Insights

Factory of the Future

Intel shares its insights into protecting critical infrastructure and industrial control systems.

intel Security

Introducing security into factories requires tight integration of information security *and* industrial control system expertise to address both information technology (IT) and operational technology (OT) risks and needs. The convergence of IT and OT is expanding the management responsibilities of CISOs and will require reshaping enterprise security practices, addressing gaps in skill sets, and bridging the cultural divide between teams that have traditionally approached security differently. Ultimately, IT and OT can work together on architecture, governance, compliance, management, and technology to secure factories.

Overview

This paper discusses, in a question-and-answer format, insights shared by Vice President and Chief Security and Privacy Officer (CSPO) Malcolm Harkins and team members at Intel Corporation and Intel Security (McAfee. Part of Intel Security.) on the process of reshaping security for its fabrication plant infrastructure.

Below is an interview with Malcolm Harkins

What was the catalyst that led Intel IT to embark on the journey to protecting the facilities and industrial systems in your fabrication plants?

Our journey started in 2002, when Intel created the Intel Security Taskforce. The previous year, a high-profile exploit first brought the potential risk to our attention and to the attention of anyone with critical infrastructure and industrial controls. As security professionals, we quickly realized that all systems with connectivity to a network or the Internet must be protected from cyberthreats or insider attacks. We began monitoring risks and threats in the landscape and observed an increase of cyberactivity and liability issues in industries such as financial services. Additionally, we recognized the need to be ahead of government regulations, frameworks, and standards.

In what timeframe did you formally prioritize securing industrial control systems (ICS)?

We developed an entire program around manufacturing that focused on availability because any change introduces risk to factories. During 2001 to 2005, we had crude network isolation, with some patching and staging and limited downtime and maintenance windows. By 2005 and through 2011, we saw a maturation of vulnerabilities and threats, which put industrial control systems on the risk map. We watched predictions come true (for example, Stuxnet). We further hardened our systems, layered network isolation zones, and applied varying degree of defense-in-depth security controls, such as enterprise virus scanning, intrusion detection systems, platform hardening, and restrictive access where feasible.

In 2012, as part of our annual Enterprise Risk Management Assessment to the board of directors, we outlined a multiyear plan, with year one being foundation-based and year two being execution-based. With the risk assessment in hand, which included data about the material and collateral damage if a factory were to be partially or entirely compromised, we campaigned internally to various stakeholders, including the operations team on the findings and recommendations.

What type of information security mandate existed previously, and how had the groups (IT and OT) operated?

It was different compared with our enterprise IT security mandates and policies. Industrial controls and the people and processes to support them have been synonymous with high-availability mandates. A typical security professional does not have the day-to-day understanding of manufacturing or industrial controls expertise. Our priorities and operating models differed and more traditionally relied on network controls.

"As operators, we gained the visibility and information on actual attacks (for example, Stuxnet), which also helped us to build common knowledge towards consensus among (ourselves) ICS technicians."

—Dennis Clinefelter
ICS team member

Initially, the critical control systems never came directly under IT management. Systems were managed and instrumented by a combination of factory employees and, in some cases, our suppliers. For example, a one-time installation, such as a gas control, is generally performed by a supplier and tied to a single-use workstation. Operations team have always had high availability in mind, with low/no downtime mandates. However cybersecurity was not as significant a concern as it is today.

How did you build consensus internally to bring security into a plant?
First, IT staff toured a factory plant. It was the most valuable activity for understanding factory operations and priorities. Internally, we approached senior leaders in the company to educate and drive awareness of specific risks. We leveraged Intel Security experts who had a deep understanding of the techniques that could be used to access industrial systems. For example, we showed a live demonstration of how, with only a few freely available tools from the Internet and a tablet, a utility-based system could be compromised in just a matter of minutes.

We also created a role-play exercise with the operators of the systems to get them involved and help change their mindset. Once the context of the exercise was set, the technicians and operators came up with numerous ideas to compromise the systems when they played the part of black hats (bad guys).

All of these tactics contributed to a turning point in the effort to align everyone and build trust, belief, and a sense of shared knowledge. But concerns about the impact that any perceived downtime could have on our business performance still lingered.

What did the process technicians and control engineers from OT learn about/from IT during the process?
Several members of the ICS operations team cited the advantages of securing systems. By participating in the process, including asset inventory exercises and segregating and securing control networks, they were able to realize how these improvements make an entire factory operation better. Additionally, they had acquired specific information on what kinds/types of exploits could be involved and had more awareness of insider attacks and human error, and the various kinds of potential impacts on isolated networks (for example, outages). The partnership with IT provided critical insights on devices and impacted systems, timely intelligence about something that could potentially or is in the process of affecting their environment, and a better connection to incident response procedures.

