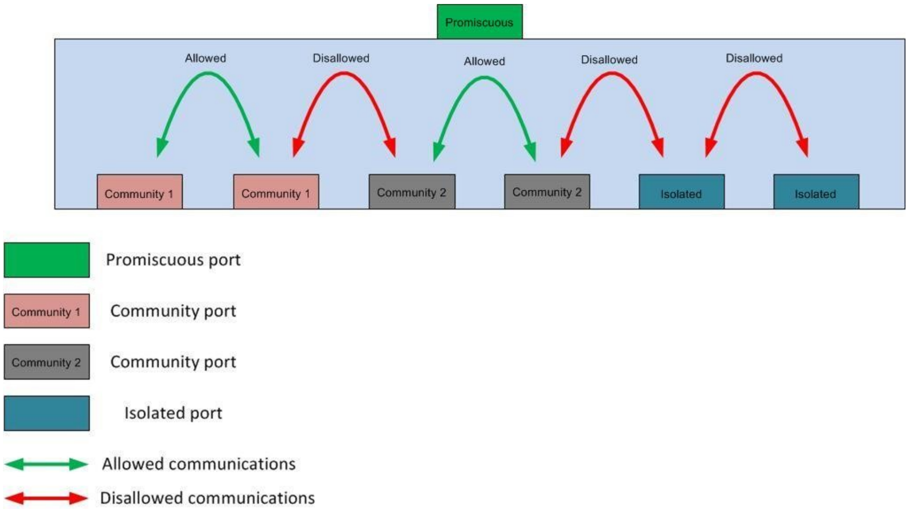


Figure 12: Private VLAN community example

4.1.6.1.3 Port Protection

Port protection is similar to private VLANs, but it is simpler and less flexible. The port protection feature works by designating a physical port as protected, at which point it will not exchange data traffic with other protected ports. Protected ports will interact with non-protected ports in a normal fashion, exchanging data. This allows administrators to prevent two machines within the same subnet and VLAN from talking without going through an upstream non-protected port that usually will have some device connected to inspect and filter traffic. Thus, making it less likely that a compromised device or virus infected machine will be used to attack other hosts without triggering alarms or logs. Port protection can be used in a data center environment to stop attackers from using one compromised server as a launching point to attack other servers on the same segment. While this is a powerful capability, it is more often used at the end user host ports (e.g. PCs), because private VLANs provide more flexibility, and data center switches are more likely to support private VLANs than switches on the enterprise edge.

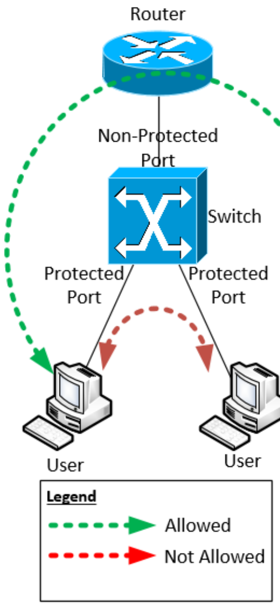


Figure 13: Port protection example

4.1.6.1.4 802.1x Network Access Control (NAC)

802.1x addresses the problem of manually managing the large majority of edge ports in an enterprise environment. In an environment where 802.1x is not leveraged, an attacker is able to plug into physical network outlets and gain access to the internal network. From a network administration perspective, it is impractical for any IT/OT support organization to manually configure and audit every active network port across an enterprise network on a continual basis.

In order to address this administrative nightmare, 802.1x can be deployed to centrally manage, via preconfigured policies, the configuration and controls placed on edge ports across the enterprise. In order to enable this capability, edge switches and host operating systems must explicitly support the feature, because layer 2 frames are exchanged using a data format that differs from standard Ethernet. If both sides are not 802.1x capable, access will not be granted. A host and an edge switch negotiate 802.1x parameters, such as machine identity, which the switch will relay to the 802.1x controller. The controller will inform the switch which VLAN the host belongs on, and potentially which downloadable ACL should be applied to the port. This is commonly determined via active directory (AD) groups. This can be accomplished for both wired and wireless hosts.

Once port authentication and NAC policies have been fully configured and deployed, it becomes one of its more powerful features to identify unauthorized or rogue devices connecting to the network. These unauthorized devices could be as simple as a visitor connecting a laptop to an Ethernet jack in a conference room or as complex as someone deploying additional unauthorized network switches or wireless access points within the facility. While vulnerability management tools may be able to identify these hosts, it would only be reactionary and there would be no proactive action taken to quarantine the unauthorized device and alert the proper technicians or security personnel. In a worst-case scenario, whether it be via malicious intent or a vulnerable third-party host with an active persistent threat (APT), NAC provides the necessary capabilities to maintain the hygiene of the devices authorized to connect to the network. By deploying NAC, any issues stemming from hosts that roam across the network are addressed by the port/connection-based policies being applied via the NAC policy engine. While deploying NAC can be costly and require significant up-front fees to institute, the level of protection a well-built NAC solution can provide is enormous, especially in a high-risk environment.

With a NAC solution in place, additional manufacturing specific capabilities and benefits can be obtained. For example, further network security automation of ICS devices can be obtained by using a policy based industrial network administration tool. Tools like Cisco Industrial Network Director (IND) integrate with NAC products like Cisco Identity Services Engine (ISE) to provide visibility and context to plant engineers for all networked ICS devices. Policies in ISE can be configured by IT personnel in advance, which can be used by the plant engineers via a user interface specifically designed for manufacturing operations. Through this interface, plant personnel are able to visualize connectivity between network devices and ICS assets so that predefined policy based changes can be dynamically made in an OT context without having the plant operators to be technically savvy. For example, consider a scenario where a plant engineer needs to allow a third party support vendor access to critical ICS components. The plant engineer, in a matter of minutes, through the IND interface can allow access to the specific device or set of devices for the vendor to access, without having engage IT or configure complex rulesets on the firewall or VPN appliance. Once the plant engineer saves his changes, the IND communicates with ISE to update the policy and push the new configuration to the necessary network devices to ultimately allow access. This capability prevents the need to maintain a persistent ACL on the firewall with access open at all times.

4.1.6.1.5 Tiered Application Architecture

Tiered application architecture as a control makes use of the functional containerizing of an application. Containerizing enables the application to be broken down into functional units, which can be implemented across multiple servers. Typical functional units include a web/presentation layer, an application layer, and a database/processing layer. Access to the functional units is much cleaner and more secure using this approach. To illustrate this example please refer to the diagram in Figure 14 below. In this diagram, access to the web server layer would be enabled through a firewall-based TCP port number(s) for the application. Since applications can be used from anywhere within the environment, a source IP address cannot be used to limit access. However, it is important to note that the users will not have any access to the database servers, as depicted in the diagram. Access to the database servers would be limited to the web server(s) only. Note that the application could have additional functional layers, which would also be protected by firewalls with tightly controlled access.

Using this strategy, access to servers can be more tightly controlled, thereby reducing the potential threat surface. Only the presentation server needs to be accessed by users. All other functional layer servers (database, application or processing servers) will have access blocked from general users. The only access to these servers will be the other servers running components of the application requiring access, explicitly permitted via the applicable firewall rules. It is worth noting that this architecture cannot be implemented without the assistance of the application support teams and the application publisher or system integrator. A determination must be made as to whether or not the application can be implemented using functional layers. Once determined that it can be decoupled logically, the IT/OT teams must undertake the effort required to move functional layers to different servers. Additionally, allowing access to the application based on IP port number leaves the server exposed to attack, as it can still be accessed by anyone with access to the network. Access is restricted, but it remains open to anyone knowing the port and IP address.

The logical diagram below shows an example of a segmented two-tier application that consists of three front-end web servers and three back-end database servers located on separate VLANs. Application end-users can access front-end servers only. Direct access to the database servers is not allowed. Communication between front-end and back-end servers is controlled by ACLs on the firewalls.

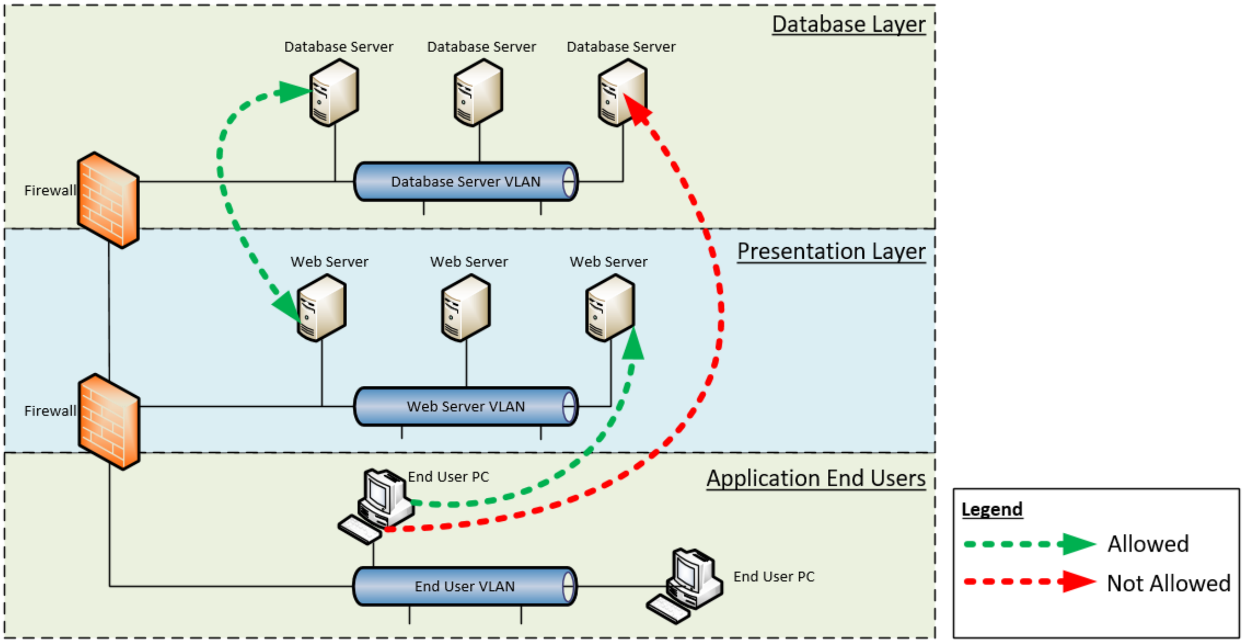


Figure 14: Tiered application flow diagram

4.1.6.1.6 Air Gap

An air-gapped network is one where there is no connection of any kind from the corporate network to the target network being protected. This architecture is leveraged in situations where the network being protected is fully self-sufficient (i.e. no dependency on other services outside of the segment) and the unauthorized disclosure of information would have a significant adverse effect on organizational operations, assets or individuals.

