Rockwell Automation

Securing the Fourth Industrial Revolution

The Zero Trust Approach to Secure Digital Transformation in OT

Introduction

Digital Transformation is both a great driver of progress and efficiency, and an economic disruption that can deeply impact the innovation and development rhythms of organizations.

Adopting digital technology to transform products, services and businesses involves gaining greater insight and control for improved efficiency, typically by leveraging new data streams. These efforts often redefine experiences, such as customer experience, and can include changes in operating models that affect the security of digital assets.

In Operational Technology (OT), Digital Transformation is driving two big changes:

- OT systems are being connected to networks that they weren't connected to before in order to extract new data about operations. By definition, these systems live at the "edge" of the infrastructure and, therefore, must be deployed, secured, and managed as endpoints.
- Data-rich software applications are being deployed in OT production environments where this new data can best be used. Latency constraints in processing the data may result, due to its high volume and bandwidth. To address this issue, applications are also being deployed, secured, and managed at the endpoint.

What's more, OT organizations face several other common challenges that impact security and must be addressed on the road to modernization.

1. Process sensors, even newer models, have no built-in security and no passwords. In one recent example, a leading supplier just shipped 3,000 new sensors to the UAE without passwords.
2. IT network security vendors typically address security at Levels 2-7. This works for most IT networks. But OT threats frequently arrive via the Level 0-1 path, where the telemetry is not monitored and thus threats are not detected.
3. Ultimate ownership for OT security remains unclear. On paper, CISOs may be responsible, and many industrial organizations are moving to assign this accountability to CISOs. However, shop floor leaders own the space and typically do not easily release control to CISOs, given that CISOs often have a limited understanding of plant floor operations.
4. The Transportation Security Administration (TSA)'s pipeline cybersecurity guidelines do not address control systems, including sensors. Yet under the Cybersecurity and Infrastructure Security Agency (CISA), TSA owns the entire energy grid.
5. The American Petroleum Institute Standard 1164, Pipeline Control Systems Cybersecurity (August 2021) effectively excluded process sensors (Clause 6.6.5.4 (b) by stating, "Inventory should not include individual instruments that are not network connected."

Despite the value of tools such as the MITRE ATT&CK tool and the CVE methodology, more work is needed. For instance, the MITRE ATT&CK tool doesn't address process sensors and other control system field devices at all, and the CVE methodology for software vulnerabilities has no counterpart for control system hardware.

Making sense of today's standards - and addressing gaps within standards that are evolving more slowly than OT threats - is not for the faint of heart.

What's more, for secure Digital Transformation to succeed, IT and OT must commit to working together on deployment, security, and management of process changes. This ensures desired productivity improvements are ultimately realized and are also secure, reliable and compliant.

Common Digital Transformation Hurdles

There are common reasons companies fall short of their Digital Transformation goals. These issues can be amplified when transforming OT.

Legacy OT systems must move from island to mainland.

The 'Islands of Automation' in traditional OT infrastructure lack the foundations necessary to enable access to data. Additionally, industrial environments are poorly inventoried, leading to a lack of awareness regarding what is connected in the environment.

Process sensors, which are ubiquitous as the inputs to control and safety systems as well as to operator decisions, are not inherently secure. Catastrophic failures can occur. This has often meant that attention to safety, which is well understood by engineering organizations, has outrun the attention to security, which is something that the engineering organizations have tended to view as the responsibility of the IT organization.

In turn, IT organizations have tended to overlook process sensor security, seeing it as an engineering responsibility outside their own scope.

At the process sensor level, however, safety and security are really the same issue.

Misaligned or undefined strategy.

The Digital Transformation strategy must include coordinated efforts to set defined, measurable results for key business goals, while maintaining the security of the critical digital assets used and ensuring compliance with industry standards.

Roadmap does not create early value.

Developing a short and long-term roadmap for delivering value from Digital Transformation, guided by business outcomes and not just technology, is an essential foundation for a successful project.

Key stakeholders driving toward different objectives.

Digital Transformation requires a change in the culture of the organization. There must be alignment between the mindsets of IT and OT leaders in order for the two stakeholder groups to successfully drive the project's business objectives.

The first step is to identify and prioritize what needs to be protected in the organization - Data, Assets, Applications, and Services (DAAS).

A Closer Look at Process Sensors

Legacy systems operating for 20+ years are often not designed to operate in an IoT environment with thousands of process sensors, which presents security vulnerabilities. Without appropriate planning and controls, modernization efforts can multiply cybersecurity risks.

