Integrating Security Into the IoT Strategy in the New Converged Environment

Richard Ku
Joe Weiss
Contents

4
IT/OT Convergence and Cybersecurity

6
General Business Challenges

7
General Security Challenges

9
Security Challenges for IIoT

11
Best Practices for the IT/OT Environment

13
Cybersecurity Framework

14
Technologies to Consider

16
Choosing a Security Vendor

17
Conclusion
Consumers want their work, home and mobile devices to communicate together to provide information that was previously not available from isolated systems. This desire is at the root of the Internet of Things (IoT). The rise of IoT started when consumers began to interconnect devices — ranging from personal computers, smartphones, tablets and wearables, to home appliances and home security systems — via the cloud, so that valuable personal and work information could be easily accessed, no matter what the users were doing or where they might be located.

Similarly, commercial and industrial organizations want to gather information across sensors, devices and control systems, often in different locations, in order to provide more intelligence about the operational status of the overall manufacturing process and to make better decisions about operations and maintenance. Hence, the emergence of the Industrial Internet of Things (IIoT), which by definition is an extension of IoT for industrial applications, such as plant floor control and maintenance.

IIoT is one of the fastest-growing innovation sectors across all segments (consumer and commercial) of the IoT market. Most of this growth has been due to significant developments in IoT, networking and big data analytics technologies that improve productivity and efficiency in the operational environment. In the operational environment, IIoT devices generally are network-ready sensors, controllers, actuators, drives and operator displays providing a stream of data, often to the cloud, for big data analytics. However, IIoT devices have not caught up with the security needs in this highly networked, interconnected world.

This paper is aimed at providing guidance to help organizations, IoT and IIoT solution providers, and the industry at large to better understand this new converged environment. It is also intended to improve the planning, designing, implementing and deployment of IoT devices, while ensuring that security is integrated into the IoT strategy across all levels of the organization.
IT/OT Convergence and Cybersecurity

The digital evolution in the commercial and industrial space has gone through many changes in the past couple of decades. Key developments have included corporate connectivity to the internet and the transformation of the organization’s information technologies (IT), i.e., the applications used to conduct daily business through collaboration and digital information exchange. As a result of this transformation, we have seen organizations’ network architectures and workloads shift from a focus on the local area network to an expansion to the wide area network and then to the cloud, enabled by such technologies as virtualization, containers and software as a service (SaaS).

And now the commercial and industrial space is going through a similar digital transformation enabled this time by the networking of operational technologies (OT), i.e., those used in manufacturing, retail, distribution, and utilities and energy operational processes. This more recent transformation enables critical data from industrial control systems (ICS) to be collected and analyzed to help the organization make the right decisions for the improvement of the safety, reliability, availability and productivity of its operating environments.

Both of these digital transformations have created huge business opportunities for the organization. But at the same time, they have exposed the organization’s IT and OT to more security threats and challenges.

In the mid-1990s, organizations began interconnecting their control systems to improve productivity, maintenance and safety. Some of this interconnectivity was to the internet via sensors, endpoint devices, human-machine interfaces (HMIs), and programmable logic controllers (PLC) or remote terminal units (RTU) connected to gateways — the precursors to IoT. While this interconnectivity helped improve reliability and efficiency, security was not a key consideration in the planning, design and implementation of networked control systems. The lack of adequate security planning resulted in increased attack surfaces and successful cyberattacks across many industries. In addition to the lack of security, there often was a lack of adequate collaboration between the OT (the term “OT” didn’t exist at that time) and IT organizations.
As you might suppose, the situation is more complicated today than it was in the 1990s or even in the early 2000s. Companies want to speed up and increase the connectivity between IT and OT to advance business productivity even more. There have been numerous demonstrations of improved productivity and cost savings using IIoT methodologies. However, security has not been a major consideration throughout this digital transformation. At the same time, hackers (individual or state-sponsored), malware writers, and criminal rings are now explicitly eyeing these environments for malicious damage and financial extortion.

