How to Gain Operational Excellence Safely and Securely

1 Understanding the needs of your environment

In industrial environments today, security is a looming concern. The threat of intruders breaking into your operations—stealing your data, damaging your brand, even endangering your workers—is a risk that you have to address head-on.

But the right security strategy is one that's grounded in the actual context and concerns of your own environment. It's not enough to extend the security strategy that was developed for the IT side of your business over to the OT side of your business. The operational environment has its own crucial priorities.

What are these priorities?

Operational excellence is everything . . . plus safety, of course

For most industrial environments the pursuit of operational excellence is the driving force for investment both in terms of capital and operational expense. But it is not the only focal point—worker safety cannot be sacrificed. These two areas drive much of today's investments in industrial automation.

What's the difference between IT and OT?

In short, IT (informational technology) deals with information while OT (operational technology) deals with machines. IT manages the flow of digital information (read: data), while OT manages the operations of physical processes and the machinery used to carry them out.

Source: Coolfire

Manufacturing

In manufacturing, transformation initiatives such as Industrie 4.0 strive for measurable key performance indicators: improve the operational efficiency, reduce costs of operation, improve quality control, allow for faster innovation and manufacturing flexibility. All of these initiatives have multiple movements to meet the goal, but the most common investment is a modernization of the manufacturing environment.

What is industrie 4.0?

Industrie 4.0 is an initiative started in Germany to modernize manufacturing. The name reflects the 4th industrial revolution.

Manufacturing

Providing secure simplified connectivity

Business intelligence

Enabling real-time impact

- Analytics for improved OEE
- Improved innovation
- Reduced risk

Business agility

Much of the modernization effort will come with a better understanding of the manufacturing process. That requires data, and data capture requires better connectivity to the sources of manufacturing data.

IT has been connecting, capturing, and providing automated analysis of data for many years. If they can do this in the plant, then operational excellence can be measured and improved. Innovation can be implemented faster, and risk to product, productivity, and workers can be reduced with that knowledge.

But the operational environment is different than a typical IT space. Success will only happen when IT can partner with their OT (Operational Technology) peers in the factory.

Explore our workforce enablement solutions for manufacturing

Utilities

In utilities, top line revenues are not growing as they once did, and the pressures to drive down costs continue to rise.

But driving down costs requires investments as well, and while modernization is clearly the path forward, it does generate some risk. Macroeconomic and political forces are unavoidable—people want cheaper and cleaner—but without sacrificing reliability.

There are so many different opportunities to make improvements—across all stages in the generation, transport, and distribution of power. Utilities have to balance the advantages of modernization with the capital expenses that each new investment requires.

And each change means something new to a previously stable environment.

Utilities

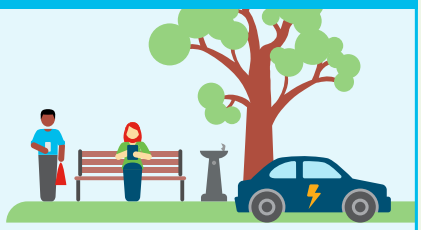
Declining revenues and business model evolution

- Funding model
- Operational cost reductions
- Unregulated opportunities

Aging infrastructure technology risk

- Grid modernization
- Increasing grid reliability
- Cybersecurity/risk
- Worker safety

Customer sentiment and expectations



- Mandates for renewables
- Clean power plan
- Prosumers
- Electric vehicles

Significant challenges associated with older industrial environments

We understand that there are challenges everywhere. Most industrial environments are well established and built at a time that did not consider the implications of a broadly connected system.

Some of those systems are rather old and built without much attention to security considerations. They were designed to maximize operational efficiency and resilience—not to anticipate, detect and remediate the types of threats we face today.

If you could just lock everything down, then you would reduce the exposure. But to compete today, businesses are moving in the opposite direction—bringing more and more of their operations online in order to improve understanding and predictability. The result is that we are rapidly connecting systems—and increasing risk by doing so.

So how do you address the continuous operational challenge while still securing the overall system?

Explore our workforce enablement solutions for utilities

2 A phased approach that keeps things running

We propose a phased approach for your security strategy, so as to reduce the chance of interruption.

The three phases

1 Secure connectivity and segmentation

Creating a network environment that ensures secured connectivity from top to bottom—where you control what can connect to the network plus who or what can connect to which systems

2 Visibility and control

Determining what systems are vulnerable and determining how to protect them against threats—while allowing you to continue to operate in a safe and efficient manner

3 Converged security and depth

Coordinating security policy across the multiple boundaries, and providing secure remote access that limits outside vendors' access to just the right piece of equipment—and only when actually necessary

But before we break down each of these phases, it's important to first address two critical prerequisites—understanding the technology stack and identifying organizational ownership.

