CYBERSECURITY POWERS SMART FACTORIES

HOW TO ENABLE SECURE INTEGRATION OF YOUR IT AND OT ENVIRONMENTS

UNISYS | Securing Your Tomorrow®

What makes a Smart Factory smart? The same thing that makes it vulnerable to cybercriminals.

As manufacturers and industrial organizations invest in reaping the considerable rewards of integrating information technology into their operational technology environment (IT/OT Convergence), security must be a core and constant consideration. This paper illustrates how Unisys and SIAS view the security risks, the challenges, and the strategic elements for manufacturing operations that are not only smart but cybersecure.

The benefits of converting traditional factory operations to the "Smart Factory" concept are many, and they are increasingly embraced across the world of manufacturing: cost reductions, productivity improvements, better products, analytics for better, faster decisions, and more efficiency and flexibility.

All these benefits, necessary for the future competitiveness and even survival of manufacturing businesses, depend on the organization's ability to assemble, analyze, and deploy the latest technologies to gain a competitive advantage from its vast stores of valuable information. That ability depends in turn on a thorough and secure IT/OT convergence.

Many manufacturers are avidly embracing the Smart Factory concept for these benefits. And now, in the wake of massive, destructive cyber breaches, they are increasingly recognizing the importance of security at every step along the way. IT/OT convergence, including the widespread adoption of Internet of Things (IoT) devices, opens the organization to malefactors – from individual actors, to highly organized groups, to nation states – who variously seek to extort money, steal intellectual property addresses, disrupt operations, and destroy vital information and infrastructure.

The successful predations of these growing and aggressive criminal operations, ranging from the nuisance of hacked IP addresses to the catastrophic takeover of whole companies, will only mount without swift, effective protective measures.

Challenges to IT/OT Convergence

In changing times, it will be the manufacturers and industrial organizations that best adapt who will continue to survive and potentially prosper. Whether by adapting to new ways of working, routes to market, or the ability to reduce costs in challenging circumstances. Although many are advancing their technological capabilities at a competitive pace, the typical organization faces impediments to the rapid adoption of IT and OT Convergence:

- *Information Silos* - In the traditional factory the information tends to be siloed in different systems, departments, locations – and thus largely inaccessible to corporate networks that could convert the information to value.
- *Fundamental Differences* – Any convergence effort quickly illustrates the gulf – almost a polarity between OT and IT. OT's machines, equipment, industrial controls and production systems are intrinsically mismatched to IT's storage, computing, infrastructure, data processing, and analytics processing. Leaders of the convergence need to recognize this gulf before they can reconcile the differences.
- *Technical and Organizational Realities* – Convergence is further complicated when an organization is replete with differing protocols and technical interfaces, varying operational processes, and differentiated teams and reporting structures. Many solutions are designed from an IT perspective, presenting gaps that OT must fill or assumptions that do not apply to the IT environment.

In a recent survey carried out by Deloitte-MAPI[1], factory leaders responded that the lack of the necessary IT Infrastructure, and the resulting security vulnerability, was a significant impediment to the Smart Factory concept.

- *Cybersecurity Worries* - Concerns about security can also hamper the necessary integration of information and operations, as smart factory advocates increasingly recognize that each instance of IT integrated with OT in effect expands the cyberattack surface.
- *Compliance Demands* – While IT/OT convergence will ultimately drive competitive advantages, it also presents challenges to existing operational processes which rely on standards and regulatory structures. Industrial enterprises need a way to maintain their business practices while leveraging these benefits.

Despite these challenges, industry leaders recognize the business imperative to continue implementing more device-to-cloud and sensor-to-cloud integration along with new communications technologies like 5G on their path to convergence. Many organizations – automotive, transport, pharmaceutical, consumer, and others – are committed to proceeding on the path to the Smart Factory.

As they do so, Unisys and Sightline draw on their cybersecurity work with industrial clients around the world to collaborate on describing how these organizations can proceed safely, ensuring that their information remains uncompromised and available for business purposes. They posit four main elements to the successful path to safe and secure IT/OT convergence.

The 4 Elements of Safe and Secure IT/OT Convergence

1. Achieving Connectivity

The critical first step is to link networks whilst maintaining a security perimeter that can authenticate users and devices on a least-privilege, need-to-know basis. This enables organizations to collect data from any source and protect the data wherever it goes. Once this is implemented, organizations can then move onto embracing critical processes like automated monitoring activities and develop custom dashboards to show essential information and data. However, once OT networks are linked to a wider corporate IT infrastructure, vulnerabilities to cyberattack notably increase. The situation demands a new approach to security.

2. A New Approach to Security: Zero Trust

The new approach is premised on the long history of breaches that hardened, patrolled perimeters have failed to prevent, and it assumes that the entire IT ecosystem is already compromised. It is based on the Zero Trust model: Trust no user or device, inside or outside the private network. Essentially, it says the organization cannot automatically trust anything inside its perimeters or anything seeking access. This approach aligns with OT and IT aspirations.

In the Zero Trust approach, information is to be secured in place, with access controlled at a granular level. It emphasizes micro-segmentation to isolate critical assets, limiting damage in the event of a breach, and it promotes automation to quickly detect suspicious activity and allow systems under attack to dynamically isolate the intruder and respond as needed.