4.1.6.1.7 Wireless Networks

Wireless networks provide a wide breadth of capability, especially for a space constricted and ever-changing factory floor layout where lean principals drive efficiencies, requiring equipment to be moved in areas where traditional cabled networks would have created restrictions [39]. When enabling wireless networks in an OT environment, especially with additional prevalence across the factory floor, there are several considerations that need to be carefully evaluated and planned for. Some of the more fundamental considerations are listed below.

- Inventory of broadcasted approved service set identifies (SSIDs) so that rogue or unauthorized wireless networks can be easily identified.
- SSIDs should be broken out by function and segmented in accordance with their data classification rating.
- An internally managed device should require a company issued certificate and AD credentials to join the network.
- Disable split tunneling across all interfaces in order to prevent multiple different networks from being unintentionally bridged.
- Ensure that AES-256bit encryption is the minimum allowable on data in transit.
- Disable any unnecessary access methods, such as Bluetooth, near-field communications (NFC), etc.
- A specific guest wireless network should be implemented for third parties that are visiting the company and need temporary access to customary services (web browsing, email, etc.). Devices in this segment shall have no access to internal resources.
- Devices that do not accept certificates (e.g. barcode scanners) should have the MAC address whitelisted so that all other unknown devices can have access denied implicitly.
- If company policy allows for the use of personal devices as part of a larger bring your own devices (BYOD) policy, a separate SSID should be used with specific and defined host integrity policy (HIP) checks. HIP checks validate the cyber health of the device (AV, patches, etc.) and should be instituted prior to allowing the device to access company resources.

- Wireless technology on the shop floor can be troublesome due to the signal interference with the heavy machinery. It is recommended that frequent wireless surveys are conducted to ensure dead signal spots do not exist where connectivity is required.

4.1.6.1.8 Separation of Production and Non-Production Traffic

Organizations should separate but mirror production segments from other segments, such as quality, test, development, etc., to ensure confidential data held on a well-guarded production server is not moved to a potentially less protected development server.

4.1.6.1.9 Separation of Enterprise and Manufacturing Traffic

Organizations should separate the manufacturing network from the internal corporate network. This is per best practices in NIST Special Publication 800-82 R2, Guide to Industrial Control Systems Security [26]. The nature of network traffic on these two networks is different. As an example, the corporate network, internet access, FTP, email or remote access should never have direct access to the manufacturing network. If manufacturing traffic is carried on the back-office LAN, it could be intercepted and subjected to denial of service (DoS) or man-in-the-middle (MITM) attacks. By segmenting the networks, security and performance issues on the corporate network should not affect the manufacturing network.

According to NIST 800-82 R2, practical considerations, such as cost of ICS installation or maintaining a consistent network infrastructure, often mean that a connection is required between the ICS and corporate networks [26]. This connection is a significant security risk and should be protected by firewalls with a well-defined rule set. If the networks must be connected, only necessary (bare minimum) connections should be allowed and the connection should be through a firewall and a DMZ. A DMZ is a separate network segment that connects directly to the firewall. Servers should be established in the DMZ, which are solely used as bastion hosts or jump boxes, to access the manufacturing network containing the data from the ICS. Only these bastion systems should be accessible from the corporate network, and in turn, are the only devices that can access the manufacturing segment. With any external access inbound, minimum access should be permitted through the firewall, including port/service restrictions.

4.1.6.1.10 Network Segmentation of Manufacturing Devices

Per NIST 800-82 R2, network segmentation is one of the most effective practices that an organization can implement to protect its manufacturing network [26]. Segmentation establishes separate security domains to enforce a consistent security policy and maintain a uniform level of trust. Segmentation, if architected with data classification in mind, can minimize the method and level of access to sensitive devices. A practical consideration in defining a security domain is the amount of communications traffic that crosses the domain boundary, because domain protection typically involves examining boundary traffic and determining whether it is permitted.

The use of a bastion host for all access to the manufacturing network, which includes all third-party vendor access, is critical to the security of the ICS. This can also be accomplished using a jump box to an engineering or supervisor workstation. If a vendor requires direct access from a non-company issued machine, a very specific rule should be devised to allow access through the firewall policy. This should require managerial approval, be labeled clearly in the relevant ruleset, and be as specific as possible. Access to the internal network or internet should be over a separate workstation and not from one in the ICS. This is to avoid creating a backdoor into the security zone housing sensitive company data.

Within the manufacturing network, improvements can be made to identify and associate like devices together into separate segments so that additional controls/protections can be placed, where appropriate. As an example, devices that perform data aggregation (e.g. sensors) should be grouped together and controlled separately from PLCs and RTUs, which should be placed into a separate grouping. Lastly, devices that allow and require regular human interaction to operate the manufacturing network, such as HMIs, should operate in a separate grouping. Continuing this example, there are now three distinct groupings, which can each have different, meaningful controls (e.g. community or isolated private VLANS, port protection, VACLs, 802.1x, NAC, etc.) aimed at protecting the data and devices from malicious activities.

4.1.7 Proposed Reference Architecture

While the PERA model provided a referencable framework that was relevant for many years, beyond a simplistic separation of networks, it really provided no protection from a security compliance perspective. Building on this model, there are a number of improvements that have been made over the years, as well as recommendations for future operating models. Below is a proposal for a reference architecture, which views the OT landscape through a single digital lens in order to provide the necessary fundamental protections for modern information systems in an OT environment.

Within this new proposed model, level 1 through level 4 are the same, relating to the type of devices that reside in each level. The differences, however, consist of the technology protections being implemented to further secure factory operations. While these technology protections were discussed earlier in the document, additional context is added below.

- Access via Bastion Host – Any IP-enabled OT devices should be managed by physically walking up to the device and connecting a console/network cable or accessing the device via a shared bastion host, dedicated to the management and administration of devices that participate in the factory operations. This provides a centralized "choke point" for all personnel to access these highly protected devices with additional controls applied at the bastion host (e.g. multi-factor authentication, enhanced logging, privileged access management, etc.). Direct management and administration of these devices are to be blocked at the firewall as well to enforce one-way into the environment.
- MAC Whitelisting – Since most of the devices at this level will not be Lightweight Directory Access Protocol (LDAP) or AD-integrated, a device-based certificate will be carried (where possible), and each hardware MAC address should be added to a layer 2 whitelist to be allowed to connect and communicate across the network.

- NAC – Network access control will prevent unauthorized devices from connecting to the network and gaining access to resources.
- Layer 2 VLAN ACLs – While redundant with the use of port protection, layer 2 VLANs act as a backstop for any misconfigured ports within the VLAN. All valid traffic should be explicitly identified so that factory operations are not interrupted.

Above level 4 a new level is proposed, level 4.5 – control network DMZ. This segment houses all remote access services to access devices in levels 1 through 4. The remote access services residing in this network can be solutions such as Microsoft remote desktop services (RDS) server (formerly terminal server), Citrix gateway or an SSH terminal. These jump boxes are to be connected to via a dedicated management network, from the enterprise network, with an elevated account that is different from the normal credentials used to access other non-OT resources. Users should also be prompted to authenticate with a second factor as part of the overall enterprise multi-factor authentication architecture. Once successfully connected, these hosts can access all devices in the factory operations from level 1 to level 4.

Lastly, an external DMZ network has been added, level 6. The external DMZ segment should host any servers/services that need to be exposed to the internet. This segment should contain services such as external client-based VPN, web services, transmission services (e.g. SFTP) or any other IP-based services that have a legitimate business need to be exposed to the internet. Access should be controlled to known, valid destinations and application services (HTTP, HTTPS, SFTP, etc.), all passing through an application aware web application firewall (WAF). All external access for third party OEMs or maintenance organizations needing to access devices in the factory should use client VPN services to establish an encrypted connection to the organization’s perimeter. Once properly authenticated, again with multi-factor authentication, the only devices that can be accessed (via ACLs on the VPN tunnel) are those that have been approved to access level 4.5 – the control network DMZ.

