Cyber Security considerations for manufacturing plants and industries

A practical approach to cyber protection of Operational Technology in processes

By Patrik Boo
Cyber Security Manager
Process Automation, ABB, USA

Executive Summary

OT, or Operational Technology controlling industrial processes, is becoming more connected to outside cloud services. This enables new powers and capability in managing industrial automation control systems, but at the same time has the risk of making them more vulnerable to cyber attacks. Deciding how to get access to these benefits while protecting your operations can be confusing.

Based on our deep experience with both cyber security and industrial process automation systems, the most important advice we can give is:
Do something rather than nothing.

There is no reason to miss out on the benefits of new digital services and what these solutions can provide simply because you are afraid of connecting your production systems to your company network and allowing traffic to and from the internet. Applying cyber security to industrial systems isn't that complicated; there are many companies that can help, and it is often more economical to outsource it. Finally, not addressing cyber security is a huge risk that is unlikely to pay off.

Here we present a stepwise and practical way in which you can take the necessary steps to implement cyber security in your processes and operations, while taking advantage of the many benefits that modern handling of big data offers.

Table of contents

Introduction

There are gains to be made in the industrial sector

In today's information era, connected devices have empowered us with knowledge, analysis, and decision-making capabilities that were unimaginable only a few years ago.

A simple example is configuring your smartphone or smart home device to set your morning routine to get the highest efficiency. The morning alarm is set, based on several factors like your first scheduled meeting, your average time to get showered and dressed, and a real-time estimate of drive time to the office. Your smart device will also inform you of the day's weather so you can quickly pick an appropriate outfit, while simultaneously brewing your morning cup of coffee and reading the major news of the day to you.

About five minutes before you need to leave, your smart device will start your car and make sure the interior is warm or cold depending on the time of year. In the event that you use a ride-sharing platform to get to work, it will even schedule a ride to ensure you arrive at the office on time for that first meeting. All of these steps optimize your time and resource efficiency, combining to result in the highest output without stressing you.

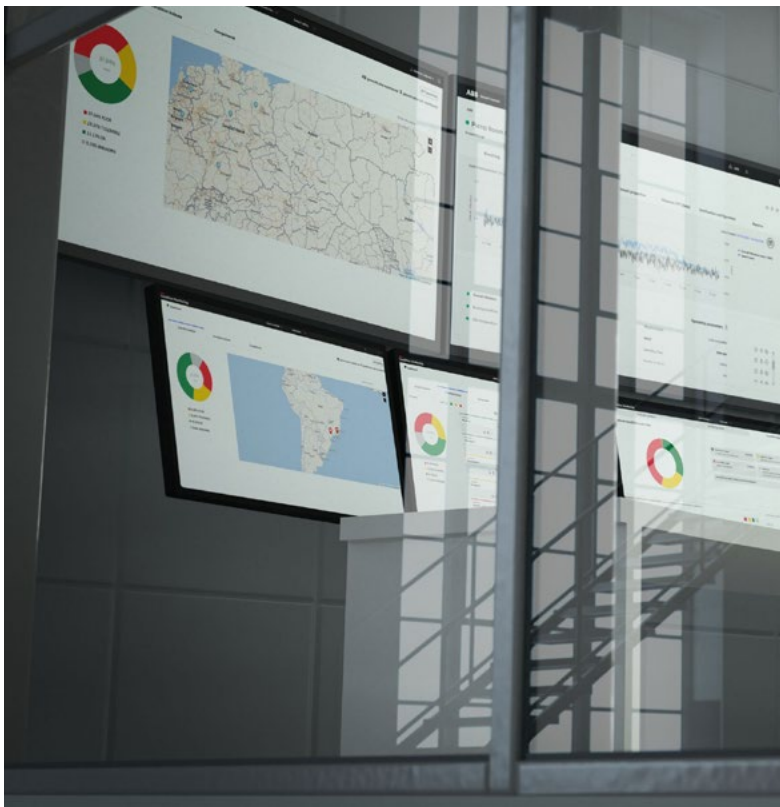
Parallel efficiency gains in industrial production
The natural question now is: Can we harvest similar efficiency improvements, and unprecedented financial gains, in today's industrial production systems by using related technology?

The answer is: Yes, digitalization and cyber principles can enable this. And it's really nothing new since we have learned much from IT, and now OT, the operational technology running industry, is going through a similar massive technology transformation. You have most certainly already heard and read quite a bit about numerous variations on this theme.

Like many developing ideas, this transformation is referred to by several different names. Among them are IIoT (Industrial Internet of Things), Industry 4.0, and ABB Ability™.
All are similar in their basic outlines yet slightly different in the details; some refer to an overall concept (e.g. Industry 4.0) and others to a specific company's implementation strategy for the concept (e.g. ABB Ability™).

No matter what name is used, the important point is that advances in technology and communication now mean you can leverage these new tools to significantly increase your industrial efficiency and productivity.

As simple examples imagine the overall financial benefits that would be achieved if you could free up capital by anticipating what the market needs and then producing exactly and only what is needed. Or being able to reduce your raw material and production costs by 10% with just small efficiency adjustments in the process. Or increase your total production output by 10% without making any additional capital investments.



