



ACCIDENTAL CONVERGENCE A GUIDE TO SECURED IT/OT OPERATIONS

WHITE PAPER



Contents

- The Convergence Initiative 3
- The Air Gap Argument 4
- Accidental Convergence 5
- Threat Actors 6
- Planning for the Security Ahead 7
 - Visibility that Extends Beyond Traditional Borders 7
 - Deep Situational Analysis 7
 - Reduction of Cyber Risk 8
 - Security that Contributes to the Ecosystem of Trust 8
 - Solutions that Scale 9
 - Accidental Convergence, Intentional Security 9



The Convergence Initiative

Modern-day industrial and critical infrastructure organizations rely heavily on the operational technology (OT) environment to produce their goods and services. Beyond traditional IT operations that utilize servers, routers, PCs and switches, these organizations also rely on OT, such as programmable logic controllers (PLCs), distributed control systems (DCSs) and human machine interfaces (HMIs) to run their physical plants and factories. While OT devices have been in commercial use since the late 1960s, a complete transformation has occurred, changing the way we operate, interact with and secure the OT environment.

Many organizations have opted to converge their IT and OT environments, which can yield many benefits; at the same time, these decisions are not without risk. Convergence can produce new attack vectors and attack surfaces; it can result in breaches that start on one side of the converged infrastructure and laterally creep to the other, from IT to OT and vice versa.

Threats that impact OT operations are not the same as those that impact IT environments, thus the required security tools and operating policies are different. Deploying the right ones can harness all of the benefits of a converged operation without increasing the security exposure profile of the organization. It is important for organizations to establish a carefully planned strategy prior to any convergence initiative, rather than bolting on security as an afterthought.

The Air Gap Argument

What happens when a business makes the strategic decision to NOT converge their IT and OT operations? Many organizations follow this path for a variety of reasons including strategic, technical and business factors. By keeping IT and OT systems separate, these organizations are implementing an “air gap” security strategy.

Traditionally, air gapping OT operations has been viewed as the gold standard when it comes to industrial and critical infrastructure environments. Operating as a “closed loop” without any interfaces to the outside world, the OT infrastructure is physically sequestered from any external environment. With no data traveling outside the environment, and nothing from outside coming in, this buffer is viewed as the ultimate methodology in securing an organization from security threats.

While the notion of air gapping seems simple enough, it is extremely difficult to maintain. Simply cutting connections is only part of maintaining a sterile environment, and there are many other paths into what is supposedly an isolated infrastructure. For example, true isolation requires the elimination of electromagnetic radiation from the devices in an OT infrastructure; this requires the implementation of a massive faraday cage to eliminate potential leakage vectors.

Over the years, additional attack vectors have been discovered, including FM frequency signals from a computer to a mobile phone; thermal communication channels between air gapped computers; the exploitation of cellular frequencies; and near-field communication (NFC) channels. Even LED light pulses among OT equipment have exposed critical systems to malicious activity.

There are countless examples of highly-enforced air gapped facilities that have suffered a breach due to something as simple and seemingly innocuous as an external laptop being used as an HMI, or a USB thumb drive used for OT purposes. In an average OT environment, upwards of 20 percent of the infrastructure comprises IT equipment. For organizations that have implemented an Industry 4.0 initiative, such as industrial IoT, the amount of IT-related equipment can balloon to 40 percent of the OT infrastructure.

Organizations that have no specific initiatives for IT and OT convergence are among the most at risk because no additional security is implemented beyond air gapping. Securing operations requires more than building a digital moat around the OT infrastructure. Even under the most favorable of circumstances, this isolation is nearly impossible to maintain. The introduction of one seemingly harmless variable into a sterile environment can permanently destroy the most stringently enforced air gap. This is known as “accidental convergence.”

Exploits in Air-Gapped Environments

Air-gapped environments are thought to be amongst the most secured. However, recent attacks that leverage previously unknown attack vectors have proven that they too can be exploited.