Why Cisco?

The underlying security controls must do their jobs well. We have invested over $7 billion in a comprehensive, industry-leading portfolio of advanced security controls across the network, user/endpoint, and the cloud. It's backed by Cisco Talos, our threat intelligence and research group. And we will continue to invest in our security portfolio to ensure that each and every individual product solves the cybersecurity challenge that it's designed to solve—both today and in the future.

More reasons to choose Cisco

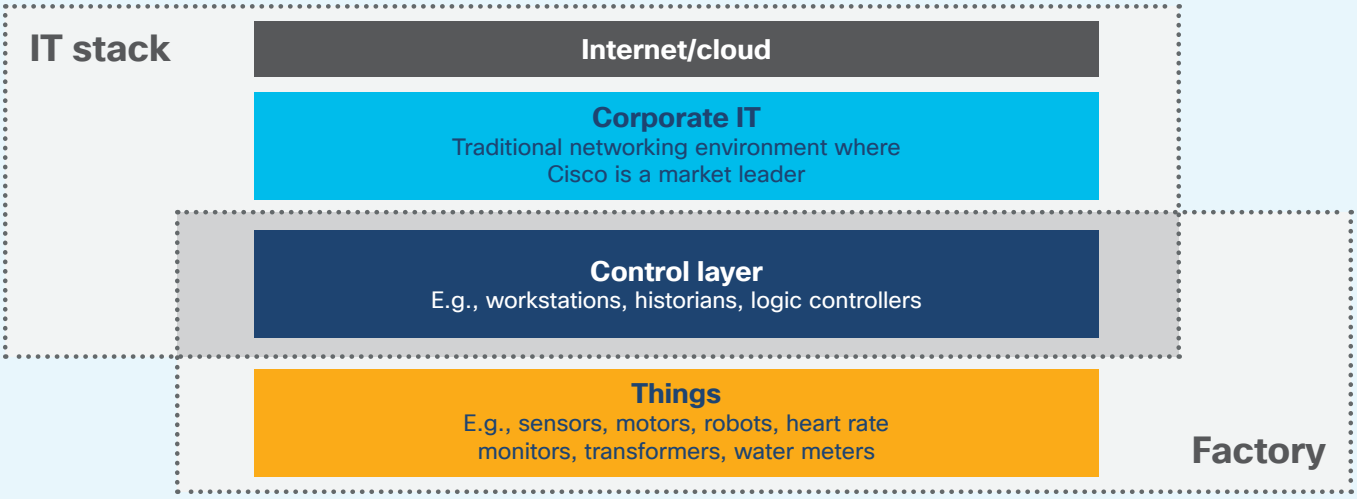
3 First, let's simplify the technology stack

What is a technology stack?

A tech stack is the set of technologies used to build and operate a web or mobile application, or more broadly, the set of technologies used to operate an organization.

Technology stacks have their own unique operating and security concerns. Before we get into the three phases, let's first understand these systems in a more simplistic view, one that focuses on the transitions of organizational ownership and technology stacks.

Manufacturing



Just as IT has been doing for a decade already, there is a growing push to utilize the cloud for deeper data analysis of operational telemetry with the goal to improve efficiency and machine availability. These are classic Cloud/IT technologies and well understood by IT.

Corporate IT remains what it always has been: that highly dynamic, highly connected space where we understand the business impacts of manufacturing success on the broader business.

The next two layers are in the factories themselves. The factory control layer is where the automation vendors have built windows-based control applications, historians, workstations and others, which instruct the "things" layer on the factory floor what to do—and evaluate how well they are doing it.

