GRANTEK

Industrial IT for Digital Transformation Guide

- Networking
- Computing
- Cybersecurity
- Complete Industrial IT

Grantek Industrial IT & Cybersecurity Services

Introduction & Purpose

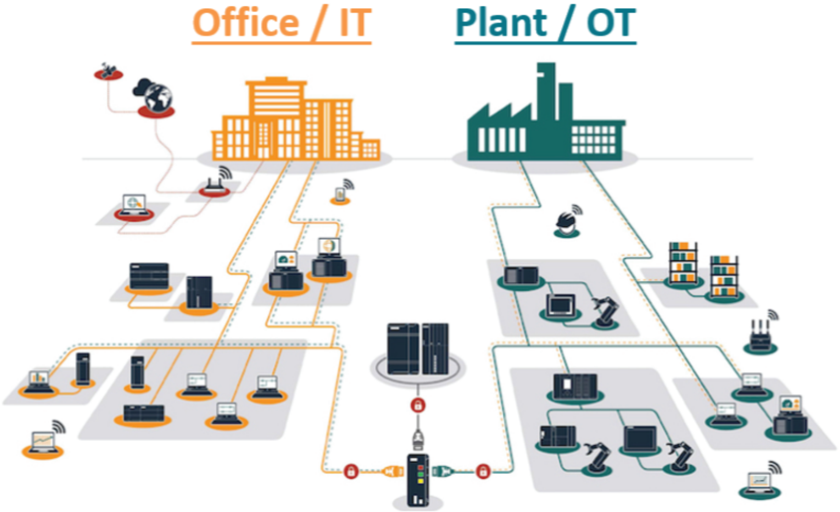
Today, the technologies which make up a company's industrial operations are evolving faster than ever (and in fact, it's accelerating). Competing platforms regularly leapfrog each other for market dominance and user preference while start-ups flush with cash from investors shake up established norms. Mergers and acquisitions can alter the trajectory of innovation and instantaneously impact experts' speculation on the future, creating a moving target for those trying to estimate what the future will be. Those facts alone make it difficult for any leader to navigate their options, but it's not just the available technologies and solutions that are changing. The underlying problems people, organizations and society are wrestling with are changing, too. For example, cybersecurity in the controls environment was not a forefront concern a few decades ago, nor was the privacy of user and customer data.

Luckily we can take comfort in the fact that, while things are moving fast, they're not moving too fast to understand and we are all riding the same wave of change together, more or less. If the problem is boiled down to its core, and we look at the past and present of our own organization and our peers, the next step isn't as difficult to determine. That philosophy can be applied to evaluate what your next big investment in Industrial IT should be to ultimately pursue Smart Manufacturing and Industrial Internet of Things (IIoT) applications.

The History of Industrial IT

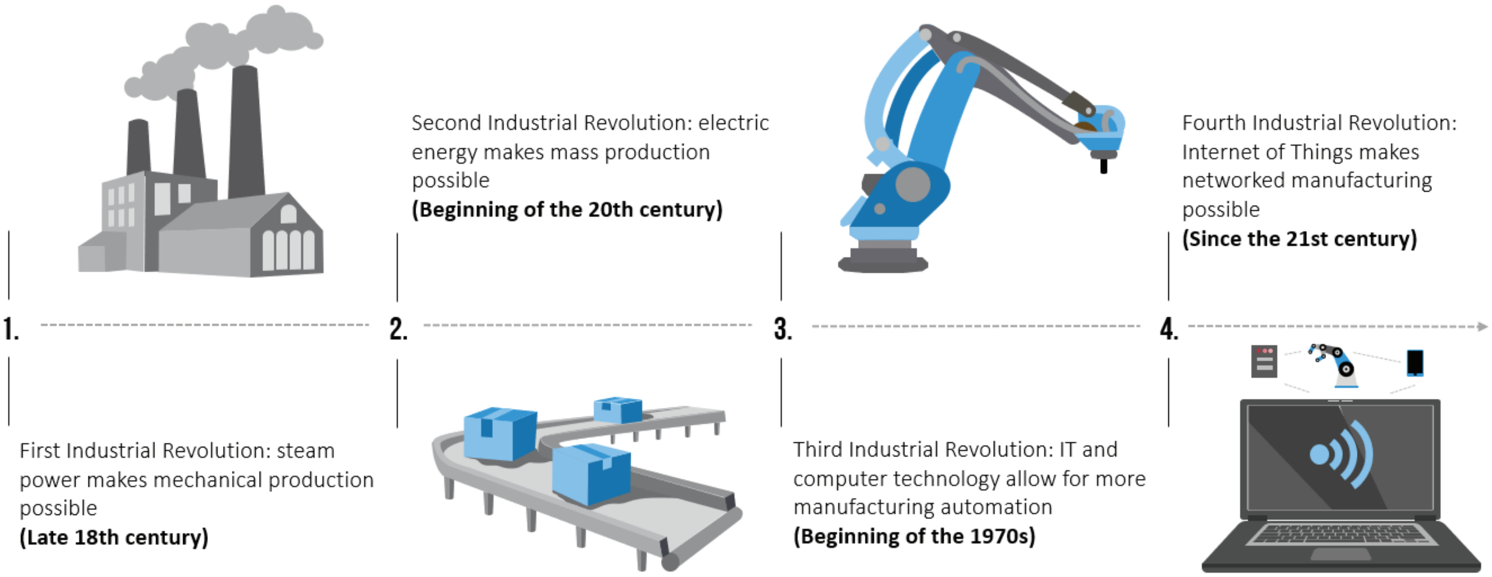
Information Technology (IT) is a broad term but today is typically used to describe computer systems and networks used by businesses, which became prevalent soon after the personal computer was developed. Operational Technology, on the other hand, describes the systems which monitor or control industrial equipment and processes. Both emerged in the same time period using similar underlying technologies, however they did so in relative isolation from each other. At times inventions on one side were adopted by the other – Ethernet is a good example of this, where it was widely adopted for the industrial environment following its success in the business environment.

During the early days of IT, interconnectivity of business systems and their connection to the internet was a necessity and as such security emerged as an IT priority. However, during the early days of OT, there was not an immediate need to interconnect industrial systems nor was there a need for internet connectivity. Because of this, whereas IT prioritized security, OT systems prioritized safety and availability – security in OT was an afterthought (and for some, still is).