There have been cases where industrial control systems have been damaged by cyberattacks¹ and plant systems held up for extortion because the adversary was able to compromise the OT environment through the IT environment. A recent example is the December 2015 Ukrainian power grid cyberattack, where the adversary was able to use the IT infrastructure to shut down the OT environment and disrupt power to thousands of households.²

As various papers, conferences, meetings and actual customer experience have shown, there are still substantial gaps in understanding between the IT and OT environments as to what constitutes a comprehensive cybersecurity plan for the entire organization. As your organization goes through the digital transformation caused by the integration of IT and OT and the increased connectivity in your operational processes, we hope this paper will provide you with some basic information and guidance to help you better plan your IT and OT security policy, governance and framework.

In this paper, we cover several important topics, including the new digital transformation and what it means to your organization in terms of general business and security challenges. We then discuss the security challenges for IIoT and the basic cybersecurity framework necessary for IT/OT integration. Finally, we provide recommendations on which technologies to use and how to select the right security vendor to help your organization thrive amid the new converged environment.


General Business Challenges

According to a forecast by Gartner, the number of IoT devices in use will reach 8.4 billion in 2017 and grow to a staggering 20.4 billion by 2020, and the market opportunity for IoT will reach US$2 trillion by 2017.\(^3\) With the proliferation of IoT devices and technologies in the commercial and industrial sectors, we are starting to see the convergence of the traditional IT and OT environments. This convergence is creating a more collaborative, productive and profitable opportunity for information sharing across the overall organization by providing connectivity for data collection, correlation and analytics.

This convergence has led to a new IT/OT environment characterized by an increase in the numbers of various elements with their respective functions within the ecosystem. There are more devices, sensors and middleware components to provide data for analysis. There are more processors and edge computing servers with added power to perform complex calculations practically in real time. There are also more technologies, such as deep machine learning, for managing and improving analytics. And there are more operating systems, platforms and protocols for facilitating interconnections between the organization and the internet.

At the same time, the convergence of IT and OT has created new dynamic business challenges for the organization. There is, of course, the cost of adopting new technologies brought about by the underlying IIoT digital transformation. This can prove expensive, entail personnel retraining and otherwise require time and resources for it to work correctly.

The need to ensure that all parts of the organization follow all legal and regulatory requirements also becomes an issue. This is because some parts of the organization might not have been subject to certain requirements prior to the deployment of IoT devices in the organization.

Furthermore, lack of visibility and control on IoT devices across the organization is magnified as cyberattacks increase. In line with this, it is critical for the organization’s reputation to be kept intact following cyberattacks or other forms of violation.

General Security Challenges

An unwelcome effect of IT/OT convergence is the expansion of the attack surfaces and threat vectors across the organization. This provides more opportunities for hackers, malware authors and criminal groups to take advantage of. As shown by the Dyn distributed denial-of-service (DDoS) attacks\(^4\) and the WannaCry\(^5\) and Petya\(^6\) ransomware incidents, the adversaries have become more proficient in exploiting these new attack surfaces and threat vectors. In doing so, they are able to bring about major disruptions such as taking down critical domain hosting providers and compromising millions of systems around the world.

Given the profusion of attacks and breaches, cyberthreats are now top of mind for discerning senior executives and board members. This awareness has resulted in increased funding becoming available for the IT environment, but not necessarily for the OT environment, where cybersecurity is still more an afterthought than an integrated part of the business plan.

As a result of IT/OT convergence, we are starting to see significant security challenges for the overall organization. These include lack of security awareness across the IT/OT environment and fragmented security solutions that don’t necessarily work in the OT environment.

Another issue is lack of standards and regulations for IoT technologies, which makes planning and implementation difficult. Also, some security models may not have been built into IoT devices and platforms, particularly those used in the OT environment.

Furthermore, many forms of malware in the IT environment can impact OT. For fear of the potential consequences, the organization itself might intentionally shut down operations due to a malware attack or even just the threat thereof. This sort of self-denial-of-service was exemplified by Honda and Renault


when they halted manufacturing at their respective plants to prevent the spread of ransomware in their systems, even though there were no alarms on the factory floor.\textsuperscript{7,8}

The prevailing security approach in the OT environment is to use IT practices and technologies. Unfortunately, this doesn't always work and, in some cases, has caused problems with operational equipment and devices. For one thing, the IT and OT environments have different views about security as they have different reporting lines and business needs. Consequently, misapplications of IT security in the OT environment arise, which in turn lead to self-denial-of-service and other complications. For example, applying IT resources such as invasive penetration testing and network mapping tools to the OT environment may impact OT systems such as legacy PLCs. Similarly, applying resource-intensive anti-virus software to legacy control system HMs may impact HMs and ICS field devices.