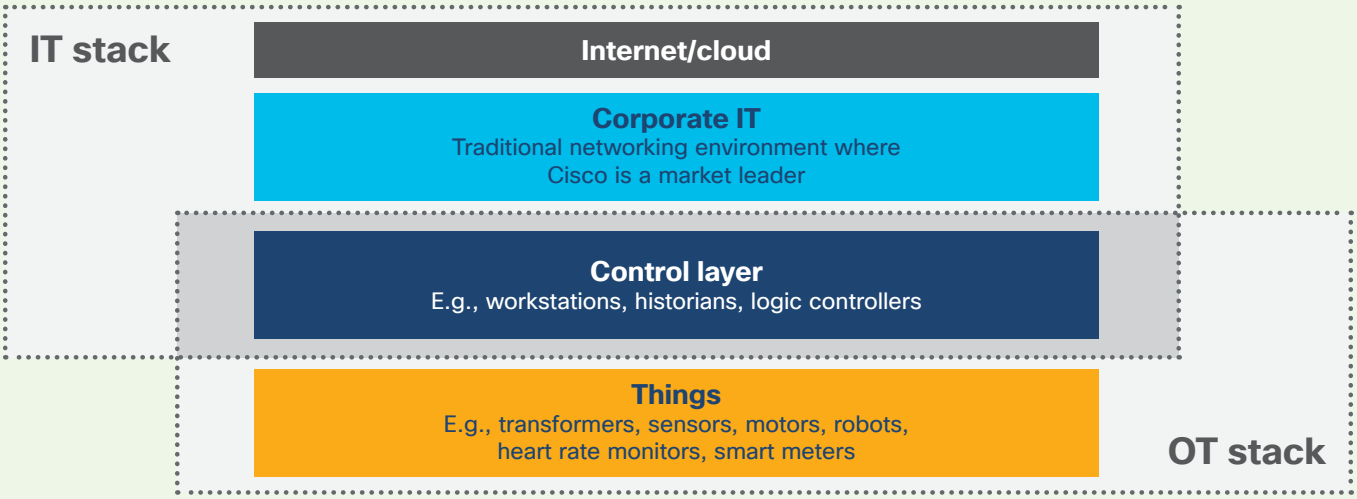
Finally, there are the "things" themselves—the machines, cells, or equipment that actually produce the goods the company sells. This is an area of highly specialized equipment and has sometimes

Manufacturing

unique networking and systems management needs and capabilities. This is the area where most traditional IT and security practices may not be applicable.

To summarize—we have different layers of technologies and responsible parties that must work together to create a modern manufacturing environment.

Utilities



While utilities have constraints on cloud use, there continues to be a growing push to utilize the cloud for deeper data analysis of operational telemetry with the goal to improve efficiency and system availability—especially for the generation side. These are classic Cloud/IT technologies and well understood by IT.

Corporate IT remains what it always has been: that highly dynamic, highly connected space where we understand the business impacts of manufacturing success on the broader business.

The next two layers are in the operational space. The control layer—which covers both generation and distribution—is where the automation vendors have built windows-based control applications, historians, work stations and others, which instruct the "things" layer on what to do—and evaluate how well they are doing it.

Finally, there are the "things" themselves—burners, turbines, breakers, transformers, capacitance systems—that actually produce and deliver the electricity. This is an area of highly specialized equipment and has sometimes unique networking and systems management needs and capabilities. This is the area where most traditional IT and security practices may not be applicable.

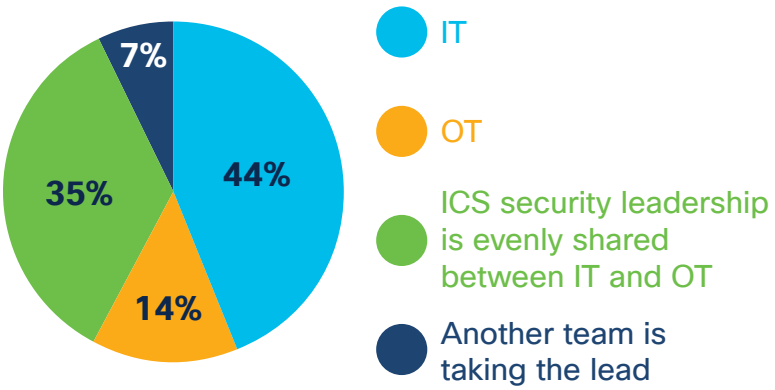
To summarize—we have different layers of technologies and responsible parties that must work together to create a modern utility.

4 First decision: Who owns industrial security?

People and organizations are key elements to successful security

Security is a function of people, process, and tools—with people being the first and most critical element. In the area of industrial systems, there is an evolving and critical question regarding ownership and responsibilities.

What organization is taking the lead on industrial security?



According to the 2019 ICS Security Report Survey from Dimensional Research, we can see that of the organizations that have both IT and OT teams, IT seems to be taking the lead on ICS security responsibility.

So, before you consider the first phase, you must first initiate a conversation regarding who owns what: capital budget, operations budget, who specifies the practices, who makes it happen. These are all key areas to investigate.