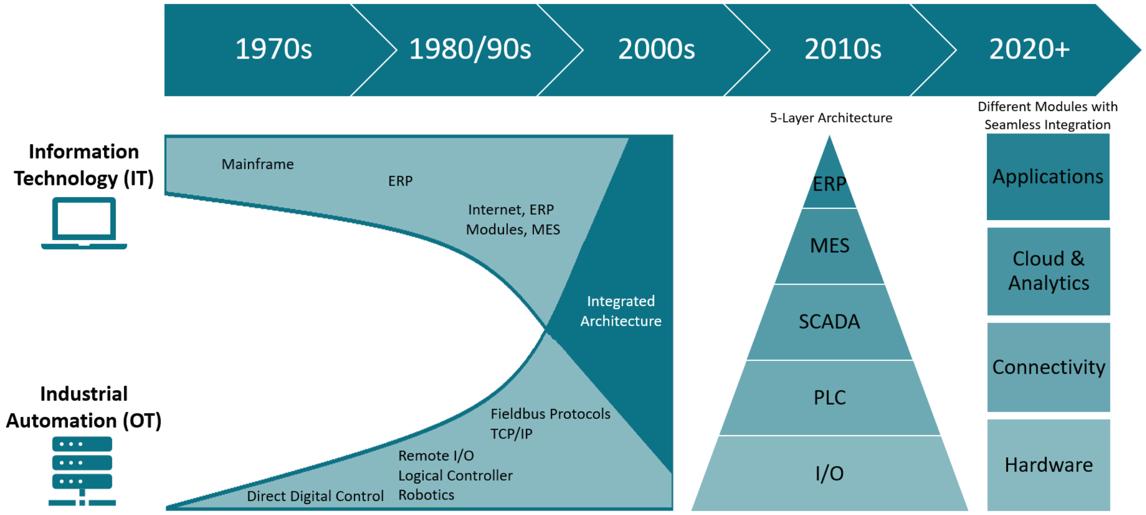


IT and OT Begin to Converge

However, over time, the financial and competitive value to an organization for interconnecting its OT systems and connecting them to the internet began to change the landscape. Cloud computing deployments and centralized virtual server infrastructures promised to (and do) deliver economies of scale and reduced operational cost. Smart manufacturing technologies such as MES and predictive analytics promised (and do) allow organizations to optimize and make business decisions based upon real-time conditions on the plant floor, which would give organizations that implemented them an edge over those that didn't. And so, organizations and solution providers began experimenting with the technologies available at the moment with the budgets that innovative companies were willing to invest to explore these goals.


1.
First Industrial Revolution: steam power makes mechanical production possible
(Late 18th century)
2.
Second Industrial Revolution: electric energy makes mass production possible
(Beginning of the 20th century)
3.
Third Industrial Revolution: IT and computer technology allow for more manufacturing automation
(Beginning of the 1970s)
4.
Fourth Industrial Revolution: Internet of Things makes networked manufacturing possible
(Since the 21st century)

Industrial systems began being connected together, routed to the internet and integrated into the business network. Tasks forces were set up to navigate an organization's "digital transformation" towards "the modern factory" under the pressures of existing through "the fourth industrial revolution." And thus the trend towards convergence of IT and OT (a.k.a. Industrial IT) and the pursuit of leveraging the Industrial Internet of Things had begun.


1970s
1980/90s
2000s
2010s
2020+
Information Technology (IT)
Industrial Automation (OT)
Mainframe
ERP
Internet, ERP Modules, MES
Integrated Architecture
Fieldbus Protocols TCP/IP
Remote I/O Logical Controller Robotics
Direct Digital Control
5-Layer Architecture
ERP
MES
SCADA
PLC
I/O
Different Modules with Seamless Integration
Applications
Cloud & Analytics
Connectivity
Hardware

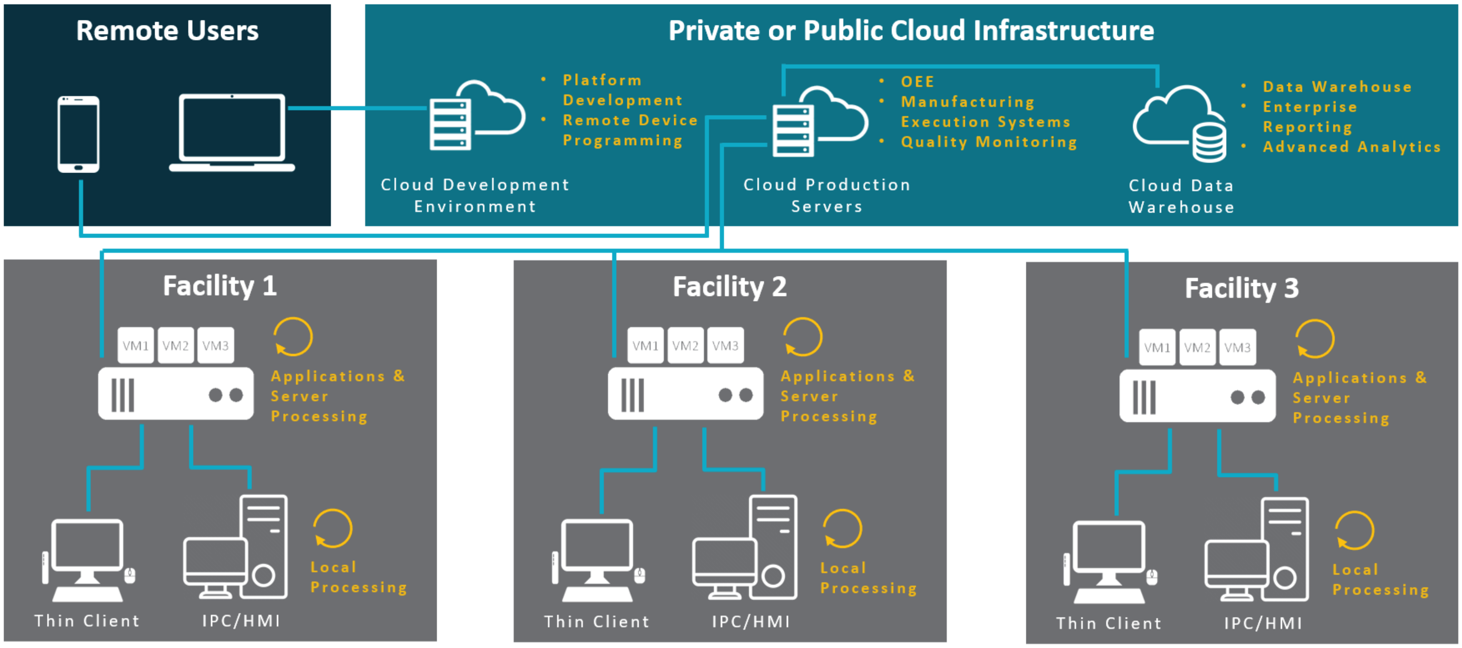
This history is critical to understand in order to explain why things are the way they are today, and to decipher where an organization should go next. Bread crumbs remain which still challenge us today – industrial communication protocols are inherently open and insecure, islands of networks remain which need to be re-networked into an enterprise-wise schema, and ownership of the Industrial IT infrastructure is not fully established. Even more significantly, the surge in connectivity cause cybersecurity risks to seriously threaten businesses' health, leading industrial control system (ICS) cybersecurity to boom into a multi-billion dollar industry decades after the underlying environment first emerged.