All of these gains are possible through the use of advanced data analytics, which can be accomplished by integration of industrial manufacturing processes with modern digital services and solutions.

The weak link that can't be ignored
There is, however, one weak link in the chain that we must address as we move in this direction.

To reap the benefits that may come from advanced data analytics, automated processes, and even automated decision making we must first connect our previously disconnected systems. To get data to and from on-premises and cloud networks we must create connections that, unfortunately, expose vulnerabilities that attackers could exploit.

A successful attack would likely wipe out any financial gain from implementing digital solutions – not to mention the possible damage to the organization's image and trustworthiness, and even harm or injury to assets or personnel.

Much like the common saying, "a chain is only as strong as its weakest link", to capture the full potential of the digital transformation chain, the cyber security link cannot be the weakest one.

Trust and teamwork are absolutely essential
In the past, and in some cases even today, the IT team and OT team within the same company may have had less than perfect collaboration. This is commonly due to mistrust between the two sides. The OT team worries that the IT team will wreak havoc on the OT systems and doesn't understand what it means to be responsible for industrial production. The IT team has similar mistrust about the OT team's experience and skill when it comes to protecting what they consider typical IT systems that they have protected for decades.

There are numerous stories about how IT, with good intention, has applied a security measure on the OT system and shut production down. The most common culprits are variations of scanners and computer information collection tools. These tools were never developed for or tested on DCS systems, and the teams responsible for the DCS never considered that they would be used on their systems.

On the bright side, there are also many stories where IT and OT decided to work together and manage to implement strong security without affecting production. These collaborations also often resulted in lower overall costs.

Animosity between these two teams is undoubtedly not in the best interests of the company. To achieve positive and lasting results, these two teams must work together and learn from each other. Not easy perhaps, but certainly not impossible.

What is OT cyber security, and how does it differ from IT cyber security?

OT stands for the Operational Technology used in industrial production, and one can argue that OT cyber security is essentially the same as Information Technology (IT) cyber security, since they are both mostly based upon the same technology. The main differences are:

1. **Where the technology is applied, an industrial system (OT) or a business system (IT).**
   An industrial system must never be stopped outside a planned outage period, meaning the availability of the system can in no way be jeopardized. An operator never wants to see a warning saying their workstation will automatically restart in 30 minutes to apply security updates. OT cyber security solutions need to be configured to work with your production schedule whilst maintaining optimal security.
   An even more fundamental difference is that IT systems control relatively modern software running on standard hardware, while OT systems manipulate physical devices often controlled by a mix of new and old technology.

2. **How cyber security is implemented**
   Even though the tools and methodologies used are often the same for OT and IT, there are critical differences in applying them. Applying common IT cyber security solutions to OT systems without making further considerations or adjustments will likely, at some point, lead to operational problems.
   One common security practice from the IT world that won't work well in OT is the very sensible protective action of locking a user's account if the password is wrongly entered too many times. If we take the same approach in OT, we may end up with an operator that is locked out of the industrial production system, unable to control the process, or perhaps prevent a catastrophe, merely because the password was mistyped a few times.

3. **How long the equipment is expected to stay in operation**
   An IT device such as a laptop is easily replaced every 3-5 years, while components in a DCS system stay in operation considerably longer. Modern cyber security controls can be applied on the laptop without much consideration because it is relatively new and seldom reliant on, or supporting, other devices. A DCS system is, however, made up of dozens of different devices that must function together. Applying cyber security on a modern server within the DCS system may negatively affect other system functions that can't handle the new security feature – simply because they are based on older technology.

Noteworthy industrial cyber security events

Let's look at a few examples. Even if some of them are a bit old now, they have been selected because of the differences in how the attack was orchestrated and because information about them is readily available online.

Merck
The pharmaceutical company Merck was subjected to a Ransomware attack in 2017. The malware got into over 30,000 computers and 7,500 servers. Years of research were lost, and normal operations were seriously affected. It is unknown what the financial impact to Merck was, but the company ultimately sued its insurance providers, claiming $1.3 billion[1] in losses.

Ukrainian Power
In 2015, a Ukrainian power producer was attacked by a team of hackers, likely a Nation-State. The attack led to over 225,000 customers[2] losing power for 6 hours. The attackers used multiple strategies and methods to access the system and shut down power production. The key factor is that the attackers had ample time to understand the system, embed themselves, and then wait for the right moment to strike.

Natanz enrichment facility
This case, commonly known as Stuxnet[3], is one of the most famous cyber attacks ever in the industrial sector, both due to its sophistication and its impact. It was one of the first malware files designed to attack an industrial system. The virus got into the facility and changed the running code in the SCADA system that controlled the centrifuges used to enrich uranium, with the intent of making them operate in a way that would lead to failures. As this occurred at a classified nuclear facility in Iran, the exact impact of the attack is unknown. One can only speculate about the extent of damage that could be inflicted in handling radioactive materials.

What, if anything, could have been done to prevent, or lessen, the impact of these attacks? The following sections of this paper will systematically break down good measures that one can apply to increase an industrial automation control system's cyber resiliency. At the end, we will revisit the three examples to see if cyber security would have made the impact less disastrous.