> "Do not underestimate that your biggest challenge with integrating [will be] changing the mindset of both IT/OT to think like each other and leverage each other's expertise."
>
> —SANS 2019 OT/ICS Cybersecurity Survey

5 First phase: Secure connectivity and segmentation

The first area of focus is segmentation—having secured connectivity from top to bottom. At the top, ensure that you have a dedicated Industrial DMZ, as with the primary enforcement point being a FirePower Next Generation Firewall (NGFW). Below that, we would like to create a resilient, defensible network infrastructure.

For manufacturing environments . . . Our Industrial Ethernet switch infrastructure would be optimal for the lower levels of your factory.

For utility environments . . . Our Industrial routers, switches, and wireless infrastructure would be optimal for the lower levels of your generation or distribution system.

Segment in stages to avoid interrupting operations

Like all projects, you need to have a starting point, a process, and hopefully a finish.

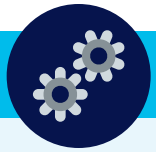
For segmentation it is the same. In this case we first look to the most critical boundary—the operational network and business network or internet interconnect, and ensure that we have a strong demilitarized zone (DMZ) boundary between them.

After that we need to discover and prioritize the componentry at their respective boundaries.

What's an intranet demilitarized zone (IDMZ)?

Sometimes referred to as a perimeter network, the IDMZ is a buffer that enforces data security policies between a trusted network (industrial zone) and an untrusted network (enterprise zone). The IDMZ is an additional layer of defense-in-depth to securely share IACS data and network services between the industrial and enterprise zones. The demilitarized zone concept is commonplace in traditional IT networks, but is still in early adoption for IACS applications.

Source: Rockwell Automation



Manufacturing

This might mean identifying production lines, individual cells or machines for your different sites, and it could mean delving deeper to identify components within each machine.

Utilities

This might mean identifying a clear ESP (Electronic Security Perimeter) for your different sites, and it could mean delving deeper to identify components within each bay.

In either case you will need to find out what is out there and do so at scale.

This is not just a task for tools—operators will have to get involved to ensure that what is visible to the network aligns with the functions we need to segregate. But this is not just about assets—the ability to detect the interactions between assets means protocol and application understanding. Again, tool and people will be at play.

Finally, we take steps to perform the segmentation. At this point we take what was discovered and align it with a resilient and defensible network design. And of course, we fulfill that network design with modern network equipment and application aware control points. With proper visibility, design, and equipment, you can protect diverse assets from potential spillover effects while improving resiliency and defensibility.

6 Second phase: Visibility and control

The next step is to be able to protect against threats and application misuse, while ensuring that the systems run as intended without network-born manipulation or interference.

Sometimes the problem is that unintended changes have impacted operations, or old equipment has started to flood the network with problematic traffic. For the control level applications, Advanced Malware Protection (AMP) is the optimal end-point solution. Next Generation Firewalls (NGFWs) at the different levels help to stop any outbreaks from spreading as well.

We provide threat protection for vulnerable systems

Nobody has discovered as many OT system vulnerabilities or delivered anywhere close to as many protections as Cisco's Talos. For the past several years we have delivered at least 100+ vulnerability discoveries and protections annually. No other company has matched our dedicated industrial security researchers in terms of creating protections and mitigations for known industrial threats.

New protections delivered in 2019:

In some cases, we can deliver a zero-day protection whose details are known only to the vendor whose product is vulnerable and those customers whom they alert. What this means is that in the real world where updates are difficult to schedule in a timely fashion, these customers can be protected without having to take critical assets off-line.

We provide a deep understanding of industrial protocols to ensure a safe operating environment.

Cisco's NGFW firewalls have the ability to parse industrial protocols and understand the components of the control language. Special protocol parsers actually understand the structure of the protocol and provide graphic user interfaces (GUIs) for easy and rapid modifications without having to learn and debug obscure regular expression constructs.

Manufacturing

With these functions, you can help prevent errors from impacting your operation and even detect undesired manipulation of the machines and cells on the factory floor.