Looking back at the trends from decades of innovation and progress, there are certain truths that can be observed. Among them is that next-generation manufacturing technologies are not going away and they all require deep interconnectivity and security, so making investments in the underlying Industrial IT infrastructure is one of the best investments a long-term thinking organization can make.

Defining Industrial IT

Fundamentally, an organization's IT group develops and supports the underlying technical infrastructure for the business systems to operate – the company's intranet, office LANs, ISP connections and internal server stacks are examples. Industrial IT can be defined along similar lines in the OT environment. Industrial IT describes the underlying technical infrastructure in the OT environment, upon which industrial applications and systems run.

To clarify the delineation of this definition, the actual instruments and controller running a machine would not be considered a part of the plant's Industrial IT, but the networking infrastructure that the PLCs and HMIs communicate over, and the server infrastructure which the SCADA application is hosted on would be. As a second example, the application hosted on an HMI would not be considered a part of the plant's Industrial IT, however the HMI hardware itself and the operating system of the HMI would be. Further, for businesses operating multiple facilities the definition of Industrial IT may expand beyond systems within the four walls of a single facility – technical infrastructure such as cloud servers hosting industrial applications, cellular connections terminating at a point in the OT environment, and remote access systems would also be considered a part of the organization's Industrial IT.



The Components of Industrial IT

The overall Industrial IT infrastructure can be challenging for manufacturing facilities to plan, maintain, and understand, especially considering that in-house skills are often not available and the value of investing in the infrastructure may not be obvious to everyone. To better understand it, the Industrial IT environment can be broken down into three core components – Industrial Networking, Industrial Computing, and ICS Cybersecurity.

Computing

The servers and shop floor PCs running and providing access to industrial applications.

Cybersecurity

The organization's ICS security posture, points of risk, and standards alignment.

Networking

The physical and logical ICS network connecting the automation systems to business systems.

Complete Industrial IT Infrastructure

Gain a detailed understanding of the entire OT infrastructure supporting your industrial systems.

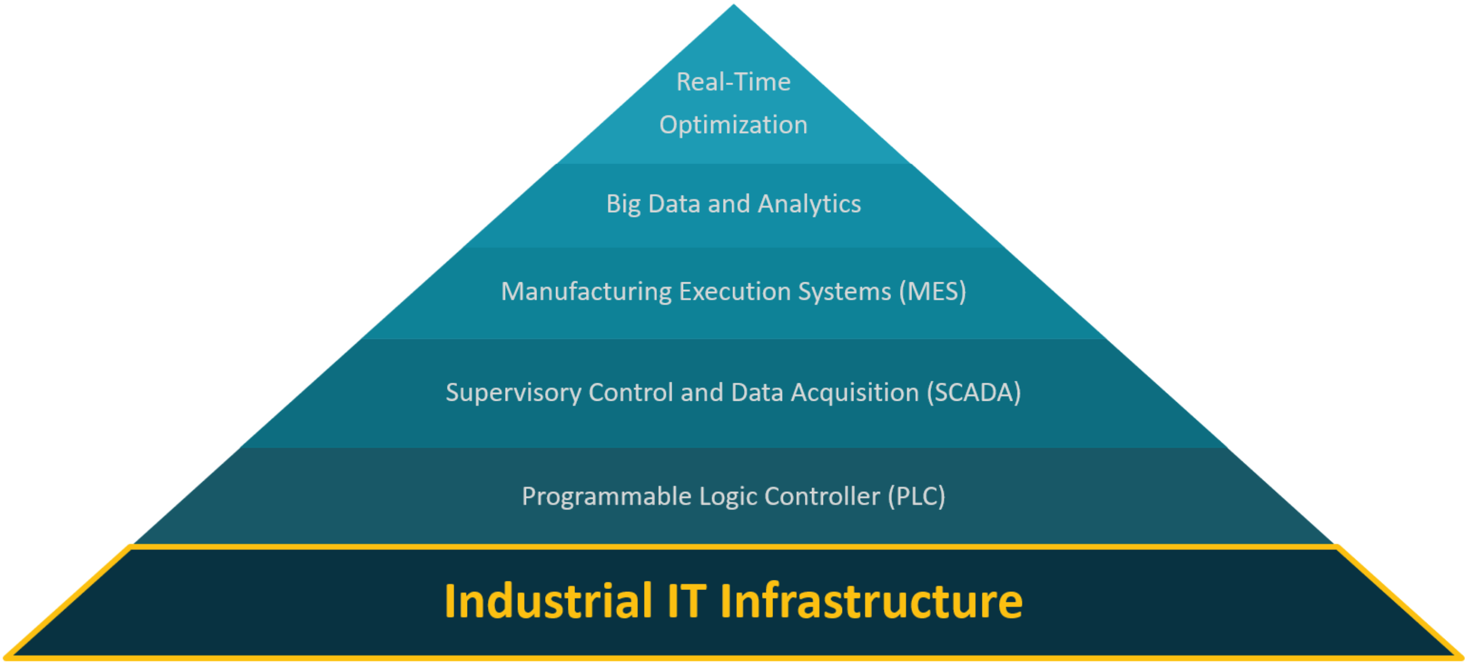
Manufacturers rarely think about their Industrial IT infrastructure in these terms. In fact, the infrastructure is often seen as a "means to an end" rather than an investment providing its own financial return, especially within organizations that have not yet started pursuing digitalization. However, whether it's recognized or not, complex collections of these infrastructure components exist in any manufacturer's facility, even for the most basic of manufacturing operations. Entire industries and solutions are built around solutions that fall within them, and organizations are reaping the benefits of (or suffering the pain caused by) the way they've assembled each.

Recognizing the Industrial IT "Layer"

Many, many organizations struggle with developing Industrial IT infrastructure which is stable, secure, and enables the pursuit smart manufacturing technologies. The primary commonly cited (and valid) reasons for this include:

- The ROI is difficult to calculate, and infrastructure costs are high in general
- The technologies and their benefits are not widely understood
- The skillsets to maintain the infrastructure are difficult to find

However, in addition to and perhaps transcending these challenges, is that organizations do not always recognize the infrastructure as it's own "layer" within their OT systems. Instead, many – especially those who are not technical – lump the infrastructure together with the control system as one. And by doing so, it makes it difficult or impossible for the organization as a whole to identify and invest in infrastructure upgrades.