Why is securing process sensors so important?

According to a recent report: "Cybersecurity threats are increasing, and sensor data delivery could be hacked as a result. How hacked sensor data affects [building] control performance must be understood. A typical situation could include sensor data being modified by hackers and sent to the control loops, resulting in extreme control actions."

Some cyber-related incidents involving process sensors have included:

- Dam malfunctioned, collapse from erroneous low-level readings
- Sensor resulting in the release of 10 million gallons of untreated wastewater
- Safety relief valve in a nuclear plant did not lift because the pressure sensor never reached its setpoint
- One voltage sensor failure in a combined cycle plant in Florida caused a 200MW load swing at the plant that resulted in a 50MW load swing in New England
- Tank farm explosions from erroneous level sensor readings
- Airplane crashes from erroneous sensor readings
- Refinery explosion from erroneous sensor readings.

Process sensors with no cybersecurity, authentication, or cyber logging make it impossible to know whether incidents like these were malicious acts, made to look unintentional.

Three important security questions need to be asked to understand the vulnerabilities inherent in process sensors:

1. Do you need a physical presence to compromise the sensor?
   No, it can be done remotely.
2. How much harm can cyber-related sensor impacts cause?
   The field calibrator calibrates one sensor at a time, but connects insecurely to the Internet. Asset Management Systems (AMS) have access to thousands of sensors. Meanwhile, the AMS may have insecure connections to the Internet and often is connected to the corporate Enterprise Resource Planning (ERP) systems.
   A real example of a catastrophic failure from sensor issues: Colonial Pipeline.
3. What happens when compromised sensor data is sent to the cloud for big data analytics, IoT or Industry 4.0 applications?
   The sensor data is assumed to be uncompromised.

OT organizations need to address process sensor deficiencies as they undertake secure Digital Transformation programs, understanding how threat actors may interrupt, degrade, or possibly damage and destroy infrastructure; what the risks and costs are; and what steps can be taken to close vulnerabilities.

Zero Trust is an available strategy for removing excess trust and risk around process sensors. Zero Trust provides full visibility and continuous validation of the trustworthiness of each 'entity' in an enterprise, whether data, applications, services, or devices including process sensors, starting by assuming a trust level of zero.

Planning for Secure Digital Transformation

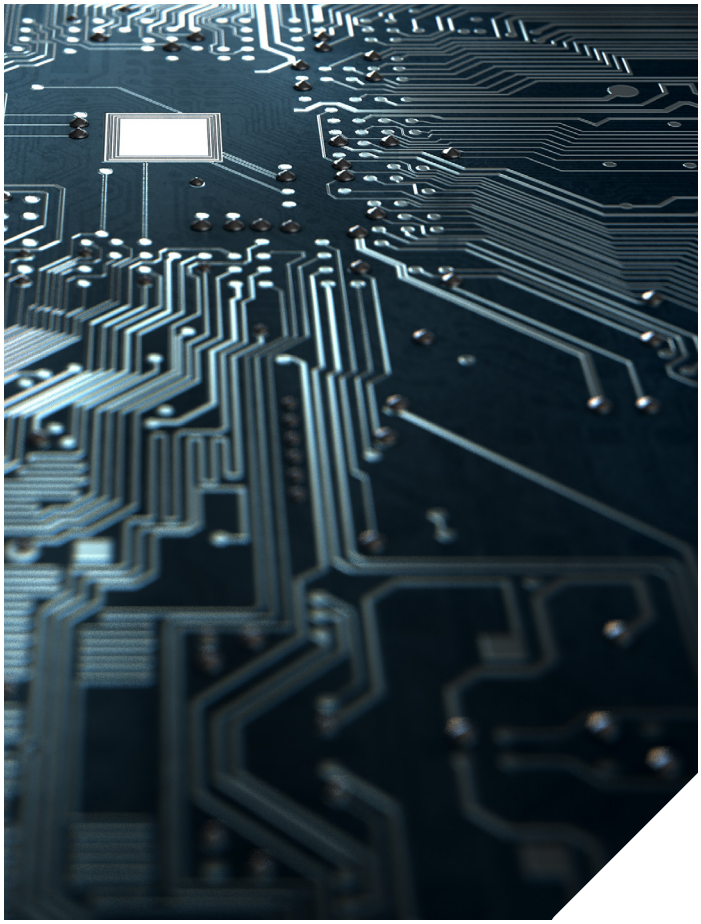
With all the secure Digital Transformation challenges that are magnified in OT environments, it's no wonder industrial organizations lag behind more IT-centric industries in modernizing.