—
01 https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
—
02 https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01
—
03 https://en.wikipedia.org/wiki/Stuxnet

Don’t panic
Start with an assessment instead

— 04 IBM’s latest X-Force Threat Intelligence Index found that attacks on industrial and manufacturing facilities have increased by over 2,000% since 2018.

Because many OT systems were deployed well before cyber security for OT systems was considered to be needed, hackers often find it easier to hack these systems than IT systems – using experience gained from IT system hacking. Because IT and OT are converging, and industrial systems are leveraging commercial IT devices and solutions, we see an ever-increasing number of cyber attacks on industrial systems.[4]

Even though the frequency of cyber attacks on industrial systems is increasing and we have seen examples of how bad the financial, reputational, and environmental impacts can be due to successful cyber attacks, it’s far from time to give up and put our heads in the sand. Implementing cyber security in OT systems is not much different than any other project or initiative you may undertake.

Start with a candid assessment to get an understanding of the overall scope of your cyber security needs. This is most easily done by answering these questions: What are you protecting? How is the system architected and does that architecture support strong cyber security? What assets do you have in the system? And what is the weakest link in the chain?

If you don’t know all these things, it is difficult to know where to start or how to evaluate whether the resources being used for protective tasks will truly bring the most significant improvement in cyber security defense.

The steps in an effective assessment might look like this:

1. Start by listing all the cyber assets in the system. Cyber assets include any device connected to the industrial network which is used by the DCS system. Most commonly, devices are connected to a network using an Ethernet connection, but don’t forget about other communication links between devices in the overall system since these may also be used in an attack. For instance, a Modbus connection can be leveraged to send false data to the system to initiate a failure or to mask an ongoing attack.
   Creating this inventory list is hard work, but there are tools and solutions that one can use to reduce the manual effort. Just remember to only use DCS vendor-validated tools and solutions to limit the risk of problems.

2. The next step is to update the system network drawings and place all the devices in a diagram. This is a critical step as it shows how the devices are connected and how they interact and communicate with each other. Make sure to include as much detail as possible since a good network drawing serves multiple purposes, not all cyber related. Other types of drawings worth considering are overview, conduits and zones, physical network, VLAN, and data flow drawings. If this is done manually, make sure to have a documented process on how to update these regularly.

3. Lastly, one must perform a risk assessment. This assessment will identify and help prioritize the parts of the system that can cause the most harm, either financially or concerning health and safety, if they are attacked. The risk assessment process forces you to focus on each device and function to answer two critical questions: How likely is it that this thing may be subject to a cyber incident? And what is the impact of that incident as far as scale and consequences? These two components, the likelihood and the impact, are what make up the total risk, and a good risk assessment will provide guidance on how to best prioritize your resources and budget.

Worth the effort

Although the process previously outlined requires a fair level of effort, it is incredibly worthwhile. When done, you will at that point have an excellent picture of which devices you have in the system, how they are connected, where the risks are, and which risks are the most serious. Equipped with this knowledge, you can start implementing various cyber security controls, but only after you have addressed another crucial task, backups.

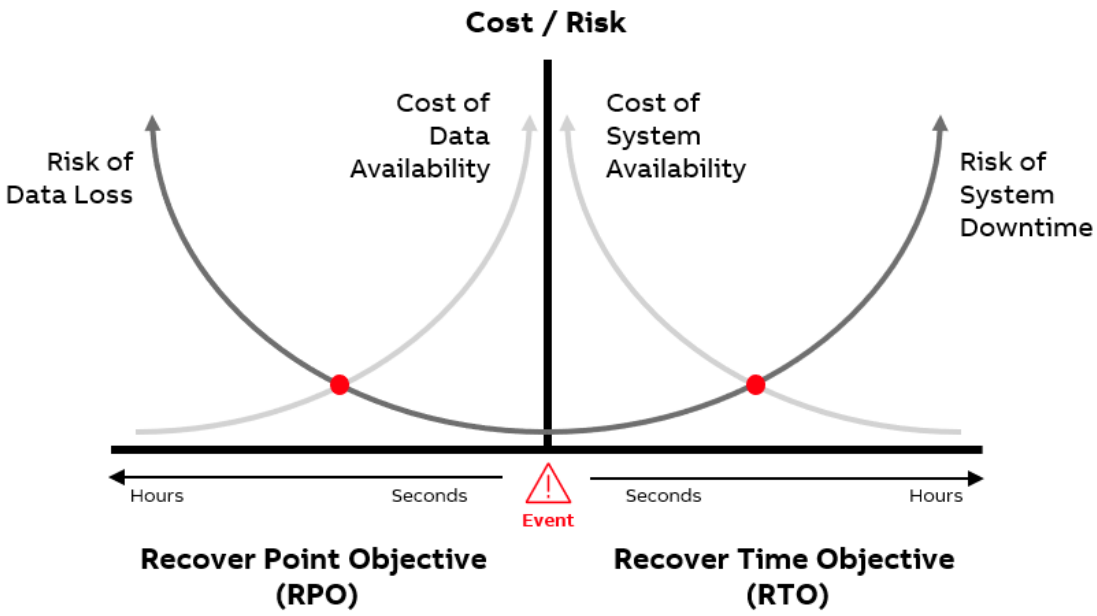
Without a backup, you have nothing

Once you have assessed your system or systems, your first step must be to implement and configure a backup solution. This is your last line of defense. A backup solution is essential since a good backup ensures that the investment made in the DCS system is protected. In case of a hardware or software incident or failure, you can easily restore the full DCS system or parts of it and then resume production relatively quickly. Such incidents or failures may be cyber-related, but often they are simply due to operator and user mistakes.