How did you approach changing the support and management of supervisory control and data acquisition (SCADA) systems from local sites to a global model?
Up until 2009, manufacturing was managed in one business unit—locally at sites. Control systems network(s) were managed by IT, but the on-site systems were not.

Gradually, some of the manufacturing systems, such as the hosts/clients and servers at local sites, were transitioned to IT, and the security teams led until we reached a maturation point and blending of common goals. We also helped IT provide the factories with the services they needed to help make them more efficient.

Our global support strategy included a design for a new network architecture that is secure in deployment, zoned for appropriate uses, and managed by our security operations center (SOC). The strategy does not put a burden on operations to meet our security controls nor does it affect the performance of the industrial systems already in the field and new fabrication plants that we have been building.

"A contributing factor to the success of the collaboration by the task force was having the funding and skilled resources that understand factory needs made available to implement security improvements."

—Janelle Klaser
ICS team member

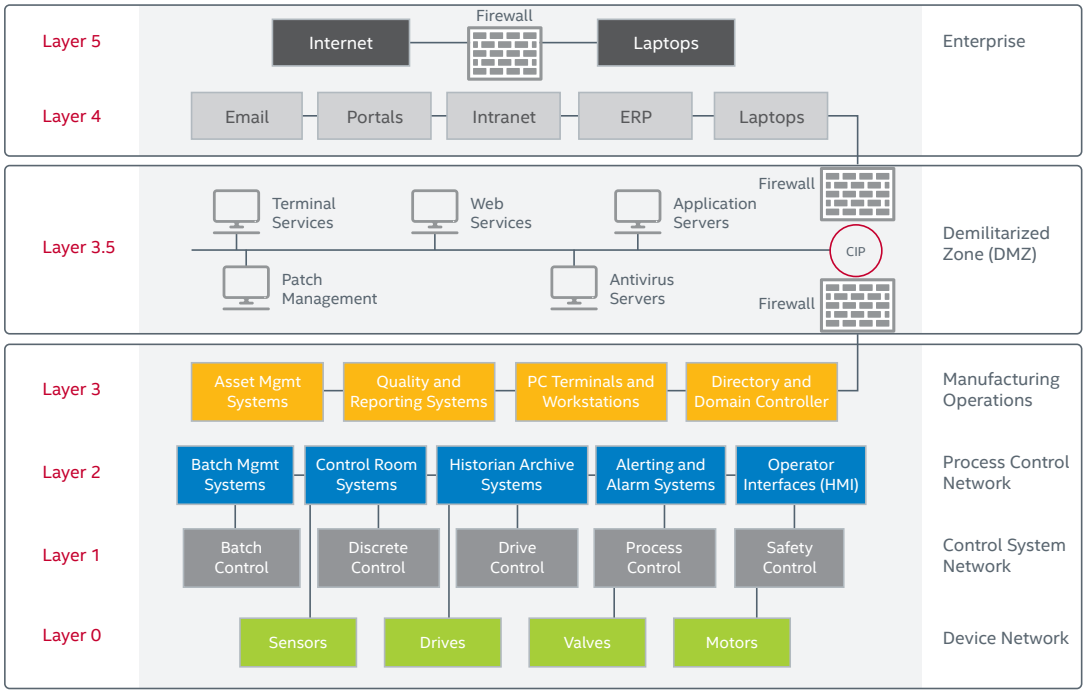

Figure 1. High-level design based on the Purdue model.

How did Intel identify core functions to secure and scope the massive undertaking into achievable phases?

Broadly, an attack against our ICS environment could compromise our manufacturing ability and/or pose a safety risk to our employees and the community.[1]

Either one of these would pose a materially significant risk to the company, and for these obvious reasons, ICS was added to the enterprise risk map. We wanted to avoid both these possibilities, so ICS was added to the enterprise risk map. We already were aware of the impact to the company if a factory's yield were to be contaminated.

Intel targeted three core functions, as a representative sample, to be prioritized in the first phase:

- Facilities monitoring systems (FMS).
- Hazardous production material (HPM) and life safety systems (LSS).
- Bulk chemical distribution systems (BCDS).