3. Rapid Detection and Response Times

The latest technologies enable vast amounts of data can now be gathered and correlated in seconds. Key data can be visualized in easily built reports and dashboards, enabling issues to be uncovered and addressed far more quickly than previously, not just within the plant but at any location with network access. Many enterprises are understanding this importance of leveraging time series data, predictive analytics, visualization, and advanced alerting capabilities to quickly turn insights into action, rather than just gathering data and highlighting challenges.

They can achieve seamless monitoring by automating data collection. They can be confident of a secure environment with their data encrypted and threats dynamically isolated.

[1] Deloitte., (2020). Implementing the Smart Factory: New Perspectives for Driving Value.

4. Unlock Efficiencies and Cost Savings

Once the tools have been implemented to gather, correlate, and output data into reports and dashboards, the stage is set for organizations to proactively make well-informed, quantitative decisions to quickly achieve new efficiency based on real-time data. They can uncover critical system failures, improve operational performance, and plan for capacity growth – all the benefits of IT/OT convergence.

Although many may be challenged to justify the business risk associated with implementing new solutions, many enterprises are still increasingly embracing the notion that now is the time to deliver IT/OT convergence because of the impact it can have in making their manufacturing operations more efficient, achieving less downtime and saving costs.

Why Unisys and Sightline

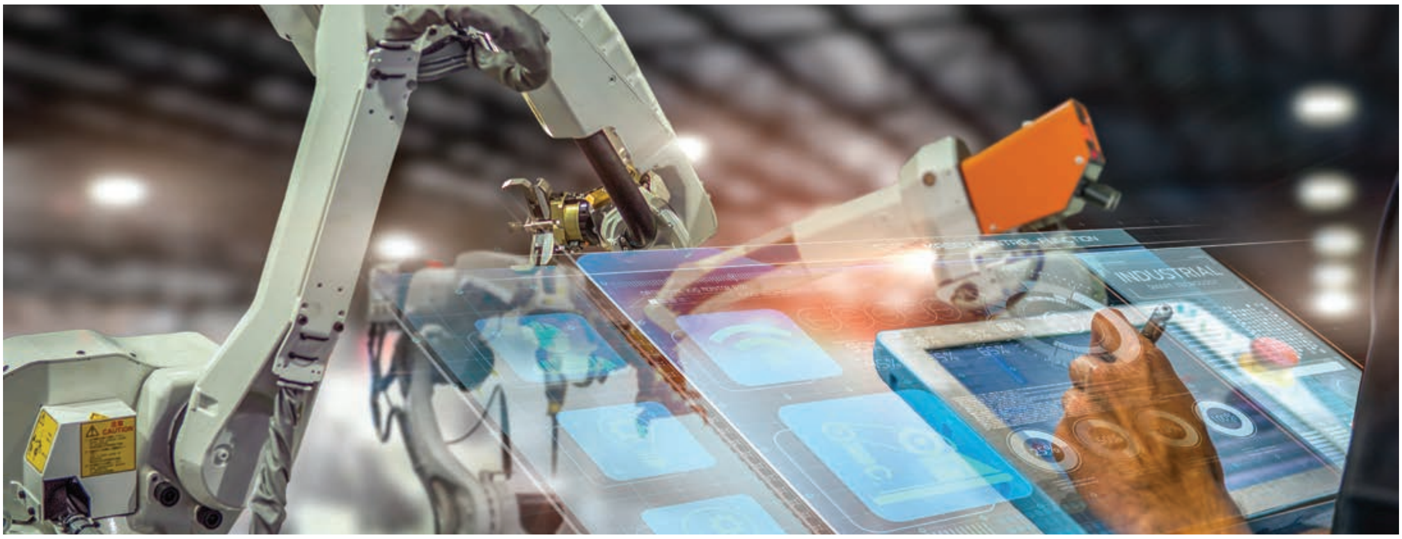
At Unisys and Sightline, we have had a long history of working with major industrial and manufacturing customers around the globe helping them to adopt innovative IT solutions, secure their vital infrastructure and constantly adapt to the challenges and opportunities they face. Our partnership has also resulted in a single, integrated solution – combining the proven technologies of Sightline's EDM™ platform and Unisys Stealth®. With this combined solution, industrial enterprises can address the challenges associated with utilizing production data, increasing production efficiencies and reducing costs. At the same time the solution gives greater confidence with maximized security against intrusions, sabotage or even user error.

Together we have a shared understanding of the manufacturing sector, appreciate modern challenges in the industry, and can leverage our joint IT expertise in truly supporting enterprises with their move to a more converged, efficient and productive way of working. That is why we aspired to develop a solution that enables enterprises to achieve the competitive benefits of integration and empower industrial executives to both analyze and leverage their data on a company-wide basis.

Our joint business offerings were presented to leading manufacturers and supply chain operators around the world at major industry security event early in 2020. Their subsequent input led to the development of a fully deliverable solution that can cybersecure the Smart Factory.

Summary

As manufacturers and industrial enterprises continue striving towards more efficient and profitable ways of working – e.g., the Smart Factory with all its benefits – their attack surface and vulnerability to cybercrime can increase if not protected with modern security approaches and technologies. To unlock the key benefits of the Smart Factory, organizations must proceed with a secure information integration strategy that benefits from the knowledge of OT and yet harmonizes with IT advances and a mandate to do so with effective cybersecurity.



For further information on how to identify and isolate threats across your manufacturing operations, please request a consultation with a Unisys representative at secureoutreach.unisys.com/SIASconsultation

For more information visit www.unisys.com