These methods include:



acoustic



light



seismic



magnetic



thermal



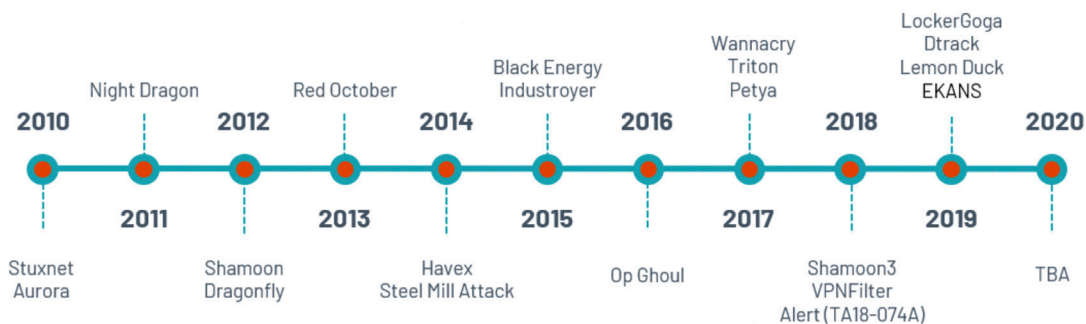
radio-
frequency



physical
media

Accidental Convergence

While air gapping OT from the “rest of the world” is often considered the gold standard in terms of securing OT environments, it is not foolproof. In fact, many organizations are easily lulled into a false sense of security even though their isolated OT infrastructure is anything but isolated; and as a result, it is anything but secure.






Over the last ten years, increased incidents of attacks have targeted manufacturing and critical infrastructure. Among them are examples of sophisticated attacks that took advantage of “accidental convergence” to infiltrate and gain a foothold within organizations. Some examples include:

- In 2010, a USB was used to infect a nuclear facility. Upon plugging in the USB to the network, it launched an attack and adjusted the RPM on the centrifuges enough to destroy them. A secondary part of the attack infected the HMIs to show that the centrifuges were operating as normal. Since then, USBs are often used to jump air gapped networks, including documented attacks such as Turla MiniDuke, RedOctober, Fanny, Remsec and more.
- In 2018, the U.S. accused Russia of “jumping the air gap” and infecting countless grid operations, essentially obtaining “red button functionality” to disable grid operations at the time of their choosing. This was a watershed moment in proactively weaponizing an OT attack to be used at a later date. These attacks became known as Dragonfly and Energetic Bear.
- In 2019, a nuclear facility deployed brand new Windows-based PCs in their OT network for command and control purposes. These new PCs arrived with a major security vulnerability. Only weeks later, the vulnerability was exploited, resulting in an OT incident that forced the emergency shutdown of two of the reactors.

The accidental convergence of IT and OT environments can occur at any time. Even more concerning is that it happens in many organizations without their knowledge and without consequence because of the erroneous belief that the air gap is doing the job. After gaining a foothold, these attacks can continue for weeks and even months until a catastrophic failure occurs. The security thought to be in place was an illusion far from the actual reality.

Threat Actors

To understand how to protect the OT environment, we need to understand who the key threat actors are.

		
External Attack	Malicious Insider	Human Error
<ul style="list-style-type: none">• External targeted attacks• Collateral damage	<ul style="list-style-type: none">• Disgruntled employees• Dishonest 3rd Parties	<ul style="list-style-type: none">• Unintentional mistakes• Compromised devices



External Attack

Threats from the outside tend to be the vector we look at first as the prime originator of an attack, and with good reason. For over three decades, the IT security community was an unwilling participant in a game of cat and mouse, constantly pursuing the latest cyberthreats. Hackers typically search for the weakest link to exploit, and now their attention has shifted to OT which in general is significantly less fortified. Outside hackers have a variety of motivations which span simple cyber vandalism to profit from stolen data and credentials. While these motivations ring true for IT, with OT there are additional factions involved including cyber terrorists and rogue nation-states.