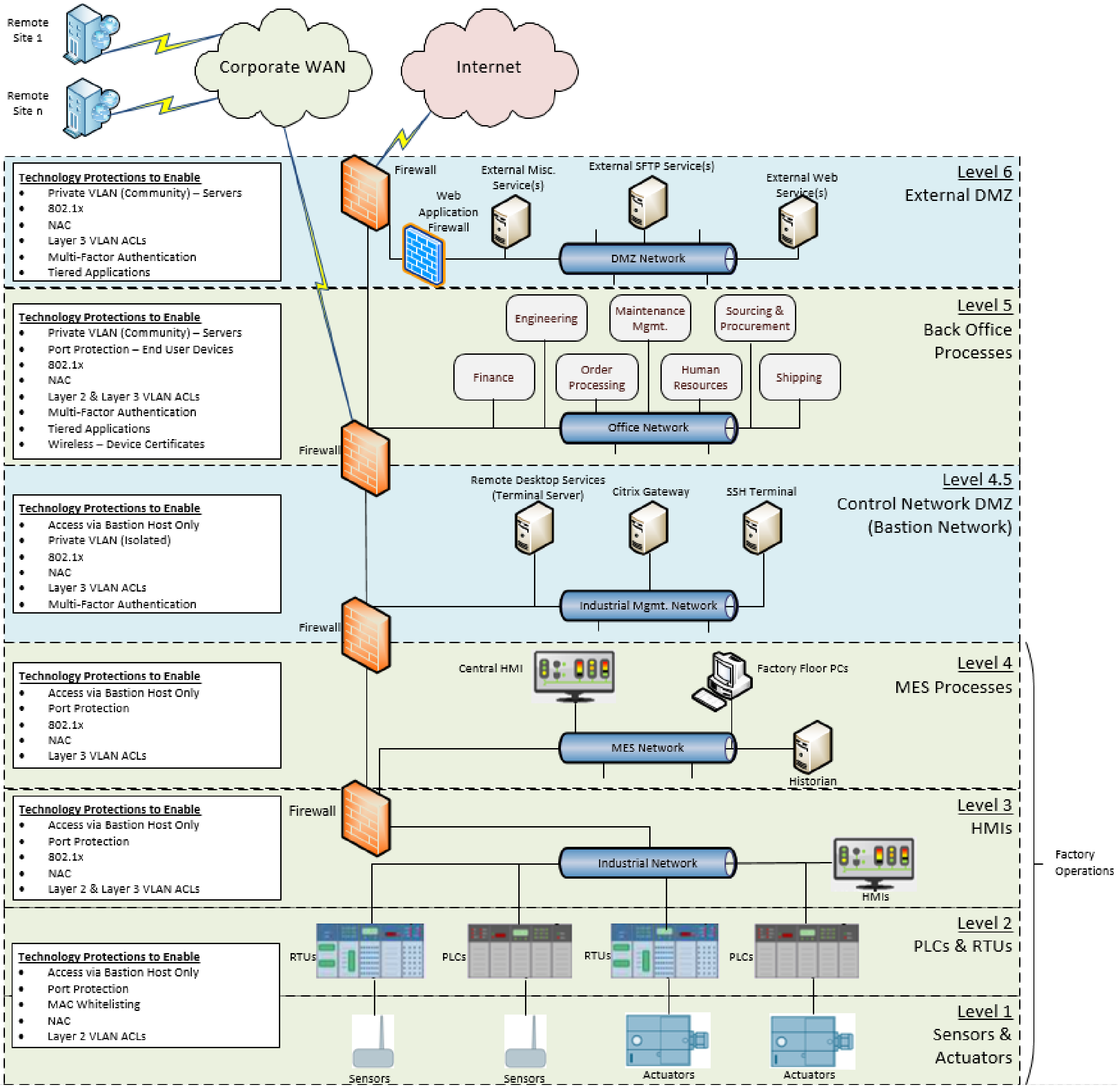


Figure 15: Proposed reference architecture for manufacturing environments

4.1.8 Hardening of Factory Floor Devices

As a precaution, organizations should understand how to harden devices within the factory environment and execute those hardening procedures for all network-based devices.

This may be a difficult task for legacy SCADA-based devices, as the OT manufacturers did not have security in mind during design. The good news is that most SCADA devices produced by reputable manufacturers can be hardened to some degree. It is important that when specifying, designing and implementing these devices the IT and OT teams work very closely with the manufacturer to ensure security considerations are discussed up front as part of the pre-sales process.

For traditional Windows- or Linux-based PCs, which participate in the factory floor processes, this step is even more important because many of the services and functions that are enabled by default are not required for manufacturing processes and should be disabled in order to reduce the threat landscape available to a malicious entity.

Across both spectrums (SCADA devices and Windows/Linux PCs), there are several actions that can be taken to significantly reduce the threat surface, such as:

- Standard image – Wherever possible, leverage a hardened standard image. This will provide a consistent baseline for a well-configured device, which internal and vendor configurations can be based upon. Standard images should be reviewed twice a year to re-establish a hardened state with releases of new operating system patches, firmware, etc.
- Eliminate access to the internet – Where access cannot be eliminated fully, whitelist the applications/services that the factory floor devices require to a defined, pre-approved list. Keep the list updated and ensure that periodic reviews are done in order to update and prune the list as technology changes.
- Browser Hardening – While the best path from a security perspective is to prevent all internet access from factory floor devices, it is understood that there may be a need to allow access to select whitelisted destinations. In conjunction with significantly limiting access, hardening the browser configuration is another avenue that should be investigated. Areas of focus include, but are not limited to:

    - Preventing installation of unauthorized/additional browsers.
    - Disabling/preventing use of browser plug-ins and add-ons.
    - Leverage URL category filtering tools for reputation analysis.
- Lock down removable drive accessibility – Restrict all access to removable drives so that read and/or write functions are disabled. Where access cannot be eliminated fully, whitelist the removable media device types, drivers, etc. that can be used and disable auto-run capability on all external media. Above all, as part of the cybersecurity awareness and training program, inform users that using removable media from an unknown source is never allowed.
- Limit Physical Access – For the back-end infrastructure, ensure that all servers and related storage appliances are in secured data centers, which prevent access to unauthorized individuals. Client access/workstations that have access to critical devices/data on the network should be in physically segregated locations within the facility, such that access can only be gained by authorized personnel.
- Prevent / Restrict Remote Access – All access from networks external to the factory operations network are blocked by default and remote access is granted for pre-approved parties via IT managed client VPN services.
- Application Whitelisting – All PCs and servers that participate in factory operations processes should have unsigned and unregistered executables blocked (by default) from running on workstations and only allowed via a whitelisting process in conjunction with the software asset management processes. Taking this preventative measure will significantly reduce the possibility that malicious software could execute within the environment.
- Enhanced Logging, Monitoring and Alerting to Centralized SIEM – All devices capable of generating logs should have the logs ingested by a centralized security information and event management (SIEM) service. An SIEM service can assemble the disparate logs and identify patterns of malicious activity so that actions can be taken to prevent or stop any further malicious activity.
- Local Administrator Rights – All too often, PCs and servers are left vulnerable by providing too many rights, as well as default configurations. The following activities should be undertaken to further protect the devices within the factory operations environment:
    - Rename the local administrator account.

    - Use a tool such as Microsoft LAPS [25] to randomize the local administrator password for each device on the network.
    - Do not allow local accounts on PCs or servers to be used. These accounts are not centrally managed and can be used to bifurcate other environment controls.
    - Do not allow accounts to have local administrator access to the device, unless absolutely necessary.
    - For the accounts being used to run the factory operations, ensure provisioning in a least privileged manner. Providing excess privileges, unnecessary to performing the duties of the role, can provide a mechanism for exploits or lateral movement to occur.
    - Remove or rename any other built-in or default accounts that may be easily guessed.
- Governance – Establish a governance process that includes personnel from information technology and operations engineering, as well as any other parties that have responsibilities related to how the factory's operations are designed, configured and maintained. With these key personnel identified, a working group or committee should be formed to address all aspects of OT's lifecycle (installation, configuration, administration, patches/firmware, obsolescence, retirement, etc.).
- Multi-Factor Authentication – One of the most valuable assets an attacker can compromise are credentials. By introducing multi-factor authentication across a factory environment, credentials and access to key resources (e.g. intellectual property, research and development information and operational processes) can be further protected. In order to be truly effective, multi-factor authentication should be placed at every level of the environment, including but not limited to access to client VPN, PC/server logins and web application logins.
- Configuration Management Tools – Configuration management tools, such as Microsoft system center configuration manager (SCCM), should be considered in order to baseline hardened desired state configurations for devices in the environment. Most of the tools in this space can reapply the baseline configuration when changes are detected, as well as provisioning alerting to IT/OT administrators so that root causes can be investigated for future prevention purposes.
- Disable Wireless – Unless required to communicate on the network, disable any unnecessary interfaces. This includes traditional wireless interfaces, as well as Bluetooth.

4.1.9 Implement Firewall Best Practices

A number of shortcomings of traditional host- and network-based firewalls have been discussed. Modern firewall technologies combined with augmenting a layered approach with respect to firewalls can provide an elevated level of protection. The recommended changes include but are not limited to:

- Implement Application Aware Firewalls – Many potent vulnerabilities exist at the application layer, which would be much more difficult, almost virtually impossible, to detect with a traditional host or network-based firewall. Application aware firewalls can inspect the traffic at the application layer and evaluate the traffic accordingly [32]. Per recent studies on firewall configuration effectiveness for SCADA environments [35], outdated firewall software was prominently in use, compromising the necessary protections.
- Decrypt Encrypted Traffic At The Firewall – Since many attacks that are executed remotely occur over an encrypted tunnel, it is paramount that this traffic be inspected as well. Luckily, many modern firewalls with specialized hardware can now decrypt that traffic as it passes through. The traffic is also inspected by the application-aware firewall rule base and assuming it is approved, it is re-encrypted and passed to the next hop. This is all conducted with negligible latency and without the source or the destination being aware, or the communication stream being interrupted.
- Deploy An Effective Defense-In-Depth Strategy – Within the anatomy of a hack and with some degree of variability based on the intended outcome, several things must go right for the malicious entity in order to comprise the target. A malicious entity must perform reconnaissance on the target in order to understand the landscape, execute an initial compromise to gain entry and establish a foothold all while operating undetected. Elevated privileges may be needed to gain access to the target data/systems, which means lateral movement and expansion of the footprint, may occur. Once the target is found, the attack is executed and if needed, the data is exfiltrated and if warranted a persistent presence is maintained for future potential malicious activities. In most cases, the time investment to perform all of these actions can be the deciding factor in whether a hacker is successful or becomes disengaged and moves on to the next target. A significant determinant of disengagement is how complex performing any one of the above activities in the lifecycle of a hack is (excluding sophisticated attacks from nation-states and terrorist organizations whose

determination is typically much higher). In order to increase the complexity, and thus, the time required to execute a hack, organizations must think and act with a defense-in-depth mindset. This mindset is not accomplished by procuring and implementing technology alone. This is accomplished by combining technical, organizational and operational controls, which co-exist in a governed manner with levels of understanding and acknowledgement across an organization.

- Rule Effectiveness – When relying on a firewall to thwart access attempts by unauthorized personnel, having a properly configured rule base is paramount. In a study conducted by Wool via Tel Aviv University in 2004, 84 firewall rulesets were reviewed [61]. Of those rulesets, 36 categories of configuration errors were established (Figure 16, 17). Of those 36 categories, 22 were either inherently risky or allowed traffic to pass through the firewall from outside interface(s).