Another aspect of backups that one must consider is the business continuation plan, where you define how much data you can afford to lose (Recovery Point Objective[5]) and how quickly after a disaster you must be back in production (Recovery Time Objective[5]). These factors determine the backup system setup, backup schemes, and price. A business continuation plan with low RPO and/or RTO requires more from the backup system than a plan where it is less critical to restore production exceptionally quickly.

Knowing that the system is safely backed up also means you can implement updates, performance improvements, and cyber security solutions quicker because you know there is a way to restore to the last properly functioning system version if something goes wrong. Now, we can start tackling the security controls.

—
05 https://www.msp360.com/resources/blog/rto-vs-rpo-difference/



Next, put basic Security Controls in place

Up until this point in the process, we have not actually made the system more secure. We have merely assessed it to make sure we apply the right security controls in the right places – where they will have the most significant and beneficial impacts. We have also made sure that we can recover from a disaster using our backup system.

Security controls are a must
Security controls are anything that actively works to protect the system. The most common security controls are malware protection and security updates. To an IT professional or even an IT hobbyist, taking these measures is so basic that it is unfathomable that any computer system would be running without them. However, the reality is that many industrial systems are operating either with no such controls or with outdated ones.

The reasons given to explain why updates and malware protection aren't applied is often one of these three excuses:

"I have never had a problem in the past"

"I don't want to risk applying updates to a running system, and I must keep it running"

"Our system is air-gapped (not connected to any other system or network)"

--

Past experience is good but absolutely no guarantee about what can happen in the future. Threats evolve and change, so what seemingly worked in the past is unlikely to work in the future.

When one applies security and malware protection updates correctly, the risk to production is far less than operating without any updated protection. Lastly, air-gapping is NOT a security control. The Natanz Nuclear Facility was air-gapped, with no network connections to anything outside the facility. If a nation-state can't successfully air-gap a system located in a hardened facility far away from the attacker, who can?

Malware protection and security update procedures
Even such basic controls as malware protection and security updates must be implemented with care to avoid a negative impact on production, both during implementation and in regular operation. Only DCS vendor-approved security updates should be installed, and only validated malware protection used.

Additional security controls
Other security controls worth mentioning include application whitelisting, asset inventory, and system hardening. Each one of these improve the cyber security defense by adding various aspects of protection.

- Whitelisting prevents unapproved applications from running, which is a robust security control but only when combined with security updates and malware protection.

- A well-designed automated asset inventory helps the user detect any newly added devices in the system. Once detected, they can be added to the set of items protected by the security controls. However, if the detected device is not known, it may be related to an attack.

- Hardening configures computers to be as secure as possible while still performing their primary functions. A system that monitors the hardening settings keeps an eye on these configurations and makes sure no one changes them to a less secure state, further reducing the risk of intentional or unintentional changes that make the system vulnerable to attacks.

In addition to these security controls, there are many other products and solutions available on the market. Suppose some of them appear to solve a specific problem or risk that you have identified during the risk assessment. In that case, it's imperative to make sure that they add security to your system and won't negatively impact system availability and production.

What we have covered so far regarding security control falls into a category of controls called technical controls meaning that we have applied technology to address the cyber risks. There are also physical (think locks etc.) and administrative controls (training and such)[6] that one can use to create a holistic defense against cyber risks.

—
06 https://www.f5.com/labs/articles/education/what-are-security-controls

Aging impacts security too

Like anything else, operating systems age, and at some point the vendor will end support of old applications. Once this happens, no further security or malware protection updates will be released for the outdated system. This must be avoided because once the updates stop coming, it is only a question of time before the system is open to vulnerabilities, like allowing a virus to get in and make the system unstable or unusable. Do not get yourself into a corner where you are forced to act just because of old unsupported software. Instead, be proactive, take control of cyber security, and drive it the way you deem best.

Training of people
Highly effective to reduce risk

At this point, we have covered assessments and security controls but have so far left out the most significant risk in any organization: Its people. Numerous successful and devastating attacks have used company employees to get into the targeted system[7]. This can be someone that either deliberately or by coercion performs the task for the attacker.

However, the most common route is that the hacker tricks someone into unknowingly helping them. A common example is using emails to get the receiver to click on a link that downloads a virus to the user's computer. Once in, the virus can spread by itself and do harm or establish a connection back to the hacker to access and manipulate the computer to get to the target. This is called phishing or spear-phishing, depending on if it is a mail blast or directed at a specific person.