Malicious Insider

Organizational insiders typically have elevated credentials which give them access to spaces the general public cannot tread. This population segment is the fastest growing group of potential threat actors because organizations give access credentials to an ever increasing and heterogeneous audience. This may include employees, partners, subcontractors and more. While the vast majority of this audience segment has the organization's best interests in mind, any rogue insider can inflict untold damage given the access provided to perform routine job functions.



Human Error

Whether it is a misconfiguration, a careless mistake or an overlooked action, human error is by far the most common threat vector. It can result from poor training, a momentary lapse in judgment or simple carelessness. While every organization intends to maintain a good security posture, human error is the biggest reason breaches occur and is the most common activity that results in accidental convergence.

Planning for the Security Ahead

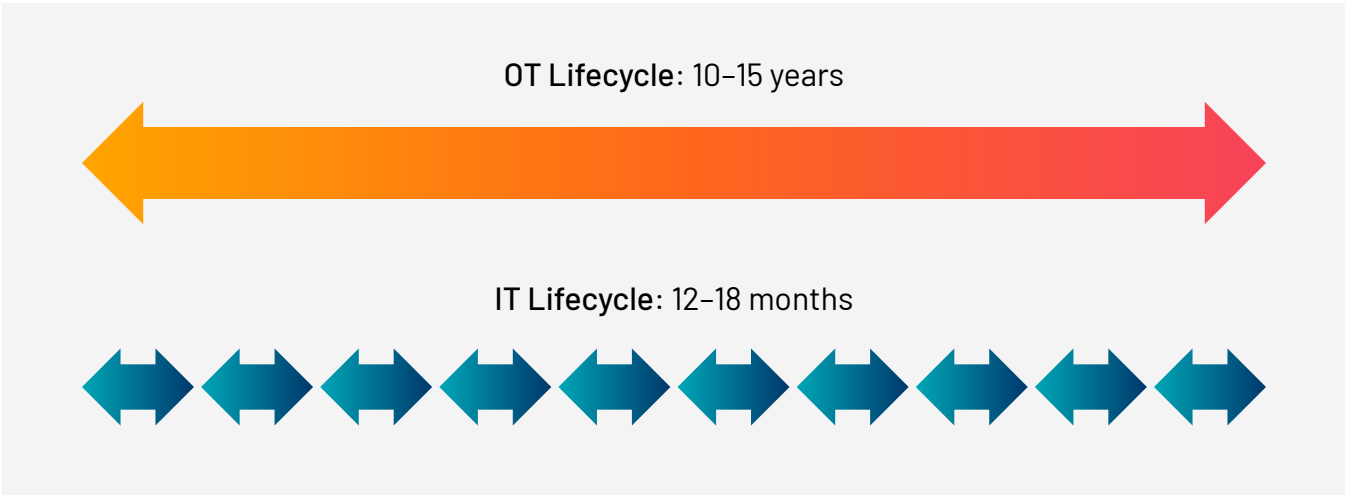
For most industrial organizations, the need for vigilant security is nothing new. Threat vectors and the security forecast is constantly evolving given emerging threats. The convergence of IT and OT operations, whether planned or unplanned, is in almost all cases a reality. Setting the appropriate safeguards will help ensure secured operations for your organization. What should you consider?

Visibility that Extends Beyond Traditional Borders

Up until this point, IT security and OT infrastructures inhabited completely different worlds, thus the ability to see into either environment was bifurcated along these lines. As this paper has illustrated, modern-day attacks are amorphous and travel across the traditional IT and OT security borders without regard. Our ability to track these types of propagation routes requires the de-siloing of traditional visibility parameters. Being able to gain a single view of IT and OT gear, along with the conversations happening between the two worlds, is essential. This “single pane of glass” view can help illuminate potential attack vectors and asset blind spots that may have eluded traditional security strategies.