Utilities

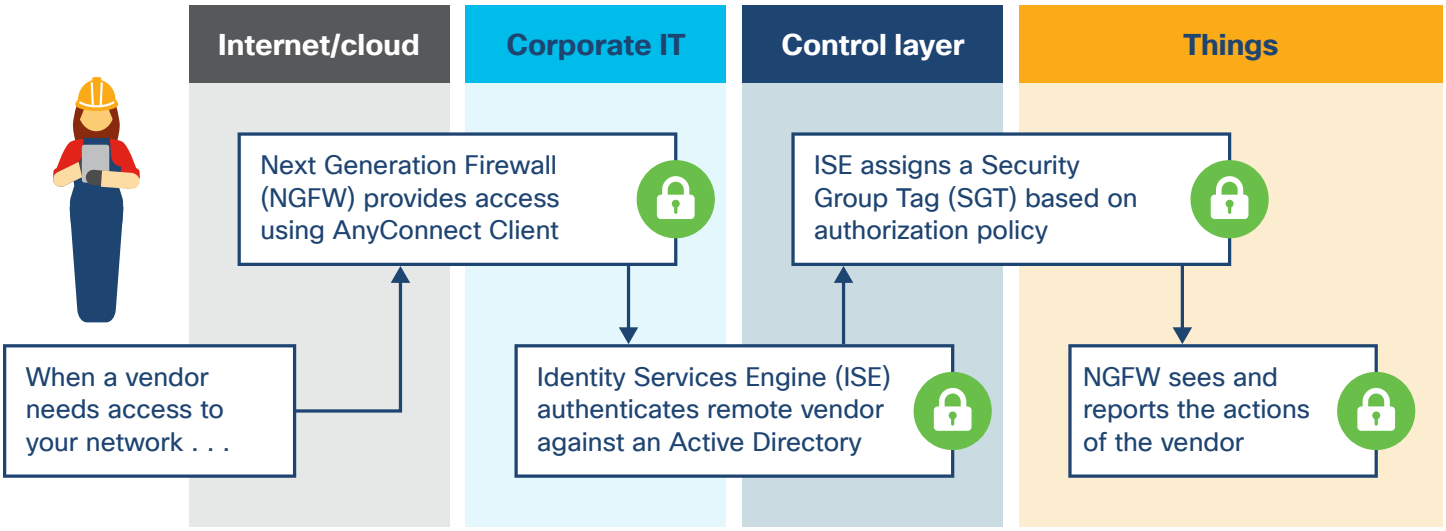
With these functions, you can help prevent errors from impacting your operation and even detect undesired set point values pushed to the equipment in Bay 1 at a remote unmanned site.

7 Third phase: Converged security and depth

The final stage is to coordinate security policy across the boundaries between IT and OT. With the long-term goal being to optimize processes, that means a greater flow of data upward. To achieve that and other major use cases, we will need to build strong foundations and reduce the fiefdoms of security policy.

Finally, there is the very challenging problem of ensuring that outside vendors have access to only the right piece of equipment—and only when actually necessary. Whether outside techs are reaching in from afar, or walking into the plant and plugging their laptops in, you need to be able to control what they have access to.

Our end-to-end security story helps address the complex challenge of external vendor access.



The reliance on partners to help maintain your operations represents a complex security challenge. You need their help, but they do represent a potential threat to your operation's security.

There are a lot of questions at play. How can we know the security state of the partner's equipment when they dial in? How do we dynamically establish a path across our business network all the way to the only piece of equipment they need to touch? And if we are dealing with a robot or dangerous device in proximity to humans, then we have to be able to provide a "line of sight" for the remote tech to know what is happening.

Naturally we are crossing multiple organizational boundaries. Just within your own company how do you coordinate access across those boundaries? Then there is the question of what is that technician doing with that equipment? Is there any means to know or control that only the actions that were agreed to are going to happen? Could you do anything if it is not?

Finally—how do you control the vendor's security state, access, and actions when they walk onto the plant floor? With an end-to-end solution like Cisco's, you have a chance. And when you progress through your security evolution, you can work from a proper base to make these things happen.

8 Next steps

We can help

Cisco has a complete end-to-end view to connect and protect modern industrial systems.

A key value Cisco provides is that we connect and protect across all of these technology stacks—from the sensor on the plant floor to your automation vendor's equipment analysis tools in the cloud. Nobody else can provide end-to-end connectivity and security like Cisco.

We protect cloud assets with Umbrella, and safely connect outside workers and vendors into your corporate networks via AnyConnect. We connect and prioritize traffic into and across your business network with tools like Identity Services Engine (ISE) and FirePower.

We secure your factory connections to the business and outside world via FirePower enforcement at the IDMZ.

At the control layer, those windows platforms running your operations are protected directly or have vulnerabilities mitigated by Advanced Malware Protection and FirePower.

Finally, we help segment the diverse portions of your factory through ISE, Stealthwatch, Cyber Vision, Industrial Network Director, our Industrial Ethernet switching, Industrial FireWalls, and TrustSec.

No matter where you are in these technology stacks, we have the means of security it.

Explore our solutions for manufacturing

Explore our solutions for utilities