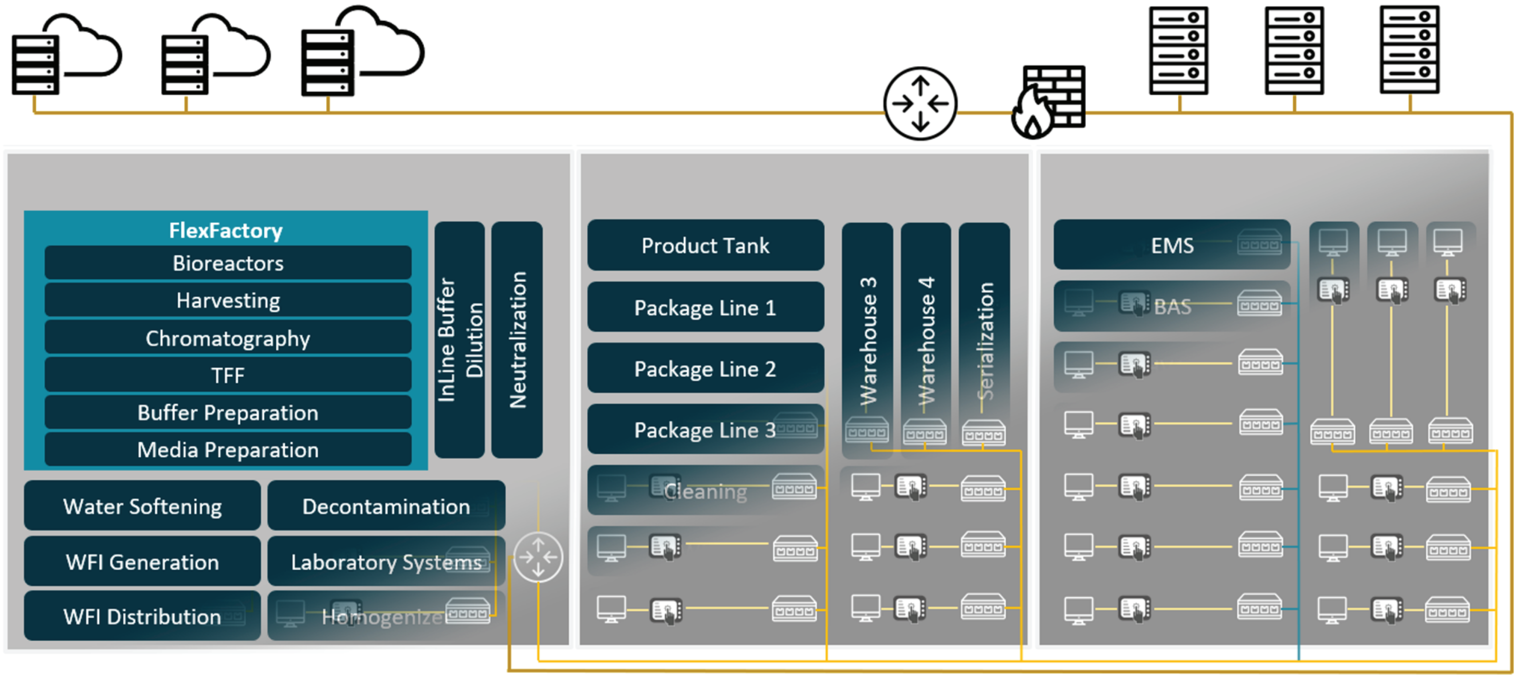

Real-Time Optimization
Big Data and Analytics
Manufacturing Execution Systems (MES)
Supervisory Control and Data Acquisition (SCADA)
Programmable Logic Controller (PLC)
Industrial IT Infrastructure

The most succinct way to demonstrate the detriment of that is by considering how control systems are purchased. When a machine or manufacturing system is procured, the vendor will deploy the system along with some networking hardware, touchscreen PCs, and perhaps servers to host the control system. Separately, a different system may be procured, which is deployed with different networking hardware, touchscreen PCs, and servers, and so on. Before long, the industrial IT within the facility is inconsistent, difficult to manage and difficult to integrate into one seamless architecture. In this way, vendors and solution providers are often contributing to the very problem they want to solve!

"...next-generation manufacturing technologies are not going away and they all require deep interconnectivity and security, so upgrades to the underlying Industrial IT infrastructure is one of the best investments a long-term thinking organization can make."

For this reason, acknowledging the infrastructure as its own separate layer is an important first step towards improving it. By doing so, infrastructure specifications and standards can be developed which can be included in RFPs to ensure consistency in what is provided by vendors. Consistent IP addressing and security features can be implemented. And rather than vendors providing physical servers, a centralized server infrastructure can be deployed which all vendors host their applications on.

When it comes to acknowledging the Industrial IT "layer", an important observation is that most organizations' IT departments already understand this deeply, and this challenge is one that is specific to the industrial environment and not the IT environment. IT departments can help resolve some of these issues by spearheading infrastructure requirement efforts for the industrial environment and being included in conversations at the earliest stages of the procurement process.



The Stages of Industrial IT Maturity

Organizations – especially those experiencing the evolution for the first time - tend to invest and build their Industrial IT infrastructure in a predictable way. However the predictable pattern isn't an optimal one – it is one which can be optimized by those following in the footsteps of other organizations and by doing so, the total cost required to achieve a mature Industrial IT environment can be reduced and within a shorter timeline.