Even air-gapped systems are vulnerable since studies show that you could simply "drop" infected USB drives in the parking lot at the intended target and hope that someone happens to pick one up and later connect it to a computer[8]. Add to this the fact that very few air-gapped systems actually are[9].

The most effective way to address these risks is awareness training. In such training, one discusses cyber security, attack vectors, and risk-minimizing behavior with anyone that will ever be close to the system or its components. This low-cost approach is often exceedingly successful. Just remember that the training must be systematic, reoccurring, and mandatory. Any new employee or contractor must go through the training before handling or being in contact with the system.

You must also train your cyber security team to get the most out of the investment in cyber security controls. The controls are only as good as the people who are using and managing them. You can pay millions of dollars for cyber controls, but if no one knows how to use them or maintain them, they provide absolutely no value. If your security controls warn you of a potential breach, but no one is looking at it, an attacker may have free reign. The same goes if the security controls aren't functional due to a lapse in maintenance.

—
07 It is believed that the Shamoon attack used employees to get the virus into the systems. https://en.wikipedia.org/wiki/Shamoon

—
08 https://www.blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf

—
09 As stated by Sean McGurk, the former Director of the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security https://blog.safe-t.com/industrial-security-is-the-air-gap-still-viable

No shortcuts to true security

Because cyber security sometimes has a stigma of being very complicated, and we tend to have an inherent need for quick results, it is tempting to fall for good marketing of products that promise to solve all of your OT cyber protection needs at once. There is no such product! One must always start with the foundation, as outlined previously.

If someone promises to solve all your cyber issues without explaining how and without covering the basics, you should be careful. You do not want to spend money or trust something that likely won't protect your OT and production processes. Or worse, give you a false sense of security to make you lower your guard.

—

Security is like safety; you can never relax or stop working on improving it.

Simple steps cover 85% of the risks

—
10 https://www.cisecurity.org/media-mention/implementing-the-cis-20-critical-security-controls-slash-risk-of-cyber-attacks-by-85/

At this point, if you have taken the previously listed measures, you should have a reasonably secure system where you have addressed the risks and are able to avoid most threats. CIS, the Center for Internet Security, estimates that up to 85% of cyber risks can be addressed with the simple measures covered so far[10]. Let's review what we have:

1. Know your system

   a. A complete asset inventory of all cyber assets which ensures that no device is forgotten or has lower security than the rest.

   b. A complete overview of the network and how the devices interact with each other to make up the production system.

   c. Knowledge of where the biggest risks are, how likely it is for an attack to be successful and what the impact will be.

2. Basic Security Controls

   a. All Windows computers in the system are updated with the most recent, vendor-approved, security updates to minimize the number of vulnerabilities that attackers can take advantage of.

   b. All Windows computers have malware protection that is frequently updated, which keeps the system secure by detecting and defending against the latest viruses.

   c. If things still do go wrong, which they can since there is no such thing as a 100% secure system, and computers break, there are backups to allow quick restoration and resumed production in case of a problem.

3. Training

   a. Everyone who can come in contact with the system, or any part of the system, knows what to do and what not to do with it. This limits the risk of malware entering the system, as well as accidental disruption due to carelessness.

   b. Those that maintain and use the security controls understand how the controls work, how to keep them running, and what to do if something happens.

As discussed previously, additional controls can be installed, but the steps covered previously should be considered the fundamental cyber security actions that any OT system owner should take.

Collaboration is well worth considering

Concepts for implementing cyber security are relatively straightforward. However, it is not always the most cost-effective strategy to take this on solely by yourself.

Consider the investment needed for cyber security, disregarding the hardware and software costs as they are often the smallest part. Managing cyber security in-house can be costly and will take time. There are many aspects to consider, such as training, tools, and procedures. System owners must balance the investment in employing people that have cyber expertise with the fact that cyber events are infrequent.

A better and often cheaper approach is to seek out a partner to help with cyber security. A company that provides cyber security services often has the best and most experienced engineers because they deal only with cyber security all day, year-round. The experience that the partners' experts can provide is tough to build in-house, especially if the cyber engineer only works in one location and with one system. By leveraging the partnership, the system owner doesn't need to figure out a way to maximize his own security expert's time but has access to the partner's security experts when needed.

Another advantage of an external company is that you benefit from their efficient processes and tools that have often been developed over many years and frequently refined and updated. As the external company works with several customers and other vendors, they have a good sense of what is going on in the world and the industry and will often keep you informed about cyber trends and threats.

When selecting an external company to help with OT cyber security you should consider a few key things:

- **DCS system skills:**
  Is the company used to working with OT, or are they purely specialized in IT? You need a partner that understands OT cyber security, how a control system works, and what you do to keep production running.

- **Support:**
  Will the company be able to support you promptly in case something happens? Can you get 24/7 support?

- **One-stop shop:**
  Can the partner provide a wide range of cyber security solutions? It is much less likely that something is overlooked if you have only one partner responsible for cyber security, reducing the risk of gaps and simplifying discussions.

- **A wide selection of cyber solutions:**
  Does that company partner with other cyber companies to provide you with the best solutions and technology, and can this technology be deployed safely and correctly?