Once we inventoried, assessed, and categorized the risks and threat levels, we were able to set a corporate standard for our layered defense strategy. The corporate standard security requirements are for Intel and its suppliers.

For organizations without a chemical component, for example, it could easily be conveyor systems, washing and cleaning systems, or any other components or system needed to make products in any industry. Organizations may use different terminology, but the criticality and regulatory handling of the functions can be very similar to ours.[2]

"I became proactive once armed with security knowledge. ICS operations teams should take the time and re-evaluate their systems and documentation."

—Janelle Klaser
ICS team member

How were you able to gain support from the broader information security and industrial controls ecosystem?
Factors related to suppliers and vendors were rated high on our risk assessment. Suppliers and vendors in the broader ecosystem had also come together to identify the protocols, systems, and technologies that they would support. We have actively driven improvements and requirements in several ways.

- Working directly with and leveraging the expertise of the largest software security vendor, Intel Security Group (formerly McAfee, now part of Intel Security), and partnering with global leaders in industrial controls, such as Siemens.
- Evaluating contract language against the way other IT services are defined and working with suppliers and vendors on definitions.
- Providing requirements to our suppliers and vendors so they know our expectations for retrofitting existing systems and developing new factories in the future.
- Documenting the business processes and mechanisms to improve how we deal with change and risks, as well as how we balance decisions between output of product and responding to a particular risk.

At Intel, we have designed processes to be variable so that they are implemented on a case-by-case basis. This offers flexibility in decision-making. For example:

Is there an availability risk?	*Yes/No*
Can the threat take the system offline?	*Yes/No*
Is there a safety risk?	*Yes/No*
Can I manage taking the system offline to prevent it?	*Yes/No*

Since embarking on this journey, what does 2014 look like for Intel in terms of the kinds of security controls and capabilities that will be implemented?
With high availability a core requirement in ICS, we have scrutinized and selected technologies and partners that are committed to security and understand our unique manufacturing needs. This includes a range of support network security, isolation, zones, locking down workstations (hosts), and those offering out-of-the-box (OOTB) industrial protocol support, integration support, and managed services alternatives.

For organizations struggling to secure and protect critical infrastructure and industrial control systems, what lesson or advice would you offer?

- Accountability and ownership is a shared responsibility between factories, manufacturing, operations, IT, and management.
- Tour a factory or manufacturing facility before embarking on a comprehensive security strategy plan to protect critical infrastructure and industrial control systems.
- Take training offered by the Idaho National Laboratory on SCADA security, or perform joint workshop activities geared to building expertise across IT and OT functions/knowledge.
- Seek out the key players in your manufacturing groups and industrial system controls and involve them in briefings and activities.
- Run risk assessments with the people most educated on the operational systems and information security together.
- Plan in phases, targeting core functions that are achievable and time-bound, leveraging frameworks by NIST[3] and network architecture design from Purdue.[4]

- Become proactive once armed with knowledge. OT should take the time to re-evaluate their systems and documentation. You do not have to wait. For example, Siemens ACM equipment already has security features and the option to configure it exists today.
- Demand security. For organizations or institutions on this journey, you need to start demanding that security be built into ICS and that information security vendors are continually integrating their roadmaps to stay current with mitigation and management. This includes evaluating vendors for turnkey security software and security compliant hardware.

"Risk surrounds and envelopes us. Without understanding it, we risk everything, and without capitalising on it, we gain nothing."

—Glynis Breakwell
The Psychology of Risk

Contributors

Malcolm Harkins, VP and CSPO of Intel
As vice president and chief security and privacy officer (CSPO) at Intel Corporation, Malcolm Harkins is responsible for managing risk, controls, privacy, security, and other related compliance activities for Intel's information assets, products, and services. This responsibility includes protecting industrial control systems and the critical infrastructure of Intel's fabrication plants around the world.

Additional contributors:

Dennis Clinefelter, FMS ICS, Intel

David Hatchell, Intel Security (McAfee. Part of Intel Security.)

Janelle Klaser, HPM/LSS, Intel

Kim Owens, Information Security Specialist, Intel

Nicolaus Rock, BCDS ICS, Intel

Carla Roncato, Intel Security (McAfee. Part of Intel Security.)

Sachin Shah, Senior Security Strategist for ICS Systems, Intel

1. Visit **http://exploreintel.com/** to learn more about Intel's environmental performance.
2. **http://www.dhs.gov/critical-infrastructure-sectors**
3. **http://csrc.nist.gov/groups/SMA/fisma/ics/index.html**
4. **http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.pdf**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com