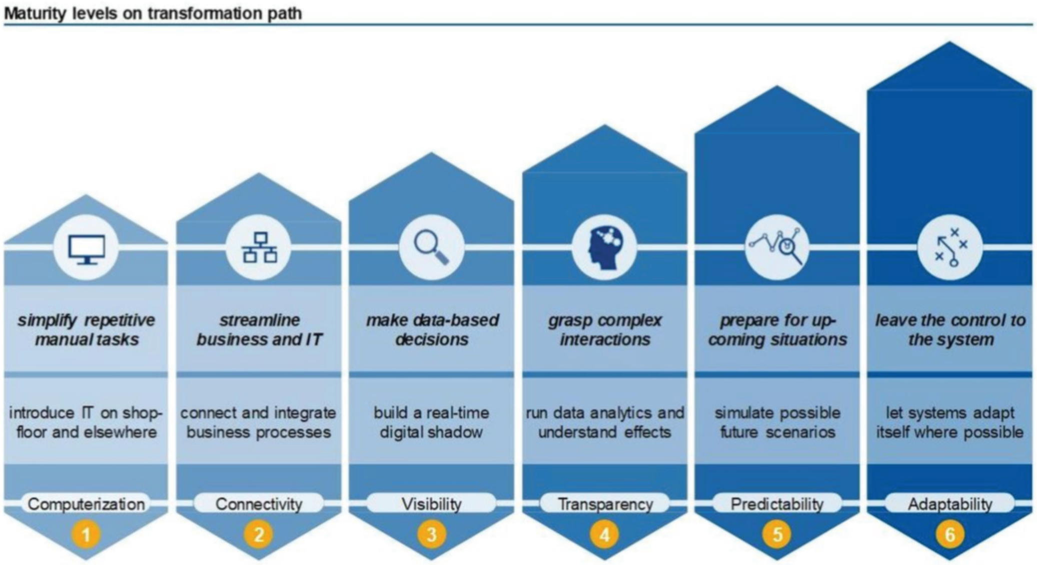
Stage 1 - Islands of Automation

When beginning the manufacturing digitalization journey, leaders are not yet familiar with the value of enhanced connectivity or, if they are, it's considered a problem that does not yet need to be addressed. In their minds, the priority is manufacturing to meet customer demand and reducing investment costs to keep operations lean. The output of this is installing OEM equipment and systems that operate independently and within their own networked environment.

This is cheaper to implement today but over time builds a fragmented and unconnected technology environment on the plant floor which is more costly to improve later. For example, when OEMs deliver new equipment on pre-set IP addresses, the new equipment might not be connected to the facility network at all. The devices and computing infrastructure applications run on are not standardized and security in the OT environment is not being managed. Ultimately machines will run and the plant will be able to produce, but remote connectivity and support is not possible and plant-wide monitoring and data historization is not feasible.

Further, it is not uncommon to see connectivity between systems being addressed in some locations, but not all locations., so the islands of automation are limited to certain areas or types of systems. For example, a facility may determine that process systems must be integrated into a plant-wide network, but material handling is less critical and can be left disconnected. In general, smart manufacturing technologies available benefit the supply chain from end to end and islands of automation cause operational inefficiencies, so it is common to see areas of a facility with less network maturity being "caught up" with the rest of the facility.

Acatech's research on their *Industrie 4.0 Maturity Index* indicated **80% of manufacturers** are in the "connectivity" stage of maturity.



simplify repetitive manual tasks	*streamline business and IT*	*make data-based decisions*	*grasp complex interactions*	*prepare for up-coming situations*	*leave the control to the system*
introduce IT on shop-floor and elsewhere	connect and integrate business processes	build a real-time digital shadow	run data analytics and understand effects	simulate possible future scenarios	let systems adapt itself where possible
Computerization	Connectivity	Visibility	Transparency	Predictability	Adaptability
1	2	3	4	5	6

Source: Acatech

Lesson Learned - Acknowledge the Industrial IT "Layer"

To be effective and efficient in growing the Industrial IT infrastructure, one must think about the infrastructure as its own system, which the control systems and application run on top of. The importance of this cannot be emphasized enough. Further, organizations must understand address all three major components of the Industrial IT infrastructure – networking, computing, and cybersecurity. Doing so as early as possible enables an organization to think about the infrastructure long-term and lay the groundwork to progress through the stages of maturity rapidly.

Lesson Learned - Create and Enforce Technical Standards

Forward-thinking executive leaders may understand that digital transformation is the future of their organization but have difficulty getting internal teams to make wise future-focused decisions. For example, despite the fact that ICS security must be prioritized in order to reach high levels of digital transformation maturity, project teams may continue to design and implement OT systems with poor security because it increases the cost of the project or poses operational inconveniences. Behaviors such as this will inflate the overall cost and increase the overall timeline of the organization's digital transformation journey because those systems will need to be upgraded or replaced at some point in the future. Countless organizations are struggling with this challenge today, but it can be avoided if the direction is set at the beginning.

Creating and enforcing technical standards early, and educating staff on their importance, is the ideal tool for combating this. They will require internal staff and vendors alike to adhere to technical requirements which will make integrating digital transformation technologies and managing security simpler in the future. Those technical standards also help combat the allure of low-cost providers who take shortcuts on important design considerations in order to reduce cost.

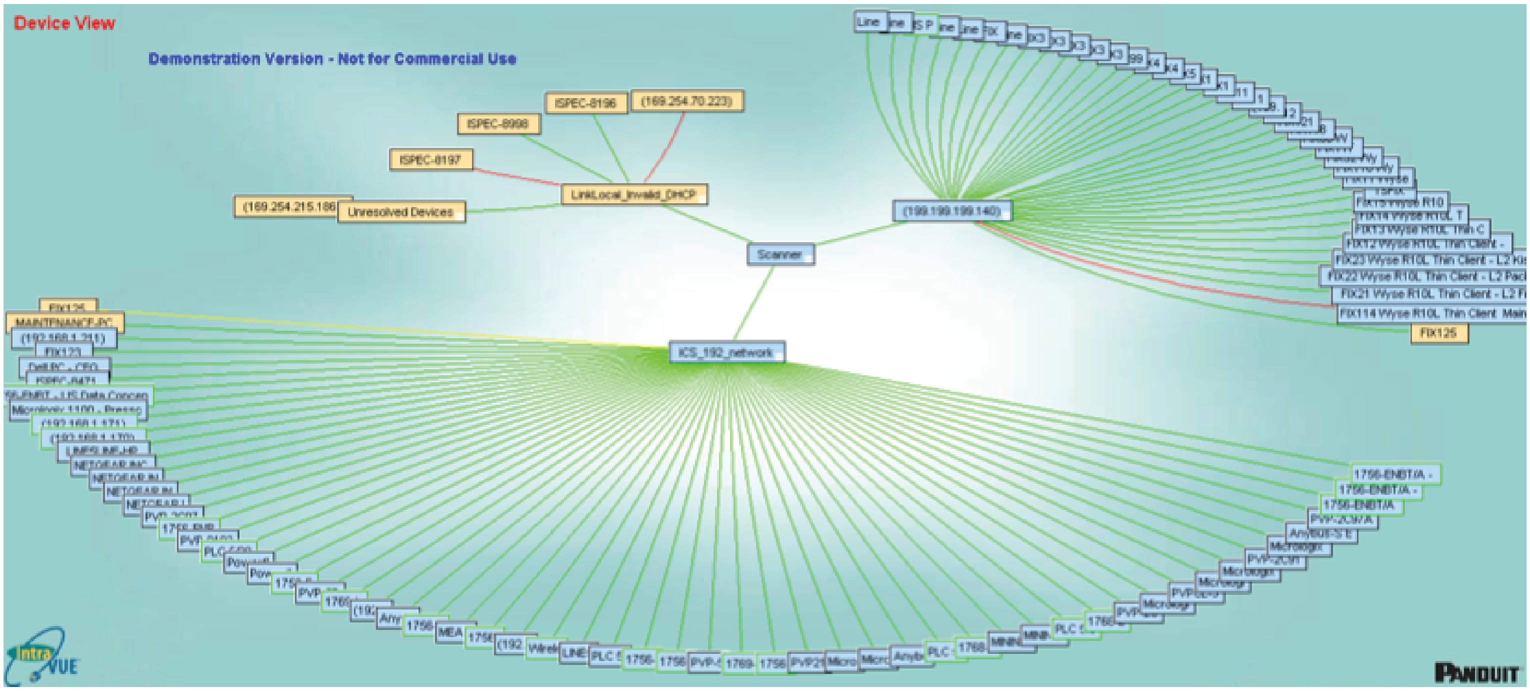
Lesson Learned - Establish a Plant-Wide Strategy