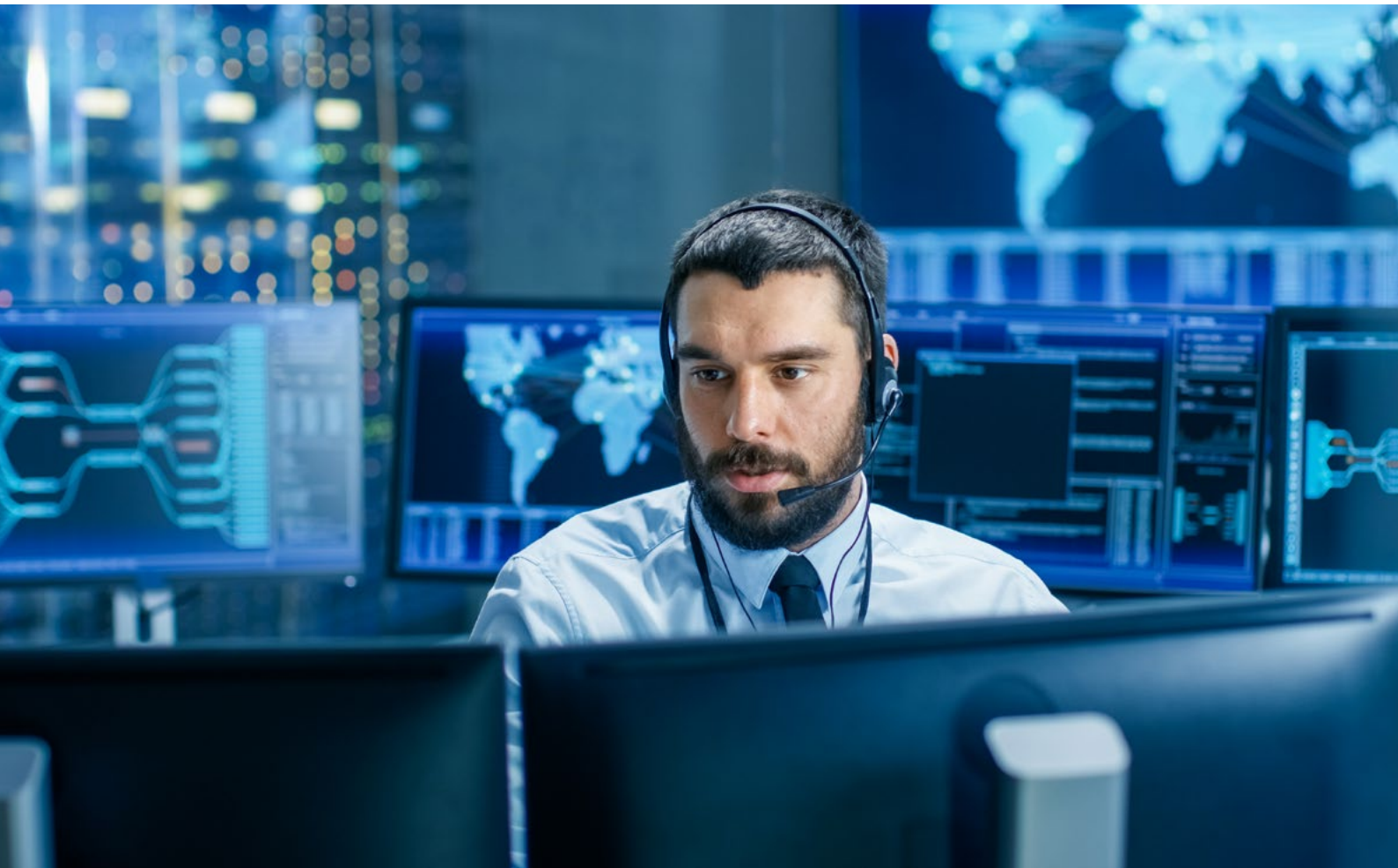
- **Resources:**
  Do they possess the right resources near to where you have operations, whether you operate locally or worldwide? Is there any risk they may leave you stranded without enough resources, locally or globally?

- **Flexible:**
  Can the partner meet you where you are at in your cyber security journey? Remember, you must build security from the bottom up, and nothing good ever comes from skipping a step.

Shared resources offer efficiency

A natural step once a partner has been found is to consider possibilities for them to handle cyber security maintenance and operation. Maintenance merely lets someone else, your trusted partner, be responsible for keeping the security controls functional so that they are always running and have the correct updates and configurations. This is often provided remotely to reduce the cost. However, one should never underestimate the value that comes with personal connections. Knowing your partner's engineers can be instrumental when a problem comes up or even when you have a question. Good personal relations are always valuable, and it is good to get your partner's people accustomed to your facility, your processes, and your people.

The next step after maintenance is actual operations, where your partner takes over the actual work that comes with cyber security. The maintenance described previously makes sure your controls are functioning, while operations ensure that your system is protected according to the service agreement. Operations may be as simple as validating backups, rebooting computers after updates are distributed, or as advanced as 24/7 security monitoring.