Deep Situational Analysis

Whether or not a planned convergence initiative is in the works, it is important to recognize the significant difference in IT and OT life cycles. While IT infrastructures update regularly, OT infrastructures often persist for years, even decades.



It is not uncommon for an OT infrastructure to be as old as the plant itself. The result is that a full inventory of assets, along with maintenance and change management records, may not be current. Therefore, crucial data may be missing, including important details such as model number, location, firmware version, patch level, backplane detail and more. Since it is impossible to secure assets that you may not even know exist, having a detailed inventory of your OT infrastructure that can be automatically updated as conditions change is essential to protecting your industrial operations.

Reduction of Cyber Risk

When it comes to modern OT environments, cyberthreats can originate from anywhere and travel everywhere. Therefore, it is important to utilize as many capabilities and methodologies as possible to find and mitigate exposure risk. This includes:

- Network-based detection that:
 - Leverages policies for white-listing and black-listing capabilities.
 - Anomaly-based detection that can find zero-day and targeted attacks and is predicated on baseline behaviors unique to your organization.
 - Open-source attack databases such as Suricata that centralize threat intelligence from the greater security community. The notion is that more eyes on a potential threat yields a significantly better security response.
- Since most attacks target devices rather than networks, it is essential to utilize a solution that actively queries and provides security at the device level. Because OT device protocols can vary widely, security and health checks must be unique to the make and model of the device, including the device language. These deep checks should not scan but rather be precise in query nature and frequency.
- In 2019, over 20,000 new vulnerabilities were disclosed, affecting OT devices as well as traditional IT assets. However, less than half of these vulnerabilities actually had an available exploit. Gaining a full awareness of the vulnerabilities that are relevant to your environment, along with a triaged list of exploitable vulnerabilities and critical assets, will enable you to prioritize the threats with the highest risk score, thereby dramatically reducing your cyber exposure profile.

Security that Contributes to the Ecosystem of Trust

While it is important to identify and leverage the best IT and OT security products for your environment, it is even more important that the products work together. The age-old notion of a layered and cooperative security approach, where point products can work together, creates an impermeable layer—the totality of the solution becomes greater than the sum of its parts.

One such example is an OT security solution that feeds valuable details to a security information and event management (SIEM) system or next-generation firewall (NGFW), providing an entirely new and important view of industrial operations to the security ecosystem. This not only enhances security monitoring and response, but also unlocks greater value and practical utility from existing security investments.

Solutions that Scale

As noted earlier, the lineage and approach of the legacy IT and OT teams could not be greater opposites. And this polarity goes far beyond product life cycle timelines.



IT teams are typically driven by KPIs involving availability, integrity and confidentiality, which result in an “always secured” mentality. OT teams monitor metrics revolving around environment, safety and regulation, resulting in an “always on—set it and forget it” approach.

Today’s need to meaningfully address security across the entire organization—not just IT or OT—requires these vastly different “upbringings” to come together and find common ground to work as one. Failure to do so leaves the organization with a gaping cyber exposure hole that, if left unaddressed, could result in unimaginable consequences.

Accidental Convergence, Intentional Security

IT and OT teams must find common ground to eliminate the substantial risk factors of both planned and accidental IT/OT convergence. But the mission does not end there. OT security solutions that work in conjunction with IT security solutions can be the catalyst that not only provides the visibility, security and control needed to thwart new cyberthreats, but also brings these once separate teams together for the common security every manufacturing, critical infrastructure and industrial organization needs to fulfill its core mission efficiently and securely.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.



COPYRIGHT 2020 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, TENABLE NETWORK SECURITY, NESSUS, SECURITYCENTER, SECURITYCENTER CONTINUOUS VIEW AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. TENABLE.SC, TENABLE.OT, LUMIN, INDEGY, ASSURE, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.