The total cost of correcting items later rather than addressing them during initial deployment and installation is almost always higher. To progress through the maturity stages as rapidly as possible, have a plant-wide connectivity plan established even if the organization is not yet ready to implement it. By doing so, the organization can ensure fewer existing systems need to be modified—or even replaced—to execute the plan. For example, the IP addresses which will be used for the industrial environment can be determined, and all purchased equipment can be provided from the factory with appropriate IP addresses set. When the time comes to interconnect the device, downtime and configuration updates to countless devices can be avoided, which is laborious and disruptive to do. As a second example, engineering can ensure that network switches are deployed where necessary as the facility's systems are being built out, so that the physical network infrastructure to establish a plant-wide network already exists.

Stage 2 - Flat, Connected Industrial Network

Eventually the operational pains of having islands of automation and the ways it restricts progress force the organization to re-engineer its industrial IT. In the absence of a higher-level plan, the operational staff make do with the resources and time available and change is made via “the path of least resistance.”

This manifests itself as low-cost, unconfigured switches being installed where physical space can be found and wherever an Ethernet connection is needed. Workstations meant for monitoring or controlling industrial systems may have internet connectivity to make staff’s day-to-day obligations simpler without thought towards security implications. When OEM equipment is purchased it is shipped to the owner with pre-configured IP addresses, so staff install a gateway to bridge the new equipment to the plant’s existing network. Or finally, to assist with on-demand troubleshooting needs, a cellular VPN router with low security is installed directly to the plant floor to allow remote service providers to troubleshoot equipment.



From a functional standpoint, a flat but connected Industrial IT architecture is an improvement from islands of automation. Basic remote connectivity can be put in place and higher-level implementations like plant-wide data collection and reporting is possible, however, the plant will face new key challenges with manageability and security. Because of the increased connectivity and complexity of systems, maintaining the network and computing infrastructure will become increasingly difficult, ultimately leading to lack of updates, hardware obsolescence and issues going uncorrected. Additionally, and perhaps a more sinister drawback is the security risk the facility is now exposed to.

The Industrial IT infrastructure is now connected, but security considerations such as computing infrastructure patching and network segmentation have not been considered. This leads to the greatest level of ICS security risk exposure to the organization compared to all other stages of maturity.

Lesson Learned - Prioritize ICS Security

It is common in the ICS environment to forgo security considerations since the risks of low ICS security are not understood by many and there is little incentive in making the investments outside of the business risk, especially in less regulated environments. However, for any manufacturing facility who has a connected ICS network, security improvements will be required.

At the earliest, an organization will start facing ICS security issues when their industrial networks are first connected plant-wide and connected to the IT network. Organizations are exposed to the greatest ICS cybersecurity risk when in this stage. At that point accidental data disclosures can occur due to employee mistakes or equipment can be lost from a ransomware attack. At the latest, an organization will be required to make ICS security investments – beyond network configurations alone – in order to pursue MES, cloud, and other systems leveraging data communications from the plant floor to the enterprise level and cloud. The difference between investing in ICS security early and investing late can be millions of dollars of lost revenue, equipment and brand reputation or even the loss of the company. Market data suggests that high percentages of businesses who suffer a significant cybersecurity incident are forced to close their doors, especially smaller businesses. Considering that deploying a high-quality industrial IT architecture early is already in a manufacturing organization's best interest, prioritizing security while doing so is best practice.

Lesson Learned - Cross-Train between IT and OT Teams

IT departments understand the importance of security deeply; it is baked into the foundation of the IT departments' purpose. The shortcuts which lead to poor security can be curtailed by providing training of IT's goals and challenges, and vice versa, and including IT in OT decisions, and vice versa. Developing an organizational culture where OT wants to work with IT to make infrastructure decisions which follow best practices doesn't just help avoid the pitfalls of a flat, unmanaged OT network; it sets the organization up for long-term success in manufacturing digitalization efforts. Achieving this starts with items like training and brainstorming discussions, and manifests itself by having IT included in engineering procurement and system specification discussions, as well as having OT at the table in remote access and change management decisions.

Lesson Learned - Provide OT the Resources to Execute

Sometimes individuals understand the importance of security and the role infrastructure plays in the overall operation, but do not have the resourced available to execute. Developing a roadmap to execute against takes time, knowledge and collaboration. Systems and projects which follow best practices and allow for long-term success can come at a premium cost. In addition to acknowledging and understanding why doing things in this way is important, OT teams must also have the budgets, internal skillset and support of their management teams to execute.