The good news: there are proven paths to success.

Achieving secure Digital Transformation in OT involves a few key strategies:

- A Zero Trust approach
- The right modern digital solutions
- Changing ownership accountability within organizations
- Improving compliance standards around such common and vulnerable assets, like process sensors. And in lieu of these improvements, addressing gaps directly

While each of these points is important, the Zero Trust approach is now the focus of this discussion.



The Zero Trust Approach

Zero Trust is an excellent strategy for deploying secure Digital Transformation technologies in industrial environments. It supports new user populations, customer engagement models, rapid adoptions, and new IoT and OT devices and sensors as the transformation matures – all with cybersecurity protection.

Zero Trust is based on five design principles that can be integrated with the following five essential steps needed to drive secure Digital Transformation across an enterprise:

1. Define assets and protect surfaces
2. Map transaction flows
3. Design architecture
4. Enforce policy
5. Perform continuous monitoring and maintenance

Define Assets and Protect Surfaces. As John Kindervag, the originator of Zero Trust, states: "Zero Trust is a strategy for aligning business strategy with cybersecurity practices." By focusing on business outcomes, security can be seen as an enabler rather than an inhibitor.

The first step is to identify and prioritize what needs to be protected in the organization - Data, Assets, Applications, and Services (DAAS) elements. The DAAS elements are highly critical to the business, and each is prioritized. These are then considered protect surfaces, e.g. ICS controls, IT networks, customer information databases, intellectual property (IP) data and so forth.

- **Data**: Classify the data based on how important it is to your organization, how valuable it would be to hackers, and whether it's subject to regulations. Documenting a plan around data governance – overall and especially within a protect surface - means the organization can identify, classify, transmit, retain, and dispose of data with effective security controls in place.
- **Applications**: Understand which applications use sensitive data or proprietary code that may be of value to a threat actor. The design must be done from the inside out. Map how the systems should work and how various components of the DAAS element interact with other resources on the network. Understanding the way traffic moves across the network, specific to the data in the protect surface, will aid in the policy development for securing the data within and between applications.
- **Assets**: Create a detailed inventory of all your devices—laptops, cell phones, manufacturing equipment, PLCs, IoT devices like process sensors, and other network-connected assets—so you know what to include in your protect surface.
- **Services**: Identify all business-critical network services that need to be protected, such as Active Directory, DHCP, and email. Service accounts in general should have known behaviors and limited connection privileges. They should never directly attempt to access a domain controller or authentication system and any behavior anomalies should be quickly identified and escalated as they happen.

By focusing cybersecurity defenses around each protect surface, prioritized by its importance to the organization, defensible perimeters can be created that are orders of magnitude smaller and more manageable than the usual enterprise attack surface, which could be considered as the entire internet.

Each organization will encounter multiple Digital Transformation projects and accompanying protect surfaces. Starting with an initially smaller but strategic, impactful, and measurable transformation initiative can give the organization experience with implementing Zero Trust cybersecurity, and a framework for success for later projects.

Map Transaction Flows. Industrial environments are usually poorly inventoried in terms of network assets, leading to vulnerabilities regarding what should be – and what actually is - connected in the environment. These systems have often grown organically, producing frequent gaps in design knowledge; or presumed secure devices may provide unguarded internet entry points to networks.

To properly design a network, you must design it from the inside out. It's critical to understand how systems should work and how various DAAS components interact with other resources on the network. By mapping traffic flows and interdependencies, documenting how specific resources interact with each other, and working these interdependencies into security policies and controls, you are able to determine types and levels of protection needed.

Mapping transaction flows and DAAS interdependencies, specifically with regard to anything intersecting with your protect surfaces, enables better safeguards without accidentally breaking any related applications, services, or workflows. It also provides greater understanding and necessary information for more informed decisions in the next step.

Design Architecture. With the protect surface defined, and flows mapped, the necessary Zero Trust architecture will typically present itself.

Zero Trust best practices call for security controls to be placed as close as possible to the DAAS elements being protected. Otherwise, Zero Trust architecture is not based on some universal template. Instead, it leverages multiple types of cybersecurity tools and policies, specific to each protect surface, to achieve its aims. Organizations must deploy and integrate a combination of capabilities that enhance identity and access management, access controls, network segmentation, micro perimeters and more as required by the DAAS element in each protect surface.

Zero Trust network design should therefore be based on how transactions flow across a network, to and from protect surface DAAS elements, and take into account how users and applications access protect surface data. With an optimized flow in mind, decisions can be made as to where segmentation and micro perimeters should be placed, using physical and/or virtual appliances.