But make no mistake: Cyberthreats in the OT environment are real. There have been more than 700 cybersecurity incidents in numerous industries worldwide, including utility distribution, manufacturing, transportation and healthcare. The impacts range from trivial to considerable equipment damage, to significant environmental damage, to major regionwide power outages, and even to deaths (more than 1,000 deaths and more than US$30 billion in direct damages have been noted to date).\textsuperscript{9} Very few of these incidents were even identified as being cyber-related — which speaks volumes about the lack of control-system cyberforensics and appropriate training. This can be expected to get even more complicated with IoT in general and IIoT in particular.


Security Challenges for IIoT

IIoT is a continuation of trends that have been on the rise since the 1990s. With its emergence, we have seen increased granularity and connectivity in process sensor and control equipment. As well, we have seen increased aggregation of large amounts of cross-sensor, cross-site and cross-customer information in enterprise-level and internet-based repositories.

IIoT advocates predict dramatic increases in the number of “intelligent” devices deployed at industrial sites, the amount of data harvested routinely from such devices, and the degree of central aggregation and analysis of this data. These trends toward increased granularity, increased connectivity and increased aggregation are expected to significantly expand IIoT attack surfaces.

The concept of IIoT comprises successive levels, along with their related security and operational issues:

- Local area networks for collecting and locally processing data from connected ICS objects. Security issue: lack of authentication and security in process sensors. Operational issue: Compromised data can lead to equipment damage, regulatory issues and personal safety hazards.

- Transmission of data to the cloud via gateways. Security issue: lack of security in protocols and gateways. Operational issue: Compromised data can lead to equipment damage, regulatory issues and personal safety hazards.

- Processing and storage of data in the cloud by appropriate platforms and specific algorithms such as big data. Security issue: lack of security of data. Operational issue: Compromised data can lead to equipment damage, regulatory issues and personal safety.

- Interfacing between platforms and end users for monitoring. Security issue: lack of secure communication protocols. Operational issue: Using the cloud for control can lead to unforeseen operational concerns.

In short, the cloud computing environment introduces security and operational concerns that need to be addressed.
IIoT applications are generally built with and therefore inherit the lack of security of existing ICS devices. Existing IIoT networks are being augmented with existing ICS devices (without adequate security) to bring in additional data needed for big data analytics. Interconnected devices currently use custom protocols or gateways to get to universal protocols such as OPC Unified Architecture. Unfortunately, the custom protocols or gateways are often developed without sufficient security considerations.

One of the key selling points of IIoT is reachability: integration between the machines and the humans who run them. Hence, new entry points will need to be introduced into the reference model to achieve increased connectivity objectives. These new capabilities introduce cybersecurity considerations that will need to be addressed.

It is assumed that many industrial applications may need to live with these insecure products for years. Consequently, it will be important to identify any gaps created by differing IT and ICS security and operational requirements as well as to develop compensating controls.

The aforementioned security challenges have led to the establishment by the International Society of Automation (ISA) of a new committee on IIoT cybersecurity: ISA99 Working Group 9.
Best Practices for the IT/OT Environment

In the world of cybersecurity, there is no silver bullet. What you can do in your organization is to minimize the attack surfaces and threat vectors, and be vigilant and proactive in your defense against adversaries. To that end, we suggest that you implement a multilayered defense-in-depth cybersecurity strategy and stop the cyberthreat early in the kill chain across both the IT and OT environments.

Below are some basic guidelines to help in your planning. As this digital transformation continues to take shape with the convergence of IT and OT, there are some fundamental security best practices that we recommend for organizations across all industries. The specific network architecture might vary across the different verticals, but the general approach is the same.