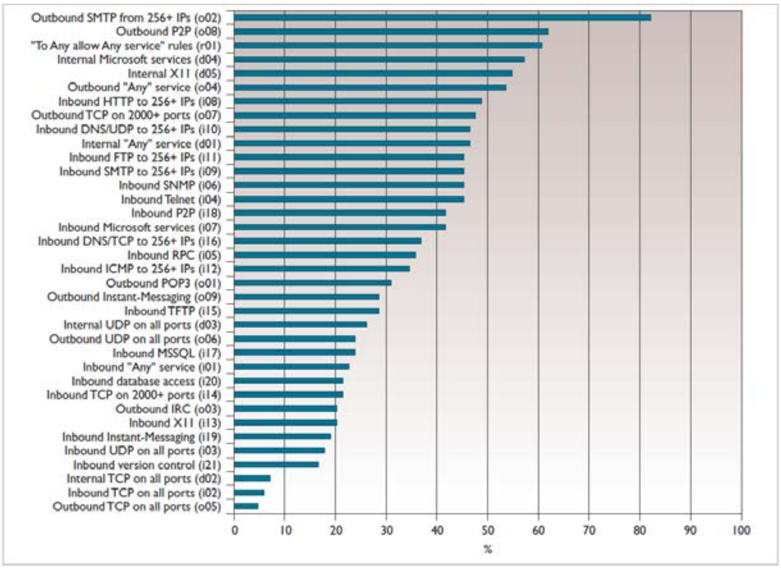


Figure 16: Distribution of firewalls, as a percent, to which the configuration error was present [61] (Outbound traffic “o”, internal traffic “d”, inherent risky “r”, inbound traffic “I”)

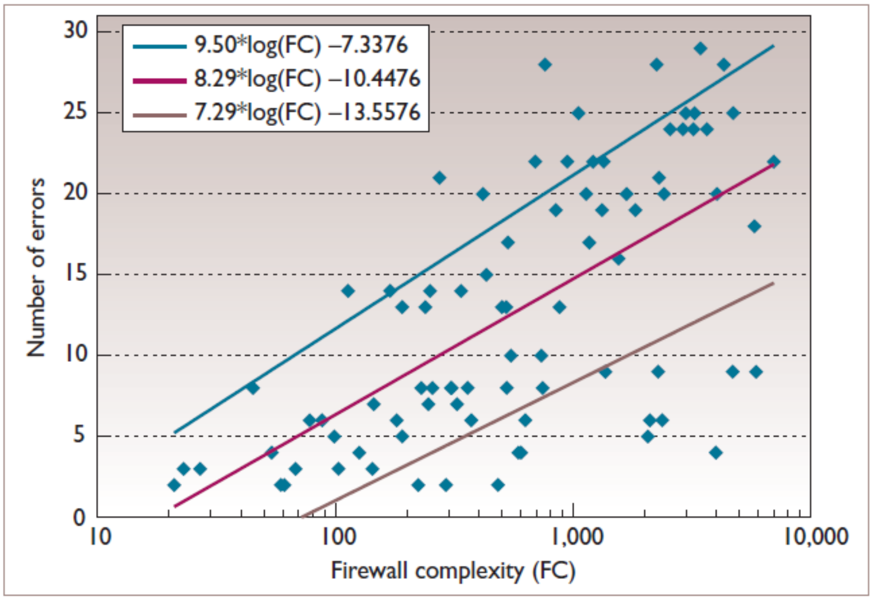


Figure 17: Number of errors as a function of the rule set's complexity [61] (Magenta – least square linear regression fit, teal – one standard deviation above, brown - one standard deviation below).

Deliberate effort spent on keeping a rule base simple is in the best interest of any organization. Studies have proven [61, 35] that organizations should prevent the use of implied or broad rules should be avoided and substituted with explicit rules based on clear intent. Doing so can be a significant contributor to generating simple and effective firewall configurations rather than complex and ineffective ones. A simple approach to firewall rulesets, from a practical perspective, is easier said than done. In order to practically address this component of a well-rounded defense-in-depth scheme, it is also recommended that annually organizations invest in a third-party led firewall configuration and rule audits. This will not only provide a sanity check as it relates to the effectiveness of an organization's firewalls, but it also acts as a health check relating to new threats that an organization may be unaware of. This is especially true within a manufacturing organization, where there may not be dedicated firewall security personnel keeping up with changes in the technology or the threat landscape.

4.1.10 Implement Meaningful Security Awareness Training

Compromises via social engineering techniques are an ever-evolving threat landscape. The attackers devise sophisticated schemes to gain personal information and/or entry into an environment. These attack schemes cannot be mitigated by a specific counter-action; however, preventing and protecting against breaches can be accomplished by applying a defense-in-depth approach as well as an effective security awareness training program. Specific to the manufacturing vertical, as part of creating a comprehensive security awareness program, organizations need to deliberately and consciously educate personnel on OT relevant concepts, industry terminology, and examples of business issues stemming from poor OT related cyber practices. As part of this comprehensive approach, organizations need to educate personnel on the threat vectors and downstream effects of using social media and how being compromised can lead to other lateral advances impacting OT.

- Security Awareness Training - Relative to a security awareness program, studies by Gartner showed that there are four key objectives when deploying an effective security awareness program that drive real meaningful actions [16].

    - Build a knowledge base - Creation of a referencable and easy to understand security and risk knowledge base across the workforce results in a shared understanding of what is important to the organization (e.g. password management, encryption of removable media). Make it available to end users and market its' usefulness.

    - Ability to comply with regulatory requirements - Where required, a regulated enterprise must maintain a cybersecurity training program to ensure that the culture is aligned with the regulatory body requirements. This involves the identification of specific provisions for compliance, capturing specific criteria to satisfy the regulation(s) and applying the necessary controls/provisions to demonstrate adherence.

    - Define a behavioral baseline - In order to be able to hold an individual accountable to adhering to the security policies of the organization, it is important that the expectations of the organization be clearly defined. Additionally, proper education must be provided with objective evidence (signing an acknowledgement form, etc.) indicating the employee has been educated on the required policy and related practices.

    - Motivate secure behavior - Encouraging positive actions while disapproving of undesired behaviors is necessary in order to achieve the desired representative behaviors. Using classical conditioning techniques via reward and penalty systems, the desired and undesired behaviors must be identified and described in enough detail to enable targeted monitoring and reinforcement.

Manufacturing organizations need to begin applying the same importance and rigor to cybersecurity as they do with overall human safety. It can be expected that in some organizations, cybersecurity training is either not addressed or only executed to "check the box" for insurance or regulatory purposes. In addition to this, cybersecurity training needs to be effective for OT personnel, at an appropriate educational level, so that correlations between actions and the impact to the factory floor can be understood clearly.

- Communication/Social Media Exposure To The Network – Organizations should ensure that there is a clear separation between the functions (email, internet access, etc.) that can be performed on PCs with access to the factory operations network(s) and those that should be conducted outside of the network entirely. For example, while there may be a productivity benefit to having an email client (e.g. Outlook) on a factory operations PC or allowing access to an organization's web email service (Outlook Web Access, Gmail, etc.), this provides a direct avenue for email-based phishing attempts to exploit PCs with direct or indirect access to SCADA environments. Access to tools should be restricted on PCs within the factory operations environment and only via an exception process, once a thorough risk analysis has been conducted with mitigating controls established to combat potential malicious activities. In exceptional cases where communications and social media tools are allowed within the factory operations environment, clear and deliberate education must be provided related to suspicious senders, methods to inject malware via content categories and advanced spoofing techniques employed by those wishing to do harm.
- Sensitive Data Handling – While data classification is an important part of protecting important company data, it is virtually worthless if the employees entrusted to work with the data and systems are not trained on how to classify, store, transfer and destroy it properly. Organizations need to ensure that end user education for sensitive data handling is an open discussion where examples can be shared and data owners are held accountable.
- Identification and Reporting of Security Incidents – Part of a proactive security awareness program addresses the ability of the end user population to speak up when something appears to be awry or troublesome from an IT security perspective. Understanding the

common indictors of concern and knowing who to contact in a timely fashion is critical to thwarting active cyber threats.

4.1.11 Implement Endpoint Protection Fundamentals Across The OT Landscape (Where Possible)

Endpoint protection is like anything else in the security realm; it is only one piece of the security posture and when combined with other technologies and practices it will be effective. As mentioned earlier, a key tenant of information security is that *which is not visible cannot be protected*. Organizations need to have an inventory of assets (hardware, virtual and software), and visibility into the respective configurations, operating system (OS) levels, protocols and communications, as well as who has access, when and for what purposes. These components of an asset inventory define the key areas most often involved when a breach occurs. Building from the asset information, the following capabilities can be addressed relating to endpoint protection.

- Anti-Virus (AV) - Ensure that whichever AV package has been selected it is regularly updated with the proper signatures. Not all signature-based AV packages are effective and should be combined with a software whitelisting service. Where AV cannot be applied within an OT environment, other mitigating controls must be put in place to lower the exposed risk.
- Application Whitelisting - An application whitelisting service allows software on a device to be approved to execute while denying any other software. This level of protection is key when it comes to preventing malware from unknowingly being installed. Within an OT environment, application whitelisting is a strong compensating control that can be instituted when other endpoint security practices cannot be leveraged due to the ICS related constraints (e.g. latency, sensitive interfaces, etc.).
- Endpoint Vulnerability Analysis - Every device within the OT environment that either is on the network or contains some type of communications port (e.g. USB) has a potential attack vector. Not all endpoints and risks are the same. Ensure that a risk-based approach is taken when evaluating investments for additional protections to ensure the broadest and most impactful net is cast when protecting an organization’s assets.

- Safe Computing Practices - IT/OT personnel must further invest in combating the potentially negative effects that human behavior has on technology. Humans themselves are extremely susceptible attack vectors and whether compromised because of social engineering or simple human error, poor education, training and computing practices significantly degrade protections.
- Configuration Management - Assuming the asset inventory has been assembled, organizations should take the next step and document the existing configurations for dissimilar device types. Having this level of information available not only allows an organization to set a strong, hardened baseline, but in the case of a compromise, variations can be more easily identified and investigated. Identifying unauthorized changes as close to real time as possible will allow an organization to limit further potential malicious activity.

Lastly, organizations must study the implications of endpoint protection in an OT context from both of the following perspectives:

- What needs to be augmented in traditional IT approaches in order to ensure efficacy in the OT realm where the devices and software are specialized?
- What constraints exist in the OT realm concerning how endpoints are updated, maintained and designed with respect to endpoint protection mechanisms, and how can human safety and revenue realization remain uncompromised?

4.1.12 Harden PLCs and RTUs

Given that PLCs and RTUs are well designed and intelligent devices running services that can be compromised (e.g. Telnet, HTTP), these devices must be treated the same as any other devices on the network.