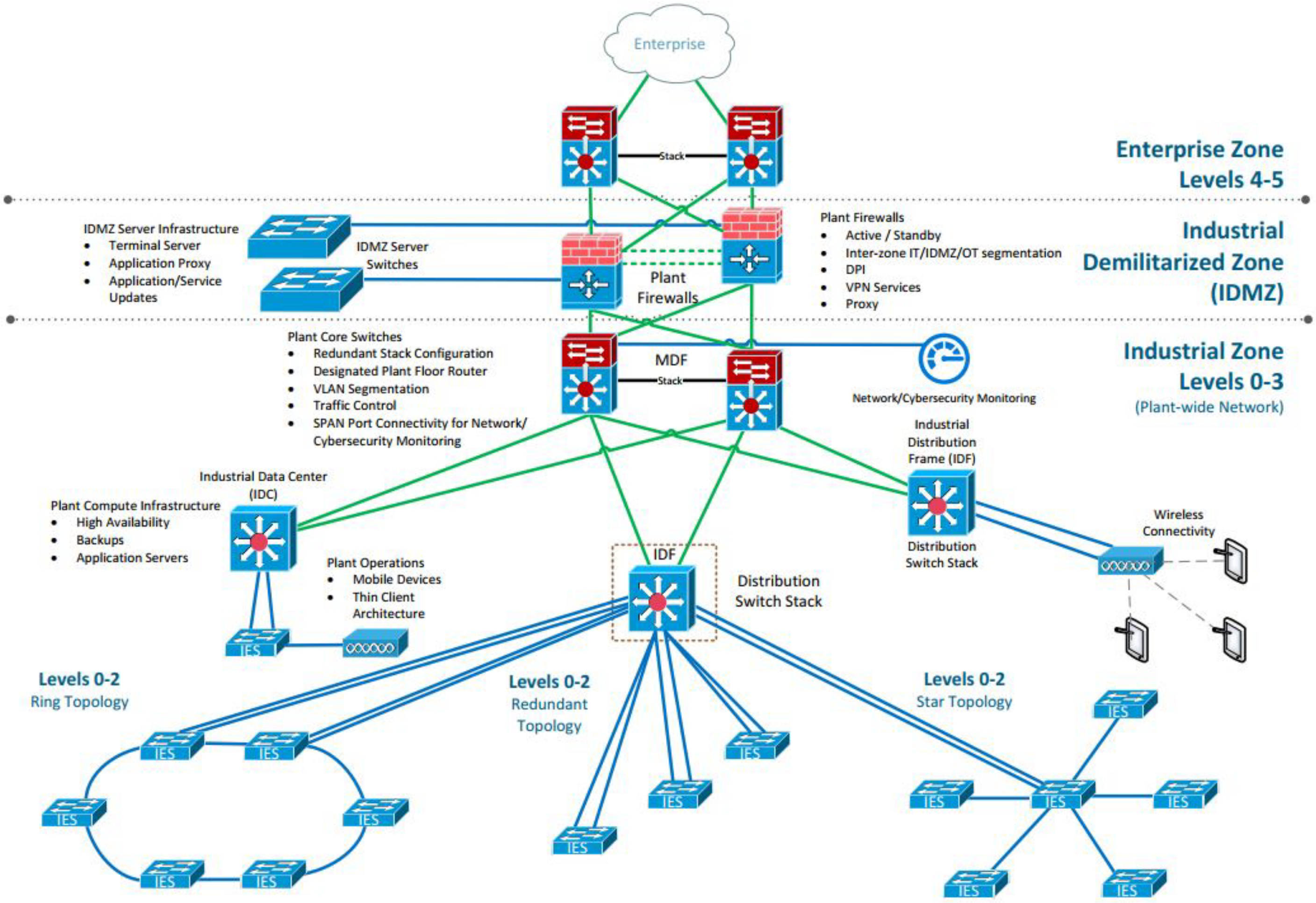
Stage 3 - Architected Infrastructure

Organizations operating with flat, connected industrial networks face pressure on several fronts to invest in Industrial IT improvements which can be summarized into three general categories.

- Organizations will start understanding the value in digital transformation technologies to remain competitive and may realize they must invest in their infrastructure to pursue those technologies.

- The operational inefficiencies, staff frustration and downtime attributed to the lack of standardization and management of their infrastructure may convince leaders to set aside funds for improving the infrastructure.

- A security incident (or multiple incidents) may force leadership's hands, requiring other initiatives to be paused in order to mitigate security risks.



However, regardless of which pressure tips the scale, most organizations will turn to validated architectures and industry best practices for further improving their connectivity and (finally) starting to prioritize security. Within their computing infrastructure, investments will be made in server virtualizations and standardized hardware. Organizations may also invest in thin client deployments and other remote connectivity solutions to centralize the way they host and access industrial applications across facilities. In terms of networking, VLANs may be implemented to segment the network and Industrial DMZs may be installed for management and IT-OT connectivity.

Lesson Learned - Consolidate Platforms and Architectures

For organizations working through deploying an architected infrastructure approach, a very common challenge is long-term ownership and maintenance of the infrastructure. For various legitimate reasons, the infrastructure maintenance may devolve into a break-fix approach or change control may be too relaxed resulting in deviations from the original intent over time. A way to make overcoming these challenges simpler is to consolidate on technologies across the entire enterprise as much as possible. Examples of platforms which may not always be consistent, but should be, include remote access platforms, access layer networking devices, and WLAN hardware. Establishing consistency across an enterprise can be challenging, so establishing infrastructure upgrades as corporate roll-outs and carefully selecting an ecosystem of implementation partners can be key.

Lesson Learned - Incorporate IEC-62443

IEC-62443 is a series of cybersecurity standards developed specifically for industrial control system environments and authored by both the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC). The series includes procedural, system and component requirements within the environment, and separate standards address the requirements which the owner must implement, the requirements which solution providers must meet, and the requirements which equipment manufacturers must meet. The best time to incorporate IEC-62443 would be from the very start, and the second best time may be when deploying architected infrastructure throughout the organization. Like many security standards, IEC-62443 lays out the specific security practices and requirements which are important to reduce risk (and those requirements are mapped to more traditional IT security standards such as the NIST Framework and ISO-27001. But, perhaps even more valuable to a medium to large enterprise, it provides a framework to ensure investment is applied where it is needed most and that facilities identify and implement security in the same way while giving individual facilities and solution providers room to operate within.