- The vision, strategy and execution of the business plan need to include security, reliability and safety. These should be part of the business planning process at all levels of the organization (regardless if you are an IoT solution provider or a customer).
- Security should be “owned” by one person at the executive level who is responsible for both IT and operations. Security policy, governance and end-user education need to extend across the IT and OT environments as systems are interconnected.
- Technologies and threats across the IT and OT environments should be clearly understood. Technologies that work in the IT environment may not necessarily work in the OT environment. Additionally, threats may be different in the IT and OT environments.
- A threat intelligence framework needs to be set up so that the organization can be up to date on the latest information on threats and be prepared to deal with them.
- Baseline security controls should be deployed across all layers of the organization’s environments. (See Figure 2 below for the security reference diagram that provides guidance on where and how to best deploy security controls across both IT and OT.)
• Regular risk assessments across all environments must be performed to identify vulnerabilities and ensure that the appropriate security controls are in place.

• The organization and customers should consider NIST 800-53\textsuperscript{10} for IT and NIST 800-82\textsuperscript{11} and ISA/IEC 62443\textsuperscript{12} for ICS and OT.

• Establish or update the security patch process to better address vulnerabilities. Follow the recommendations laid out in IEC 62443-2-3, which describes requirements for patch management for control systems.

• Develop ICS-specific policies and procedures that are consistent with IT security, physical safety and business continuity.


Cybersecurity Framework

In defining policies and procedures around the implementation and management of security controls in an enterprise environment, the organization is advised to adopt a cybersecurity framework. This is a series of documented processes that can provide the baseline best practices to help the organization plan, design and deploy security controls on cyberthreats.

Pertinent standards include the NIST 800-53 cybersecurity framework and ISO/IEC 27000 series\(^\text{13}\) for information security, and IEC 62443 for control systems. A security program typically includes the following core components across both the IT and OT environments: Identify, Prevent, Detect, Respond, Recover and Predict. Within each phase, there are specific processes and activities that the organization should follow to ensure the successful execution of the entire framework.

![Diagram of Cybersecurity Framework]

---

Technologies to Consider

For IIoT to provide its projected benefits in the IT/OT environment, security concerns associated with its implementation must be addressed first using available technologies and capabilities.

Doing so, of course, entails development of secure and authenticated process sensors. There’s also the need for a system to detect malware and other ICS network anomalies. In line with this, process anomaly detection could be put in place and correlated with ICS network anomaly detection to understand the process system impact of network issues.

Next-generation firewalls also need to be installed to properly segment IIoT networks and provide predictive threat analysis. As well, integrated configuration management systems are necessary for the integration of security information and event management (SIEM) with ICS configuration management.

There are many other available technologies and capabilities that an organization can adopt to help address its cybersecurity challenges in the new converged environment. These include:

- Next-generation IT and OT host-based intrusion prevention and detection systems, including all IoT and IIoT protocols
- Anti-malware and ransomware protection for both IT and OT environments
- Whitelisting for both IT and OT environments
- Network sandboxing technology that can analyze and monitor for vulnerabilities and threats on the different types of IoT protocols without affecting the operational process
- Threat analytics and correlation solutions that can collect information across different environments to help the management team make decisions
- Encryption technologies for providing authentication and verification, which are a must across all IoT devices and control systems
- Technology for managing versions of devices, control systems, patches and the like across both IT and OT environments to ensure the organization understands the risk across both of these environments (includes management of version, status, last update, control system version, patch version, etc.)
- Security capabilities in the form of software development kits (SDKs) or application programming interfaces (APIs) that can be directly integrated into devices
Deploying security controls across the entire organization also requires a good understanding of the network architecture across both the IT and OT environments. By understanding the network architecture, the organization can better analyze where the threat is coming from and what controls need to be applied in the network architecture to address the threat. Below is a network diagram showing the architecture of the IT and OT environments and where to best deploy security controls to ensure a defense-in-depth protection strategy. By applying security controls and policies in all layers of the network architecture, the organization will make it more difficult for attacks to succeed.

![Network Diagram](image_url)

Figure 2. Basic security reference architecture in the new IT/OT environment
Choosing a Security Vendor

There are many companies that provide security products and services for IT and OT environments. Needless to say, selecting the right vendor is key to the success of cybersecurity implementation across the organization. To help you make the ideal choice, here are some questions you might want to consider when evaluating the security vendor options for your organization.