- Disable Unnecessary Services / Hardening - Most of these devices come from the manufacturer with many unnecessary services enabled. IT/OT administrators must take the time to work with the manufacturer and understand which services are essential for operation and then disable all other services. Where overlap exists with previously managed services, such as DHCP, a singular solution should be leveraged that provides the most hardened configuration. Once defined, an organizational standard should be established to define a baseline configuration for other like devices within the organization.

- Controls to Limit Ports, Protocols and Services - As part of the hardening process, a system architecture diagram and the requisite data flows should be established to understand the components through which the traffic traverses. This data flow mapping process will allow the organization to understand where the weak links are in a potential attack path so that hardening activities can be applied to the same [30]. Once understood, access control lists (ACLs) should be established to control traffic to the active and necessary ports, services and protocols. If application-aware firewalls are in use, ACL definitions can be created at the application layer [30].

4.1.13 Account Management Practices

Having solid account management practices across the environment, for both elevated and non-elevated accounts, provides another layer of fundamental protection against potential negative impacts. Throughout the recommendations presented earlier in this document, several best practices were discussed, such as changing default accounts/credentials, maintaining a secured asset inventory of highly sensitive credentials, deploying multi-factor authentication, etc. There are additional protections, which should be examined and considered for use; these include but are not limited to:

- For administrative tasks requiring elevated credentials, provision different elevated accounts for different environments. For example, an elevated account used to administer network devices (e.g. firewalls, routers, etc.) should be an entirely different account than the one that is used to administer servers. Separating what each elevated account has access to reduces the threat surface should one of the elevated accounts be compromised. It should be noted that this is all predicated on the assumption that the individuals with these elevated credentials create separate and unique passwords for each account. Sharing the same password reduces the effectiveness of the intended separation.
- Where possible, systems and applications should be configured to require complex passwords for elevated accounts. Complexity should include a minimum of 15 characters,

upper case, lower case, special characters and numbers. Increasing the permutations of possible character combinations significantly decreases the likelihood that elevated credentials can be compromised by brute force methods.

- When new accounts are generated, ensure that passwords are created using a password randomization tool, and the account is placed into a state where the password must be changed upon first use.
- Where possible, have all successful and unsuccessful login attempts be captured by an SIEM so that log correlation and analysis can occur. Provisioning a SIEM in any environment is not an advanced capability; however, using technologies such as user behavioral analysis (UBA) tools are. UBA toolsets provide the capability to analyze disparate sets of logs in order to determine if tasks are being executed that are abnormal to the typical behaviors of the individual (e.g. logging in from another country, logging in in at an abnormal time, etc.).

4.1.14 Data and Systems Backup

Backing up of data, applications and configurations within a SCADA environment may not be a common practice. Organizations that do not have IT and OT integrated teams have a tendency higher potential to forget about the need to backup these critical systems. Additionally, due to the real-time nature of the SCADA systems, specialized software or practices may be needed in order to ensure that the state, data and configurations are properly backed up so that the data can be recovered should a need arise [24]. Along with ensuring that backups are being completed, it is important that other customary practices, such as backup quality validation and testing, occur on a regular basis to ensure that the backups work as designed, should they be needed to restore applications

4.1.15 Organization/Personnel Posturing for IT and OT Success

A notable similarity between IT and OT relates to managing risk. This is the necessary common ground that IT and OT teams should seek in order to improve risk posture and minimize risk that cannot be reasonably addressed. While risk comes in different forms, it is not assessed and mitigated on a consistent basis, nor is the risk strictly viewed from a cybersecurity lens. In order to effectively manage all technology risk in an enterprise (IT, OT, IoT and safety where tech and physical intersect), a manufacturing organization should look to establish the role of a Digital Risk Officer (DRO). The DRO should be functionally separate from IT and plant management and should primarily be a business leader and specialist at engaging teams and effectively communicating in order to assess and eliminate/mitigate the technology risks within an organization. This person should not be a technologist; however, he/she should be able to fulfill the expectations detailed below and in Figure 18:

- Work with executive management to determine acceptable levels of risk
- Establish a governance framework; define roles, responsibilities and awareness thereof
- Develop a security vision and strategy for the entire organization (IT and OT)
- Establish and maintain the combined security program
- Develop, manage and control the security policy framework

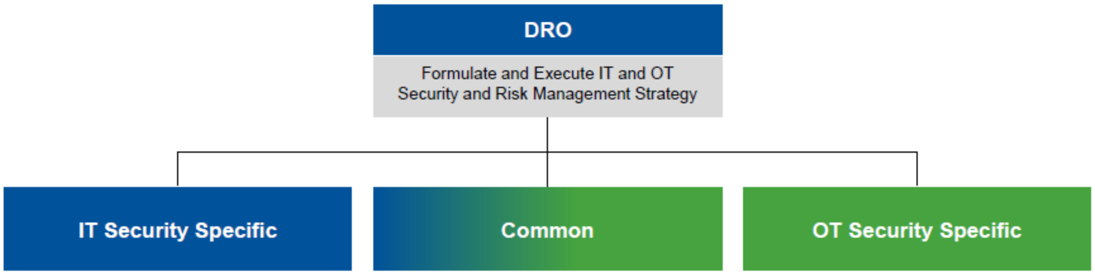

DRO
Formulate and Execute IT and OT Security and Risk Management Strategy
IT Security Specific
Common
OT Security Specific

Figure 18: Digital Risk Officer paradigm [58]

By establishing a DRO within the organization, security is no longer an IT or an OT issue, it becomes an issue of managing digital risk from a business perspective. Handling the digital risk in this manner breaks down cultural barriers between the different organizations, and allows both to operate on neutral territory, working in the best interest of the organization. With the neutral, third party DRO in place, it is somewhat natural that he/she becomes an advocate for functional leaders and helps to navigate this evolving landscape. A sample representation of how the DRO fits into the organization with other executives/leaders is shown below in Figure 19. This person will need to be business minded when facing complex problems and will need to navigate the politics of an organization to reduce the examined risk, regardless of which departments are impacted.

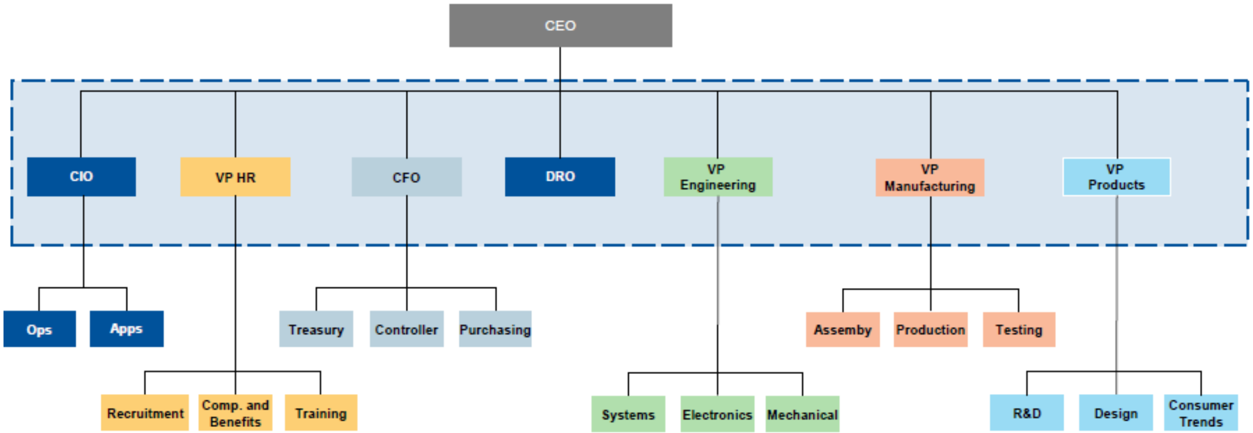


Figure 19: Digital Risk Officer and enterprise alignment with other executive roles [58]

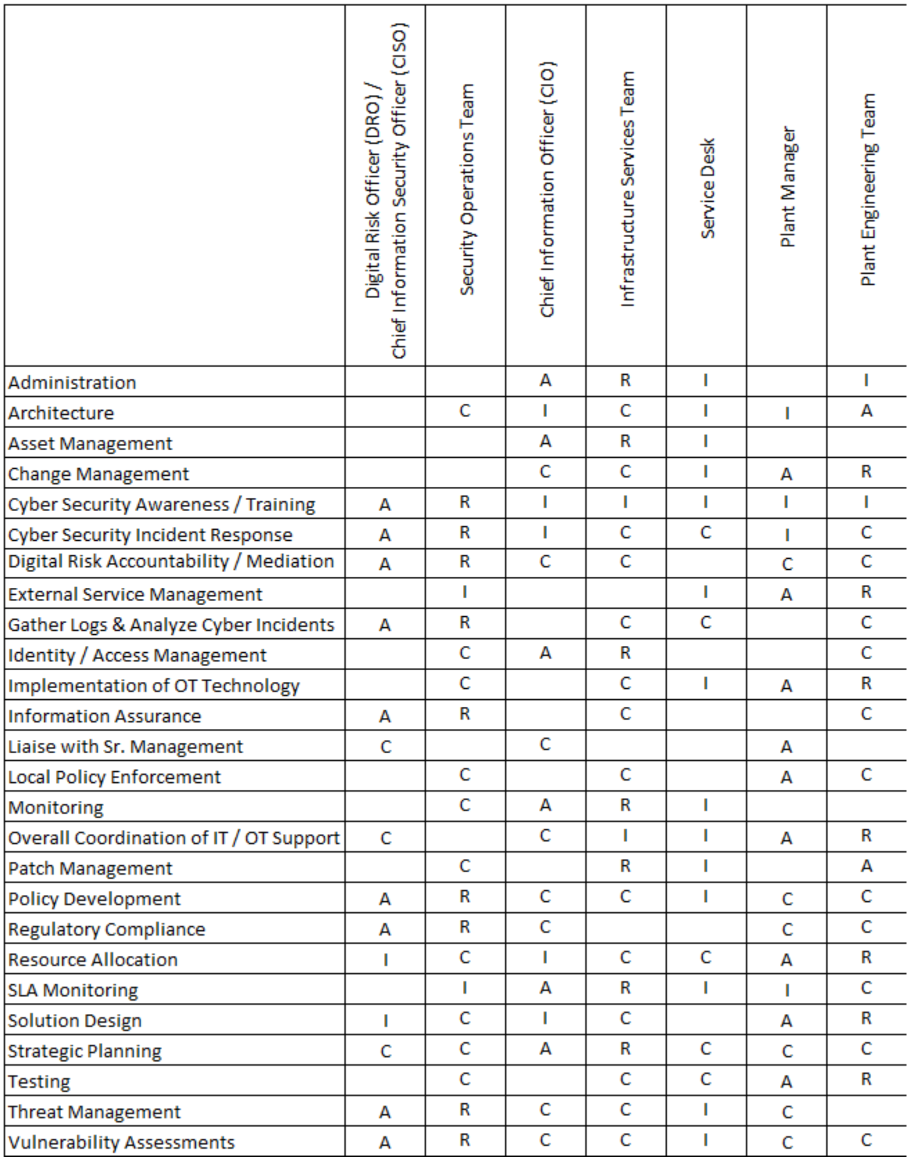
4.1.16 Governance for IT and OT Success

Aligning personnel across the organization with the combined IT/OT strategy is necessary before technology decisions are made. This is usually difficult because the stakeholders of IT and OT are different individuals in the organization and may view and accept risks differently, which in turn can create conflict between technical departments/individuals. This is another important example of where instituting a DRO can pay dividends.