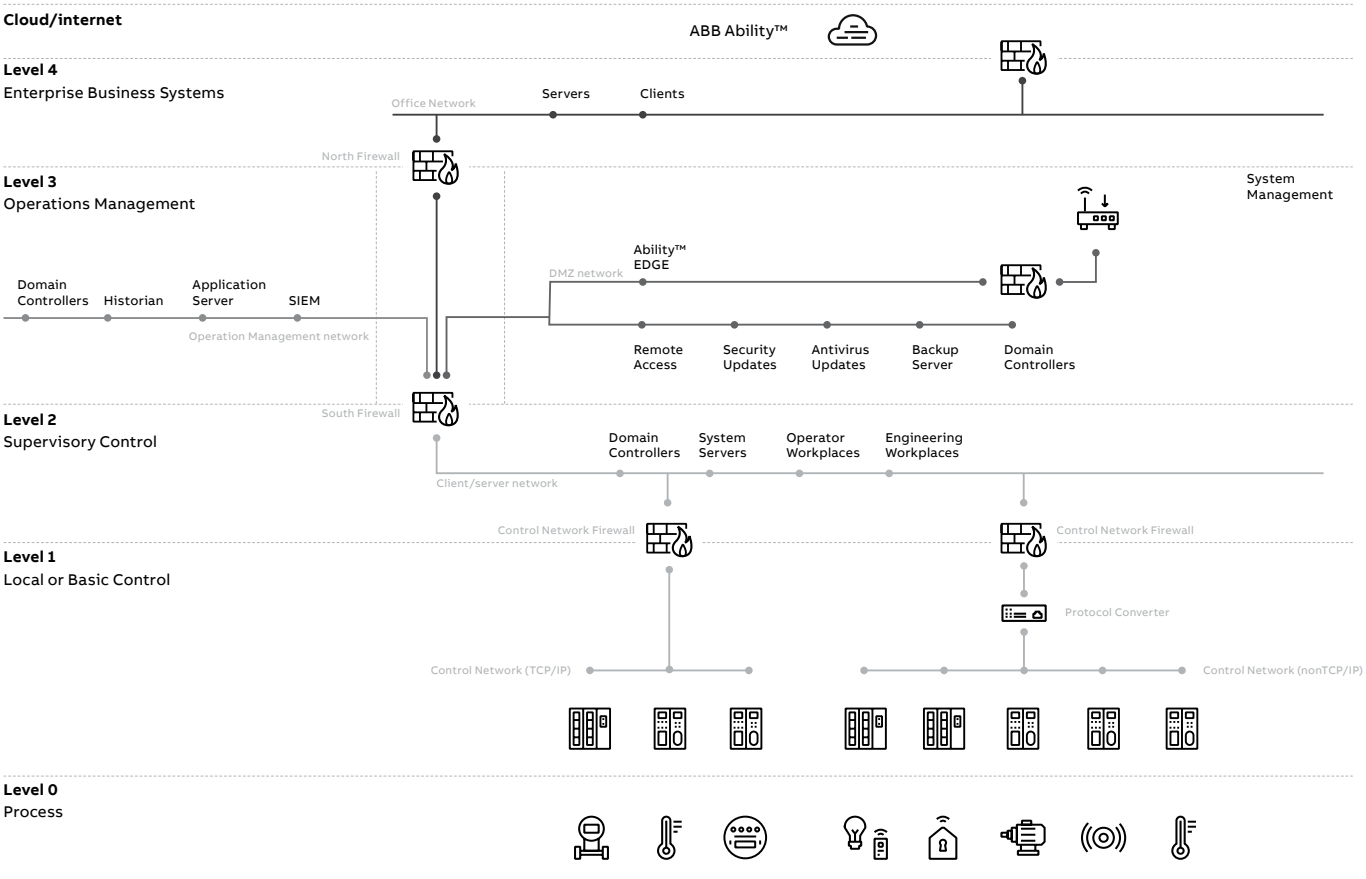
Reference Architecture

At the beginning of this paper, we looked at how interconnectivity today benefits us all and how industry should also be able to use the insight that comes with interconnectivity to improve operations and make better production decisions. Applying good cyber security is one of the critical steps needed to reap the benefits of cloud computing securely.

The other essential step is having a well-designed network where special care has been taken to enable the required data to go to and from your industrial systems while keeping it safe. Most security standards and best practices cover this need to one degree or another. Transforming these documents' recommendations into an actual design that allows data between your DCS system and a cloud service is not very difficult. Still, there are several aspects to consider that can make it tricky.

A better option than doing this by yourself is to rely on one of the many models or reference architectures available. Some of these reference architectures are made for IT systems and some for OT. Some are general in nature, and others are designed to sell more of a vendor's products. While most are very good and provide the necessary security, you must be careful to pick one that works optimally for you, your needs, and your systems.

A good architecture is also required if your ambition is to meet certain standards, such as a specific security level like the one defined in IEC62443-3-3. You save much effort if you pick one architecture that already meets or exceeds the level you are aiming for.



Advanced security measures

Without security built on a strong foundation, your system is extremely vulnerable. As indicated earlier, with good basic security you can avoid upwards of 85% of the threats that constantly risk impacting your production. However, you may want or need an even greater level of protection.