- Does the vendor understand IT and OT risk assessment and management?
- Does the vendor have security and threat experts from the IT, OT and cloud environments?
- Is the vendor willing to bring in experts where necessary to address specific issues such as ICS?
- Does the vendor use proven technologies that can work in the IT, OT and cloud environments?
- Does the vendor have the technologies to deal with threats across the environment?
- Is the vendor willing to modify and adapt the technologies to deal with evolving threats and challenges in the new converged environment?
- Does the vendor have a proven history of working and developing new technologies to deal with the evolving technology landscape?
- Is the vendor willing to help you go through your digital transformation process?
- Is the vendor going to be around for the next five to 10 years?
Conclusion

IoT, IIoT, IT and OT. As far as the digital transformation in the commercial and industrial space is concerned, these seemingly interchangeable initialisms are far from just being superfluous bits of jargon. Indeed, organizations need to recognize IoT and IIoT as integral parts of the environment brought about by the interconnectivity of IT and OT. It’s also imperative that organizations acknowledge the critical importance of security across all levels of this new converged environment. In the age of IoT, IIoT and IT/OT convergence, security is a concept that organizations simply cannot neglect or treat as a mere afterthought if they are to continue to thrive and survive in the face of cyberthreats.

Consequently, deeper collaboration between IT and OT should be established. This collaboration is necessary because IT has the security knowledge while OT has the domain expertise to know just how security technologies may affect the operational systems. It is also essential to include the C-level executives who need to consider security in the overall business plan, as well as to ensure that IT and OT meet the basic requirements and have the necessary resources to work seamlessly together.

Of course, choosing the right vendor is vital to the enforcement of cybersecurity within the enterprise. In doing so, however, organizations need to bear in mind that in the long haul, security is more than just a product — it’s a process. It’s therefore important for organizations to select a security vendor that has a comprehensive understanding of the ins and outs of cybersecurity as it applies to IT/OT convergence as well as the technologies necessary to address the challenges created by the rise of IoT and IIoT.
Glossary

The following definitions of key terms are used throughout this white paper.

- **IoT (Internet of Things)** – IoT refers to the internetworking of physical devices (also referred to as “connected devices” and “smart devices”). IoT often includes consumer-like devices such as smartphones, tablets, personal activity trackers, and smart appliances, watches, cameras and printers, all of which can connect to the internet. (Note the term “smart,” which implies a remote capability that can be vulnerable to cyberthreats). In the past few years, IoT has been extended to include vehicles, buildings and other objects embedded with the networking capability to collect and exchange data.

- **IIoT (Industrial Internet of Things)** – IIoT refers to the use and incorporation of IoT technologies within industrial applications, using machine learning, big data analytics and machine-to-machine (M2M) communication protocols. When adequately secured, these technologies enable greater efficiency and consistency, and more reliable and safer industrial operation. IIoT normally refers to robotics, medical devices or industrial applications. It requires smart sensors and remote connectivity (though not necessarily to the internet), as well as secure remote access and network segmentation.

- **OT (operational technology)** – This term includes the networking associated with industrial control systems (ICS) — such as supervisory control and data acquisition (SCADA), plant distributed control systems (DCSs) and programmable logic controllers (PLCs) — and any operational process. OT does not encompass the actual control systems including sensors, actuators, drives and plant equipment such as turbines, valves, compressors, transformers and robots. As ICSs are “purpose-built,” not general-purpose systems and devices, many ICS devices have limited computing resources and often use proprietary operating systems and communication protocols. ICSs often are designed with “security by obscurity” and rely on “air gapping” for security (i.e., isolation from the network), even though the air gap does not actually exist.

- **IT/OT convergence** – This refers to the integration of IT systems used for business-system data-centric computing with OT systems used to monitor and control physical processes in commercial and industrial operations. This requires close integration with the IT and operational organizations.
About the Authors

Richard Ku is the senior vice president of commercial IoT business and market development at Trend Micro. He has been working for 25 years in the cybersecurity industry as researcher, product manager and head of Trend Micro’s user protection product group.

Joe Weiss, PE, CISM, CRISC, is a managing partner at Applied Control Solutions. An ISA fellow, IEEE senior member and ISA99 managing director, he has been working for 40 years in the ICS and security industry.
TREND MICRO™
Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners’ needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.