Clear governance will defuse conflict. Establishing a single governance body and associated processes will allow all interested parties to participate collaboratively in order to ensure the right decisions are being made and the risks (initial or residual) are acceptable to the organization. The benefits of a clear and well-understood governance model for the security of IT and OT include but are not limited to:

- Establish Accountability, Responsibilities and Authority — The combined governance team should set the roles, responsibilities and authorities of all resources in the organization, regardless of whether it is in the IT or OT realm. This will reduce the number of conflicts and enable optimal resource use.

- Align Risk Tolerance — The single governance body should agree on a common risk tolerance for integrated IT/OT environments.
- Act As The Steering IT/OT Security Committee — The single governance body should oversee the security program activities across the IT and OT landscapes. This facilitates the identification of duplicated effort, the optimization of security skills and the allocation of the security investment/budget based on risk to the organization.
- Ensure That Business Objectives Are Properly Supported — By including senior business representatives with operational and financial accountability in the combined governance body, business goals will be included in the scope of the security program for both IT and OT.
- Set The Overall Direction — The governance body should set the strategic direction for the security program, taking non-security-related topics into consideration where impacts are potentially detrimental to the security program.
- Prioritize Security Activities Across IT And OT — The priorities for all security-related activities can be set across both domains.
- Reconcile Periodic Conflicts — Typical conflicts that require negotiation include situations in which:
    - A resource owner believes he/she has a valid business reason for requesting exemption from an existing policy.
    - Different resource owners have different risk appetites for respective systems, even if these systems share hosting resources.
    - A business owner may be willing to accept a risk, but the risk exceeds the enterprise's risk tolerance.
- Set and Agree Upon Responsibilities - Understanding that the stakes are high and that potential benefits are on the horizon, it is recommended that organizations clearly define and assign responsibilities. It is also recommended that organizations implement a responsibility and accountability structure, also known as a RACI matrix. In situations where ambiguity and complexity must be addressed, a well-defined RACI can provide clarity. It indicates which personnel or departments are responsible and accountable and which need to be consulted and informed. A sample RACI, can be found below.



	Digital Risk Officer (DRO) / Chief Information Security Officer (CISO)	Security Operations Team	Chief Information Officer (CIO)	Infrastructure Services Team	Service Desk	Plant Manager	Plant Engineering Team
Administration			A	R	I		I
Architecture		C	I	C	I	I	A
Asset Management			A	R	I		
Change Management			C	C	I	A	R
Cyber Security Awareness / Training	A	R	I	I	I	I	I
Cyber Security Incident Response	A	R	I	C	C	I	C
Digital Risk Accountability / Mediation	A	R	C	C		C	C
External Service Management		I			I	A	R
Gather Logs & Analyze Cyber Incidents	A	R		C	C		C
Identity / Access Management		C	A	R			C
Implementation of OT Technology		C		C	I	A	R
Information Assurance	A	R		C			C
Liaise with Sr. Management	C		C			A	
Local Policy Enforcement		C		C		A	C
Monitoring		C	A	R	I		
Overall Coordination of IT / OT Support	C		C	I	I	A	R
Patch Management		C		R	I		A
Policy Development	A	R	C	C	I	C	C
Regulatory Compliance	A	R	C			C	C
Resource Allocation	I	C	I	C	C	A	R
SLA Monitoring		I	A	R	I	I	C
Solution Design	I	C	I	C		A	R
Strategic Planning	C	C	A	R	C	C	C
Testing		C		C	C	A	R
Threat Management	A	R	C	C	I	C	
Vulnerability Assessments	A	R	C	C	I	C	C

Figure 20: Proposed sample IT/OT RACI

Overall, as IT and OT continue to converge, organizations will need to pay special attention to these areas of concern and will need to leverage a defense-in-depth strategy with a risk aware, governance-based operating model. IT-based security controls in OT environments are not as straightforward to implement and maintain. Effective policies and procedures revolving around risk management, mitigating practices/controls, cybersecurity awareness, and security compliance assessments act as enablers to apply security controls from a standpoint of acceptable risk, prioritizing safety and reliability.

Chapter 5: Review of Selected Recommendations Which Have Been Implemented

5.1 Introduction

This section aims to select a subset of the recommendations identified in Chapter 4 and discuss the implementation of those recommendations as a means to share the results of those efforts and what was learned. In each subsequent section, we will review each subject matter area's starting position, the technology / approach implemented and the outcomes of the completed effort.

5.2 Firewalls

The existing firewall architecture was a legacy installation, leveraging Cisco Adaptive Security Appliances to filter and restrict traffic based on source address, destination address and ports attempting to being accessed. The existing solution provided a fundamental level of protection, however, it was dated and improvements were desired in order to elevate our security posture, specifically as it related to application-aware capabilities. We evaluated a number of different vendor solutions and selected Palo Alto as our next solution for the enterprise and over a one year period, we replaced all legacy devices with Palo Alto firewalls. Some of the outcomes of the efforts are noted below.

- Implementing these modern application-aware firewall rules in order to evaluate traffic at a higher level, increased visibility to application level security threats. As an example of the improved visibility, by doing this we were able to identify OT services leveraging HTTP (over port 80 and 8080) rules being used to exchange information in an unorthodox way. The legacy firewall technology was unable to identify this issue and was allowing the application to bypass the need for specific firewall rules as well as creating an unneeded security hole to the OT firewall zone. Once identified, this was addressed with the plant engineers and remediated with the third party system integrator.

- Third party support organizations, with the help of the plant engineers (shadow IT), had deployed a VPN concentrator to establish site-to-site connections between organizations to allow direct access into our environment over HTTPs. The Palo Alto firewalls were able to decrypt that traffic and identify it as a VPN tunnel, not just a persistent HTTPs connection. We were able to work with the plant engineers to cease that behavior and have that tunnel terminate on an IT managed Palo Alto firewall, thus eliminating an insecure and unmanaged backdoor connection.

5.3 Network Segmentation

At the beginning of the effort to improve network segmentation for the enterprise, the ICS environments were on the same network as other enterprise assets. Needless to say we had a long road ahead in order to improve the security posture; a number of advancements were implemented.

- Segregating all OT devices from the enterprise network was the first task and the most laborious. A lack of a complete and up-to-date hardware asset inventory required a significant manual effort to be conducted to not only understand the role of the device on the network, but also identify if it participates in any way in manufacturing operations. All OT devices were placed within one firewall zone off of the Palo Alto firewall pair. After a few weeks of evaluating the traffic traversing the firewall zones in a listen only mode, we had enough information in order to implement the initial ruleset to restrict traffic as necessary while dropping all other traffic. This allowed us to reduce the threat surface for the OT environment by restricting access inbound / outbound for this segment.
- With the environment segmented and the Palo Alto firewalls in place, leveraging the application aware capabilities, we began to understand more as it relates to the traffic patterns of our OT environment. By doing this we identified a number of improvements necessary to retain traffic within the manufacturing firewall zone. Some findings related to simple misconfigurations and others required services housed on shared servers to be split apart so that we could effectively segregate all traffic properly and prevent unnecessary traffic from traversing the firewall.
- For the majority of our OT environment we segmented devices into one of two private community VLANs. The first contained devices that commonly did not require human

interaction (e.g. PLCs, sensors, etc.) and could be contained within the same community VLAN. All other OT devices, which commonly did require human interaction, such as HMIs, factory floor PCs, data historians, and other MES processes were placed into a second community VLAN. In order for devices to talk across communities, traffic exits to the promiscuous port which in our case is a layer 3 switch. We still have work to do in order to apply ACLs to restrict traffic further, however, the foundational pieces are in place so that when ready, we can begin evaluating traffic as needed.

- For IT administration purposes, all IT admins have been provisioned a dedicated virtual server in a bastion host network. All IT / OT administration activities are to be performed from these dedicated virtual servers within our corporate data center. These virtual servers are themselves hardened and not allowed to access the internet, company email services as well as a handful of other controls to reduce the potential for compromise. Additionally, their assigned company laptop is no longer allowed to be used for any administrative activities; it is solely to be used for general, non-elevated business functions (e.g. email, internet access, etc.). This set of changes was not well received by the IT staff as we were modifying how each administrator conducted their day-to-day duties. Despite it being an unwelcomed requirement, the complaints have subsided and we have even identified opportunities for further improvement in tangential areas of interest (e.g. script repositories for common administrative tasks).

These changes have been implemented for a subset of the enterprise where the greatest risk to human safety and our intellectual property exists. We've focused on a small number of pilot sites in order to operationalize the thinking, approach and implementation plan prior to rolling this out across the enterprise globally. This effort was conducted hand-in-hand with the site leadership, with detailed planning and organizational change management along the way.

5.4 Asset Inventory / Management

At the beginning of our asset management journey, there was no asset inventory other than outdated, ad-hoc spreadsheets to denote what PCs had been assigned to which employees. As an asset management strategy was assembled, it was decided to focus on software asset management first and address hardware asset management once network segmentation was properly implemented so that we could leverage the capabilities of NAC and Cisco industrial network director to identify and fingerprint all network connected devices.