Lesson Learned - Re-Define Ownership and Roles

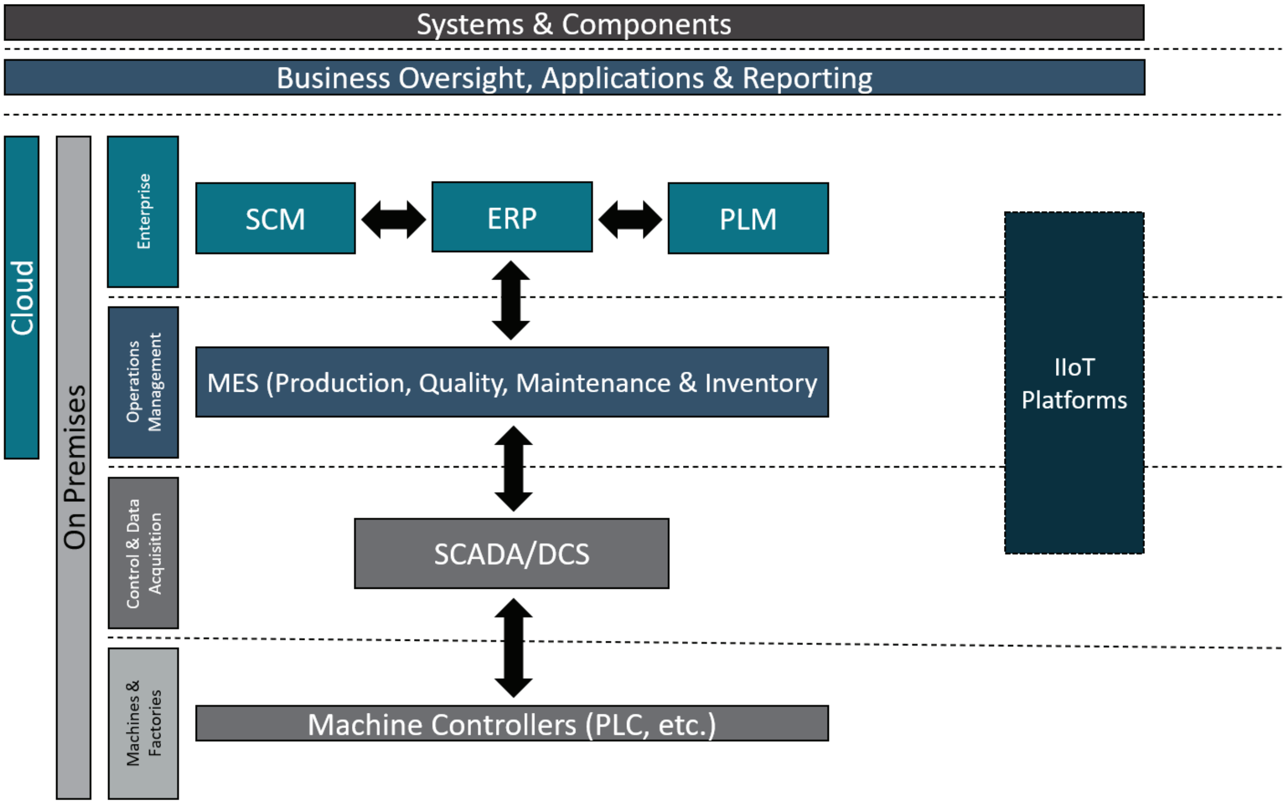
When an organization has an architected infrastructure deployed, the lines in the sand separating IT systems from OT systems, separating the infrastructure from the control systems which run upon it, and separating policy and procures which govern it all become blurred. A careful re-evaluation of how systems should be purchased, designed, reviewed, implemented and maintained in the OT environment should be done against existing department roles, corporate policy, operational procedures and even individual metrics. Examples of questions which should be asked include “should IT be involved in all OT system purchases, only ones which fit a certain criteria, or none?” A second example includes “What is each groups’ role in a OT cybersecurity incident, who has authority over the response and who has authority over internal and external communications?” Answers to questions such as these change during the Architected Infrastructure stage of maturity, and the appropriate answers for each organization may differ.

Stage 4 - Managed ICS Security & Cloud Technologies

Once an organization has an underlying Industrial IT infrastructure following best practices and standard architectures, they will be well-suited for implementing Industry 4.0 technologies and optimizing their operations. Plant floor data may be collected and analyzed to improve OEE or quality, and data may be uploaded to the organizations ERP in real time to improve business decision making such as managing supplies and product orders. The organization may also begin performing apples-to-apples reporting and comparisons of their facilities to identify where the largest improvements can be realized.

Many of these digital transformation pursuits – and others – will convince manufacturers to expand their computing and networking infrastructure even further to leverage the cloud, unlocking access to IIoT implementations and further improving the manageability of the infrastructure, reducing costs, and improving accessibility. Further, with operational data centrally organized the organization will have access to leverage big data analytics and AI engines, increasing their business competitiveness in ways competition may not be able to.

Industrial IoT Platforms in the Industrial Software Landscape


Systems & Components
Business Oversight, Applications & Reporting
Cloud
On Premises
Enterprise
Operations Management
Control & Data Acquisition
Machines & Factories
SCM
ERP
PLM
MES (Production, Quality, Maintenance & Inventory
SCADA/DCS
Machine Controllers (PLC, etc.)
IIoT Platforms

However, just as the organization experienced during its transition from having islands of automation to a connected industrial network, the ICS security risks increase as these infrastructure improvements are made. It will be identified that technical configurations alone – such as VLAN segmentation – are not sufficient for managing the cybersecurity risks, and that a continuous cybersecurity program akin to a safety program is required to manage the ongoing risk. An ICS security team will be established with KPIs and reporting to monitor progress, ICS security specific solutions will be deployed, programs for maintaining asset inventories and patching will be launched, and organizations will turn to ICS specific standards such as IEC-62443 for guidance on how to make investment decisions.

Lesson Learned - Prioritize Cloud Deployments

The tools required to take advantage of cloud hosting are available, and once the infrastructure is in place to support it a breadth of opportunities are at the organizations' disposal. Both off-the-shelf industrial systems hosted in the cloud are available, as are custom-developed industrial applications in the cloud. Remote access platforms purpose-built for the ICS environment with capability of hosting industrial programming software in the cloud can be implemented to improve access between personnel and software and devices, and migrating data into the cloud provides the opportunity to establish a single source of truth for decision making across the organization.

Prioritizing which migrations and cloud implementations will provide the organization with the greatest strategic or operational benefit is key. Cloud implementations provide the greatest value when utilized by the most facilities and personnel, and establishing wide-spread use across an enterprise takes time. So rather than making tactical cloud-system decisions, aim for getting the most bang-for-your-buck by prioritizing which investments would benefit the most facilities, people, and organization as a whole.

Lesson Learned - Simplify ICS Security Management

Organizations are at their highest level of risk when infrastructure is connected in a flat, un-architected way. But if security isn't managed, even after architecting the infrastructure the organizations' overall risk can increase again as greater connectivity, IIoT and cloud technologies are implemented. Continually managing and improving a security program is key to managing that risk.

To do this effectively, it is important to follow standards and leverage technology to simplify the process and ensure effectiveness. From a technical perspective, tools exist which can monitor the industrial environment, detect new devices and atypical behavior being introduced and develop a list of software and hardware vulnerabilities requiring patching. From a procedural perspective, a centralized security operations center or a centralized point of program evaluation and improvement can be established to ensure activities are producing results and - if they aren't - communication is occurring to course correct. An overarching principle to follow which can help produce results is to keep the balance between following best practices and keeping things simple to manage and execute against.

Conclusion and Take-Away

While this guide provides an insightful summary on how manufacturers typically progress through Industrial IT maturity, the greater value is in understanding the stages and the lessons to be learned, then leveraging that knowledge to improve your business' plans. Any organization who is traversing through their digital transformation journey – especially those in the early stages – have the opportunity of learning from the mistakes of those before them and making forward-thinking decisions to shorten the process. From that perspective, less matured organizations have a significant advantage. Organizations can plan ahead for the challenges of tomorrow and make investments now which will accelerate growth in the future and avoid decisions which ultimately limit the company's options later. In this way, organizations today can transform more rapidly and more cost effectively than ever before.

To get started, contact Grantek today at 866.936.9509 or info@grantek.com

GRANTEK

1.866.936.9509 www.grantek.com