First, you must understand what your risk tolerance is and what the financial impact of a cyber incident could be. Only when you know these things can you decide whether to spend more on security or not. There is no reason to pay more for security than what you stand to lose in case of an incident.

Naturally, many factors make up the financial impact – not only in direct production losses but also in other things like reputation, fines, or health and safety. Foundational security may be enough, or you may need to deploy more security to reach the right protection level. If you conclude 85% protection is not enough, then you need additional cyber security measures.

To be clear, no matter what you do, you can never be 100% protected. This is simply not achievable.

Monitoring watches for suspicious activities

But to get closer to 100%, you must augment the basic controls with monitoring. Monitoring helps detect abnormal activity, so if something sneaks by the first line of your cyber defense, you can take action to mitigate the newly detected risk.

There are essentially two methods of monitoring: Event Monitoring and Network Monitoring. Event Monitoring uses available logs in the OT systems and devices to detect suspicious activity, while Network monitoring uses network traffic to do the same. They complement each other and deciding which one to start with depends on many things.

Event Monitoring is a proven methodology that alerts the user about any suspicious activity based on rules (e.g. USB drive is attached to machine or user has repeatedly logged in with an incorrect password). Network monitoring is another popular solution that detects anomalies in the network traffic (e.g. a machine in your network tries to reach a destination IP address in another country). Network monitoring often requires an investment in upgrading network equipment before deployment.

Independent of which one you start with, it is critical to have a team that monitors the generated alerts to respond if necessary. Without this, you cannot realize any value from your security investment.

As far as staffing these monitoring functions, you can either build this team yourself or find a partner to provide it for you. Unless you have an extensive production system or several of them, it is likely not financially worthwhile to recruit, train, and build your own team.

The next security component, which dovetails into monitoring, is incident response. This is the action taken after the event monitoring or network monitoring systems have detected something suspicious. When this happens, time and fast action are critical if you are to succeed in protecting your operations, and it is thus vital to have the right people in place who know how to take the right steps to mitigate the risk. This is another task that you can choose to do yourself or outsource to your partner, depending on your cost/benefit calculations.

Notable events – in retrospect

Regarding the attacks mentioned at the start of this paper, let's add a little insight into these cases.

Merck
Ransomware is a nasty virus and something you want to avoid.

- Basic controls: The best defense against this is to make sure that the latest security patches and malware protection are installed as soon as they are available. Unfortunately, there may still be unknown (aka zero day) vulnerabilities that the attacker can leverage.
- Training: A second measure that can significantly reduce the likelihood of being infected with ransomware, or any virus, is awareness training that teaches every employee and contractor to identify a phishing or spear-phishing attack. These are often how the ransomware gets into a system. Another method that is mitigated by training is the USB trick covered earlier.
- Backup: Take backups and make sure that they work.

Ukrainian Power
This attack could have been avoided, or at least had greatly reduced impact, with a well-implemented cyber security program.

- Basic controls: Some of the attack surfaces would have been closed if the systems were updated correctly, with security updates and malware protection.
- Reference Architecture: A well-designed network with zones and conduits would have made it harder for the attacker to move around.
- Monitoring: Event or Network monitoring would have provided an early warning of what was going on and, if acted upon, this could have stopped the attack before production was impacted.

Natanz enrichment facility
The Stuxnet case is different than most because it was a targeted attack where the hackers' only goal was to disrupt this one facility. It is hard to defend against the attackers if you are unlucky enough to become an explicit target. However, the same basic protections discussed in this paper still apply and will reduce the risks but not eliminate them. As mentioned earlier, there is no such thing as absolute security.

—
05 https://www.msp360.com/resources/blog/rto-vs-rpo-difference/

Conclusion

If you haven't already implemented cyber security in your OT processes, please start. It is not too late, and it is not that complicated. The seemingly-apparent steps covered previously will significantly increase your system's cyber resilience and enable you to take advantage of the new digital services delivered on-premises or in the cloud. If done correctly, your system will be able to handle the vast majority of cyber threats, and as a bonus, you are likely to get a more stable system that performs better and is easier to maintain.

Imagine a future where your cloud-based predictive maintenance system provides you – in advance – with actionable information that makes your industrial process run smoother, more predictably, with increased efficiency and higher uptime. Many of these benefits are available already. For instance, you don't have to spend any time with regular checks of your DCS system since some service does this for you and lets you know if something needs your attention. This directly saves time that you can spend on more important things and also directly gives increased system availability. Similarly, you can use pertinent process data to determine when valves and control loops need attention. Optimized control loops are directly correlated to improved quality, reduced material costs, and increased production.
For cyber security controls, you often unlock additional functions and features by enabling a connection to various online databases and systems. Vulnerability assessment tied to asset inventories, done via network monitoring, is just one example where an internet connection provides considerably more value out of your investment.

Finally, on top of all the benefits listed previously, you also know that you have a system which is safeguarded against over 85% of all cyber threats.

I don't know about you, but I sure would sleep better at night knowing that the system I am responsible for is protected.

—
For more information,
you can contact

Patrik Boo
Cyber Security Manager
Process Automation, ABB, USA
patrik.boo@us.abb.com