The first step to introduce software asset management to the organization consisted of evaluating and selecting a toolset to act as a software entitlement reconciliation engine to inventory and assess our landscape of installed software. After careful analysis and evaluation we selected Snow Software for this task. With this SaaS solution we installed agents on every PC and server in the enterprise globally. The inventory information as well as statistics related to frequency of software usage, software signatures, location, MAC & IP addresses as well as a plethora of other associated metadata are synchronized to their cloud services and made available for our use. Some of the other important benefits of implementing the solution include but are not limited to:

- Ability to gain visibility to the software install base for specific application packages. This becomes useful to determine which PCs have OT related software installed so that additional investigation can be performed (e.g. hardening, identifying users with access to OT, etc.).
- In conjunction with application whitelisting efforts, the database which gets created as a result the software inventory and reconciliation process is a useful tool in order to assess any newly identified software blocked by Carbon Black. While these two tools are not integrated, the Snow license entitlement engine acts as a useful resource for manual assessment related to information on the software publisher, installation information, licensing status, scope of usage by location/department, etc. to compare against.
- Through the Snow engine, we are able to identify cracked and potentially malicious software in the environment. This has allowed our asset management resources to investigate, and work with the networking team to place the asset in quarantine while the root cause and corrective actions are instituted.

The one constraint we faced when deploying this solution was that we underestimated the potential risk relating to General Data Protection Regulation (GDPR). Given that this is a cloud solution and information could be gleaned from the service which could be used to infer an employee's productivity (e.g. the frequency to which applications are executed), we needed to work with our German data privacy officer in order to demonstrate how this information would be used, who has access to this data as well as the cyber protections that have been implemented to protect this data. Upon proceeding through the formal process for GDPR compliance we were granted approval to continue execution of the project.

5.5 ICS Device & OT PC Hardening

At the beginning of this effort, the existing environment did not have any OT devices hardened. Many of these devices were implemented out of the box and never properly configured prior to deployment. As we progressed in our analysis, as identified a theme that OT machinery vendors typically implemented the devices ensuring that the equipment was unencumbered in any way from potentially having operational issues in conjunction with the rest of the environment.

Relating to ICS devices, once I was able to separate the OT environment from the rest of the enterprise network, the first action taken was to use Nessus, a vulnerability scanning tool, to perform a port scan in listening mode, in order to understand what ports and protocols were being leveraged across the OT networks. Conducting the port scan in listen mode prevented any issues related to Nessus attempting to assess vulnerability compliance, thus potentially knocking some sensitive OT devices off of the network. Once this was completed, the results were examined and assessed against the newly devised software asset management database and environment architecture diagrams (outdated but useful to understand the OT architecture). Once the assessment was complete, we were able to identify a number of problems, including but not limited to:

- Unnecessary and redundant services running in the environment, such as DHCP. To remediate we shut off those services and leveraged singular IT managed services where available.
- Many devices were configured to listen on multiple services such as HTTP, HTTPs, FTP, Telnet, SSH, etc. Upon further investigation, it was determined that most of the devices only needed one of these to be active. Where possible, the secured version of the protocol

was selected (SSH over TELNET, HTTPS over HTTP) and the other unnecessary protocols were disabled.

- It was determined that many of the devices were configured to be logged into using default administrator credentials. As part of the remediation effort, credentials were streamlined where possible to limit access, create complex password strings, secure shared credentials in a PAM tool and where possible, ensure plant engineers had individual accounts to login to the devices rather than using shared credentials.

The effort to harden the ICS device footprint was initially met with resistance and concern. The project was executed with executive sponsor approval and done so in a manner where the plant engineers were side-by-side with the IT engineers and third party vendors every step of the way. At the conclusion of this effort, all parties were satisfied, with no unplanned downtime or negative consequences otherwise. Additionally, as a by-product of these efforts to port scan the environments looking for unnecessary services, we were able to make material improvements to our vulnerability management practices.

Specific to the Windows PCs which operate in the OT environment, a number of different actions were taken in order to harden those devices. They include but are not limited to:

- Creation of a set of Windows 7 and Windows 10 operating system images solely to be used for OT PCs. This image was hardened by removing unnecessary services, applications and applying numerous registry edits to limit the threat surface.
- All internet access from these PCs was removed other than those destinations necessary to perform their job function (supplier portals, timecard services, payroll, etc.).
- In order to login to the OT PC, plant operators were required to login with multi-factor authentication using a combination of Duo Security SaaS software and Yubikey hardware.
- All removable media was restricted from use. Access was only granted on an exception basis, for a specific individual and time period. Business justification, manager approval and security operations center review are all required in order to gain exception approval.

- Application whitelisting was implemented leveraging the Carbon Black suite for endpoint protection. To begin, agents were installed on all OT PCs and servers in low-enforcement mode. While in low-enforcement mode, the agent fingerprints the PC or server to understand what applications are executed in order to build a “white list” of known good executables. This was performed for about three months at which point in time the environment was slowly migrated to high-enforcement mode. When in high-enforcement mode, when ay software is attempted to be executed, the agent checks to see if it is a known good application in the “white list”. If found in the list, the execution is allowed; if not found, the execution is blocked with user asked to provide context to the action (if they were aware) or to deny that anything was executed (potentially malware).

At the completion of the Windows hardening efforts the majority of the implemented controls were still in place with only a few changes.

- The multi-factor authentication requirements needed to be revised for some sensitive OT PCs which required a shared account to be used to execute a legacy manufacturing application. Having multi-factor authentication enabled was preventing the process from automatically starting. Over time, various other processes needed to be exempted for similar reasons but the majority of the environment is still protected.
- A few key plant engineers required perpetual removable media exceptions in order to obtain diagnostic data from the OT PCs. This was allowed as the alternative would have required the PCs to be able to upload their data to an internet hosted cloud service.

Chapter 6: Conclusion

6.1 Summary

15 to 20 years ago, a robust cybersecurity posture for a manufacturing company most likely meant that the company patched Windows devices, had implemented firewalls at the edge and had other protection-based services for the enterprise network, leaving the OT environment untouched, and in many cases, unprotected. The days of fundamental protections and turning a blind eye to the manufacturing network are no longer. Technology is much more complex, threats have significantly advanced and attack methods are specialized, targeted and persistent.

The evolution of smart manufacturing is on the rise and organizations are beginning to pay attention to the compelling benefits for customers and the bottom line. As organizations look to achieve the benefits of SM, it is crucial to also look at the manufacturing organization's security posture in a focused and deliberate manner. Otherwise, organizations will not only fail to realize the benefits of SM, but more importantly, will potentially introduce a new array of security vulnerabilities and threats. Organizations must perform the fundamentals to prevent, detect and mitigate risks to the manufacturing environment, whether the risks currently exist or are introduced via an effort to drive SM adoption. Inability to implement a reasonable and prudent defense-in-depth strategy will introduce new risks, some of which will be unlike anything previously seen by the IT/OT support organization(s). Manufacturing leaders need to assume a breach, work to mitigate risks and take a proactive cybersecurity stance to protect customers, and more importantly, the safety of employees.

6.2 Future Research

Smart manufacturing is quickly evolving. Technology is rapidly augmenting as new concepts and use cases are developed by manufacturing organizations and the possibility of a "connected factory" provides new and exciting insights, daily. Given this evolving backdrop, there are several topics that can be explored beyond this research. Further research topics include but are not limited to:

- Cloud Manufacturing Operations – Cloud-based ICS/SCADA services are being introduced to integrate and manage factory floor operations. How it affects the traditionally staunch and slow-to-adopt mentality and investment cycle of the manufacturing vertical could be game changing.
- Encryption in ICS Environments – The state of encryption across the factory floor, and how devices currently do/do not securely communicate across the LAN and WAN could be investigated, along with cipher strength capabilities and limitations.
- Technology Leapfrogging – Given the established nature of manufacturing technology, opportunities for companies to strategically delay investments as SM becomes more mainstream could be investigated in order to leverage the advantages of being a late adopter.
- Software Defined Everything – How the software defined paradigm of everything, from firewalls to controllers, impacts manufacturing security operations, as well as OT.
- Bring Your Own Device (BYOD) – The impacts of BYOD on a manufacturing operation, the risks and control issues.
- Boundary Defense – Additional boundary defense protections could be investigated, which could be specific to OT environments in order to quarantine/defend from external and enterprise-focused attacks.
- Smart Manufacturing Standards – The vast array of authoritative bodies (ISO, IEC, NIST, country sponsored initiatives, etc.) could be assessed, focusing on where there is overlap, consensus and lack of agreement. Additionally, specific research could be conducted regarding the lack of U.S. involvement as a nation in driving SM and Industry 4.0 from the top down (government), as compared to other countries (e.g. Germany with Industrie 4.0, China with its China 2025 initiative).
- AI for Manufacturing – The potential cybersecurity concerns associated with adopting AI and ML within manufacturing environments deserves further consideration.

- Data Privacy – The issues that exist relating to the manufacturing industry, both from a product creation perspective and the services portion of produced goods. Some products create and store data, potentially accessible by the manufacturer, so global government regulation (e.g. GDPR) should be analyzed as it affects the cybersecurity of the end user.
- Block chain – The application of block chain to manufacturing processes in order to manage cyber-risk.