Enforce Policy. In this fourth step, policy rules are written for the segmentation gateway based on the expected behavior of the data and the user or applications interacting with that data.

Once the design team has determined the optimum traffic flow, the next step is determining how to enforce access control and inspection policies at the segmentation gateway. Policy should start with a coarse-grained approach and become more granular as a greater understanding of user needs and business requirements

emerge, as the Digital Transformation matures and business insight develops.

A key principle of Zero Trust is limiting access to a need-to-know basis – the principle of least privilege - and applying strict enforcement of this access control. To define these rules, the design team must have a detailed understanding of which users have access to what data, along with contextual information.

It's no longer enough to know the source address, destination address, port, and protocol. Security teams need to understand the asserted user identity as well as the application, which will often serve as a proxy for the data type in the modern segmentation gateway.

For one resource to talk to another, a specific rule must allow that traffic. Developing that rule entails answering the following:

- Who should have access? This defines the 'asserted identity.'
- What application to what resource? What application is the asserted identity using to access a resource inside the protect surface?
- When should the user have access? When is the attempt to access the resource being made?
- From where should they have access? Where is the data packet destination?
- Why are we doing this? Why is this packet trying to access this resource within the protect surface? This relates to data classification, where metadata automatically ingested from data classification tools helps make your policy more granular.
- How should we protect it? In order to protect it, you must understand how the asserted identity of a packet is accessing the protect surface via a specific application.

Continuous Monitoring and Maintenance. This is the fifth step in the implementation of the Zero Trust approach.

This iterative process means continuously looking at all internal and external logs through Layer 7, focusing on the operational aspects of Zero Trust. By sending as much telemetry as possible about the environment, new insights will be gained regarding how to improve security and efficiency over time, as well as to develop useful insights for transforming new areas.

Technology environments are subject to myriad threats. Enterprises must maintain a continuous monitoring capability to ensure they are aware of what is occurring within their environments. Then, the more a network is attacked, the stronger it will become, due to making policies more secure and informing iterative designs with architectural tweaks that further enhance security

Industrial Security Standards

OT industries are guided by four primary security standards.

- IEC 62443 Industrial Automation and Control Systems (IAC) Security
- Department of Homeland Security/The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- NIST 800-82 Industrial – National Institute of Standards and Technology
- Department of Homeland Security/Idaho National Lab

Each is based on a Defense-in-Depth security architecture that in itself has vulnerabilities. What's more, these standards are not actually a strategy, but more a deployment of tactics to address specific point vulnerabilities through a control or product solution, based on the Industrial Demilitarized Zone concept (IDMZ) - a boundary, buffer or 'air gap' within a manufacturing or process facility between the organization's business systems and the industrial control systems with different security requirements, and sharing no inherent trust in each other.

Digital Transformation alters the trust factor for both systems. Trust, today, must be observant, contextual, and adaptive if the interaction of the new business models developed through the Digital Transformation are to succeed and provide the anticipated positive results.

Rockwell Automation aligns to the IEC 62443 Industrial Automation and Controls Systems (IACS) security standard, as well as to the Zero Trust approach. Zero Trust design principles map well to IEC 62443 requirements, simplifying compliance while strengthening defenses against a continuously evolving threat environment.

Summary

Secure Digital Transformation in OT can leverage Zero Trust as a key framework for ensuring that transformation projects are launched with appropriate cybersecurity protection in place.

Both Zero Trust and secure Digital Transformation are journeys that should be incrementally implemented. Because Digital Transformation alters the trust factor between the industrial control systems and business systems, a plan to achieve a secure Digital Transformation should be executed using complementary strategies for achieving improved efficiency and increased productivity, with full cybersecurity visibility and enforcement that extends across every point of connection on the network.

The planning of an initial Secure Digital Transformation project, and identifying, prioritizing and protecting the DAAS elements within each protect surface in the project, will aid the organization in realizing early value from their efforts and sets up a pattern of cybersecurity safeguards to protect the organization during transformation.

Putting it All Together

Rockwell Automation is highly skilled in Secure Digital Transformation within complex OT environments. Call upon our expertise to help you design, implement and monitor your organization's projects for greater operational rewards, ensuring the right cybersecurity protections are in place from planning through production.

Take action

Learn more about Secure Digital Transformation.

Learn more about Zero Trust in OT cybersecurity.

Speak to an expert about how to get started.

Connect with us.

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-WP003A-EN-P - May 2022