References

1. "2008 Turkish Oil Pipeline Explosion May Have Been Stuxnet Precursor." 2014. http://homelandsecuritynewswire.com.
2. Antova, Galina, and Patrick McBride. "The Folly Of Vulnerability & Patch Management For ICS Networks." Dark Reading. 2018. https://www.darkreading.com/vulnerabilities---threats/advanced-threats/the-folly-of-vulnerability-and-patch-management-for-ics-networks/a/d-id/1329154.
3. Byres, Eric. "Summing Up Stuxnet In 4 Easy Sections." Tofinosecurity.com. 2011. https://www.tofinosecurity.com/blog/summing-stuxnet-4-easy-sections-plus-handy-presentation
4. Byres, Eric. "Using ANSI/ISA-99 Standards To Improve Control System Security." 2012. Tofinosecurity.com.
5. Cimpanu, Catalin. "Researchers Create Poc Ransomware That Targets ICS/SCADA Systems." Bleeping Computer. 2017. https://www.bleepingcomputer.com/news/security/researchers-create-poc-ransomware-that-targets-ics-scada-systems/
6. Cuppens, Frédéric, Nora Cuppens-Boulahia, and Joaquın Garcıa-Alfaro. "Detection And Removal Of Firewall Misconfiguration." *International Association of Science and Technology for Development* 2005: 154-161.
7. "Cybersecurity Framework." NIST. 2018. https://www.nist.gov/cyberframework
8. Dalakov, Georgi. "History Of Computers And Computing, Automata, Ctesibius Of Alexandria." History-computer.com. http://history-computer.com/Dreamers/Ctesibius.html
9. "Everything You Need To Know About IIoT." Ge.com. https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things
10. Franzi, Christa, Ian Flatt, and Jim Damicis. "Understanding Advanced Manufacturing." Camoinassociates.com. 2014. https://www.camoinassociates.com/understanding-advanced-manufacturing.
11. Fruhlinger, Josh. "What Is Stuxnet, Who Created It And How Does It Work?" CSO Online. 2017. https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html
12. "GTAI - Policy." Gtai.de. 2018. https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Why-germany/industrie-4-0-why-germany-policy.html
13. Hanes, David et al. *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things*. Cisco Press, 2017.

14. Harp, Derek R., and Bengt Gregory-Brown. "IT/OT Convergence - Bridging The Divide." Ics.sans.org. 2018. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf
15. Hayden, Ernie. "An Abbreviated History Of Automation & Industrial Controls Systems And Cybersecurity." 2014. https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf
16. Huisman, Joanna. "Effective Security Awareness Starts With Defined Objectives." Gartner.com. 2018. https://www.gartner.com/document/3606018?ref=TypeAheadSearch&qid=9bc3e77d968bdc55e7d390
17. "ICS-CERT." Ics-cert.us-cert.gov.
18. "ISA/IEC 62443 Cybersecurity Certificate Programs- ISA." Isa.org. 2018. https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/
19. Kelly, John E. "Computing, cognition and the future of knowing." Whitepaper, IBM Reseach 2015: 2.
20. Berry, Bob. "Knowledge Base: SCADA System History And Brief Overview." 2011. Dpstele.com. http://www.dpstele.com/scada/knowledge-base.php
21. Caswell, Jayne. "A Survey Of Industrial Control Systems Security." Cse.wustl.edu. 2011. https://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html
22. Hall, Linda et al. "IT Key Metrics Data 2018: Key IT Security Measures: By Industry." Gartner.com. 2017. https://www.gartner.com/document/3832778?ref=ddrec&refval=3833070
23. Lee, Robert M., Michael J. Assante, and Tim Conway. "ICS CP/PE (Cyber-To-Physical Or Process Effects) Case Study Paper - German Steel Mill Cyber Attack." Ics.sans.org. 2014. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
24. Li, Xiao-lei, Yong Zhai, and Ru-zhi Xu. "Research On Data Backup And Recovery Technology In SCADA System." 2009 First International Conference on Information Science and Engineering (2009). https://ieeexplore.ieee.org/document/5454780
25. "Local Administrator Password Solution." Technet.microsoft.com. https://technet.microsoft.com/en-us/mt227395.aspx
26. MacMillan, Robert, and Jouda Christine Seghair. "Breach Detection | Controlling Dwell Time Is About Much More Than Compliance." Medium. 2018. https://medium.com/secjuice/controlling-dwell-time-its-about-much-more-than-compliance-23a2149e590e
27. "Made In China 2025: Global Ambitions Built On Local Protections." Uschamber.com. 2017. https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf
28. "Manufacturing USA." Manufacturing USA. 2018. https://www.manufacturingusa.com
29. "Mcafee Labs Threat Report." Mcafee.com. 2017. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2017.pdf

30. McQueen, M.A. et al. "Quantitative Cyber Risk Reduction Estimation Methodology For A Small SCADA Control System." *Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (HICSS'06) 2006.
31. "Obscurity No More: 4 Steps To Securing The OT Environment For Manufacturing." *Verizon Enterprise Solutions*. 2017. http://www.verizonenterprise.com/verizon-insights-lab/VES/obscurity-no-more-4-steps-to-securing-the-ot-environment-for-manufacturing
32. Peisert, Sean, Matt Bishop, and Keith Marzullo, "What Do Firewalls Protect? An Empirical Study of Firewalls, Vulnerabilities, and Attacks," UC Davis CS Technical Report CSE-2010-8, March 2010.
33. Polityuk, Pavel, Oleg Vukmanovic, and Stephen Jewkes. "Ukraine's Power Outage Was A Cyber Attack: Ukrenergo." Reuters. 2017. https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA
34. Rad, Ciprian-Radu, et al. "Smart monitoring of potato crop: a cyber-physical system architecture model in the field of precision agriculture." Agriculture and Agricultural Science Procedia 6 2015: 73-79.
35. Ranathunga, Dinesha et al. "Case Studies Of SCADA Firewall Configurations And The Implications For Best Practices." IEEE Transactions on Network and Service Management 13.4, 2016: 871-884.
36. "Ransom.Wannacry." Symantec.com. 2017. https://www.symantec.com/security-center/writeup/2017-051310-3522-99
37. Rathwell, Gary, and Ted Williams. "PERA Enterprise Integration Web Site." Pera.net. 2018. http://www.pera.net/
38. Rossmann, Markus et al. "Smart Factories: How Can Manufacturers Realize The Potential Of Digital Industrial Revolution." Capgemini.com. 2017. https://www.capgemini.com/wp-content/uploads/2017/07/smart_factories-how_can_manufacturers_realize_the_potential_of_digital_industrial_revolution.pdf
39. Ruffa, Stephen A. *Going Lean: How The Best Companies Apply Lean Manufacturing Principles To Shatter Uncertainty, Drive Innovation, And Maximize Profits.* New York: Amacom, 2008. Print.
40. Salah, Mohammad. "SCADA Systems." Msalah.com. 2018. Web. http://www.msalah.com/A/SCADA.pdf
41. Selko, Adrienne. "What Makes A Manufacturing Company Competitive? Labor Productivity." Industry Week. 2012.
42. Schuetz, John. "Traditional Industrial Vs. Advanced Manufacturing---Is There A Difference? | Trade And Industry Development." Tradeandindustrydev.com. 2013. http://www.tradeandindustrydev.com/industry/manufacturing/traditional-industrial-vs-advanced-manufacturing-t-8304
43. Scott, Austin. "Tactical Data Diodes In Industrial Automation And Control Systems." Sans.org. 2015. https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057
44. Waltermire, David et al."Security Content Automation Protocol." . 2018. https://csrc.nist.gov/projects/security-content-automation-protocol

45. Shearer, Jarrad. "W32.Stuxnet." Symantec.com. 2017. https://www.symantec.com/security-center/writeup/2010-071400-3123-99
46. "Siemens Productcert And Siemens CERT." Siemens.com. 2018. https://www.siemens.com/global/en/home/products/services/cert.html
47. Sija, Baraka D. et al. "A Survey Of Automatic Protocol Reverse Engineering Approaches, Methods, And Tools On The Inputs And Outputs View." Security and Communication Networks 2018 (2018): 1-17. https://www.hindawi.com/journals/scn/2018/8370341/
48. Snitkin, Sid. "Unidirectional Security Gateways Reduce Risk Of Industrial Cyber Attacks | ARC Advisory Group." Arcweb.com. 2015. https://www.arcweb.com/blog/unidirectional-security-gateways-reduce-risk-industrial-cyber-attacks
49. Stine, Kevin et al. "Volume I: Guide For Mapping Types Of Information And Information Systems To Security Categories." Nvlpubs.nist.gov. 2008. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf
50. Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication 800.82, 2011: 16-16.
51. Stouffer, Keith et al. "Guide To Industrial Control Systems (ICS) Security." nist.gov. 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf
52. Styczynski, Jake, and Nate Beach-Westmoreland. *Industrial Cybersecurity Threat Briefing*. Booz Allen Hamilton, 2016.
53. Tajitsu, Naomi. "Honda Halts Japan Car Plant After Wannacry Virus Hits Computer Network." Reuters. 2017. https://www.reuters.com/article/us-honda-cyberattack-idUSKBN19C0EI
54. Thareja, Priyavrat. “Manufacturing Paradigms in 2010.” December 17, 2012. Proceedings of National Conference on Emerging trends in Manufacturing Systems, *JMIT*, Radaur, March 15-16, 2005. Available at SSRN: https://ssrn.com/abstract=2190326 or http://dx.doi.org/10.2139/ssrn.2190326
55. Tsuchiya, Akihiro et al. "Software Defined Networking Firewall For Industry 4.0 Manufacturing Systems." *Journal of Industrial Engineering and Management* 11.2, 2018: 318. Web.
56. Uribe, Tomás E., and Steven Cheung. "Automatic Analysis Of Firewall And Network Intrusion Detection System Configurations." *Journal of Computer Security* 15.6, 2007, 691-715.
57. Vidal, Steve. "Introduction to PLCs." EC&M Electrical Construction & Maintenance, vol. 106, no. 11, 2007. http://0-link.galegroup.com.wizard.umd.umich.edu/apps/doc/A172065822/ITOF?u=lom_umichdearb&sid=ITOF&xid=41fd145e
58. Voster, Wam. "How To Organize Security And Risk Management In A Converged IT/OT Environment." Gartner.com. 2017. https://www.gartner.com/document/3778363?ref=solrAll&refval=209011499&qid=4249dcae4e4ff146b1d65a4c06019455
59. Voster, Wam. "Establish Successful Executive Security Steering In An Integrated IT/OT Environment." Gartner.com. 2018. https://www.gartner.com/document/code/343544?ref=grbody&refval=3873972

60. "What Is Distributed Control System (DCS)?" Electrical Technology. https://www.electricaltechnology.org/2016/08/distributed-control-system-dcs.html
61. Wool, Avishai. "Trends In Firewall Configuration Errors: Measuring The Holes In Swiss Cheese." IEEE Internet Computing 14.4 (2010): 58-65.
62. Huelsman, Trina et al. "Cyber Risk In Advanced Manufacturing." Www2.deloitte.com. 2016. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-cyber-risk-in-advanced-manufacturing-executive-summary.pdf.