ARC VIEW

JANUARY 26, 2023

Critical Infrastructure Operators and Suppliers Need Cyber-Physical Cybersecurity Strategies

By Sid Snitkin

Keywords

Critical Infrastructure, Cyber-Physical Systems, Cybersecurity, Deloitte

Overview

Society depends on the safe, reliable and secure operation of critical infrastructure, such as power and water systems, healthcare, transportation, and buildings, as well as producers of basic commodities that include: food, fuels, and chemicals. The significant impact of any disruption demands comprehensive cybersecurity strategies that cover the systems and devices that automate and control this infrastructure.

Critical infrastructure operators need comprehensive security programs that can manage cyber risks across the full spectrum of OT, IT, IoT, and IIoT technologies.

The risks of serious critical infrastructure cyber incidents have grown significantly. Critical infrastructure has become a prime target for ransomware and sophisticated nation state attacks. At the same time, integration of operational technology (OT), information technology (IT), and cloud systems are proliferating attack pathways. Vulnerabilities are likewise exploding with the proliferation of internet of things (IoT) and Industrial IoT (IIoT) devices and expanded use of remote access.

While many critical infrastructure operations already have cyber defenses, most were built for yesterday's technology and threat environments. Today these assets are controlled by sophisticated systems that integrate IT, OT, IoT and IIoT and demand more comprehensive cybersecurity programs that can manage risks across each of these technologies.

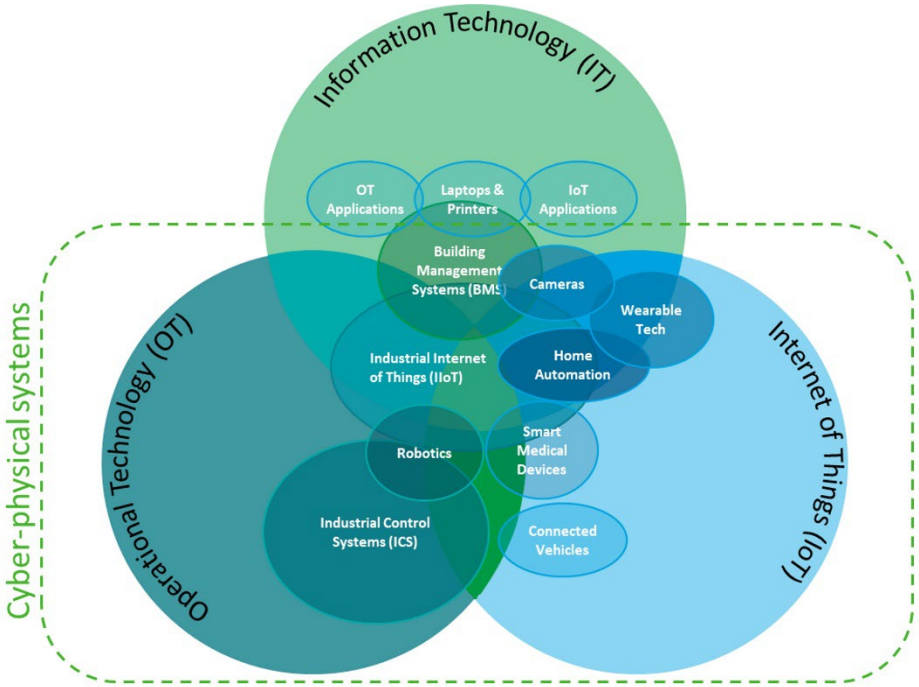
Recently, ARC Advisory Group discussed these issues with executives from Deloitte & Touche LLP (Deloitte). This demonstrated the company's deep understanding and experience in critical infrastructure security and their extensive capabilities to help operators and vendors address their OT, IT, IoT,

and IIoT security risks. A brief overview of their security offerings is included in this report.

Cyber-Physical Security Risks Are Growing

Energy companies invest in new capabilities to satisfy growing demands for clean energy and sustainable resources. Manufacturers invest in new practices to satisfy customer demands for low cost, eco-friendly products. Logistics companies build new, automated facilities to keep pace with changes in global commerce. Life science and healthcare companies invest in new diagnostic and delivery systems to satisfy privacy requirements and ensure proper patient care. Facility and smart city managers upgrade systems with new technologies to keep people safe and comfortable.

What do all these developments have in common? They all rely on cyber-physical systems that interact with or control the physical world. Furthermore, these systems are vulnerable to cyber incidents with serious consequences to health, safety, environment, and business continuity.



Cyber-Physical Systems Integrate IT, OT, and IoT Technology

Cyber-Physical Systems, or CPS, are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users), and support real-time, guaranteed performance in safety-critical applications.[1] In the big scheme of things, CPS contain elements of IT, OT, and IoT systems. Other names may be used to describe specific applications within those areas, such as smart medical devices, robotics, or building management systems. Regardless, they all fall under the general category of CPS.

Security of CPS is particularly important as a compromise in any element could lead to safety incidents, damaged equipment, and costly operational disruptions. At the same time, the complexity and widespread use of CPS presents new challenges for cybersecurity teams. For example, some critical industries, like healthcare and smart cities, may not have OT security teams and their IT security teams often lack the expertise to secure traditional and embedded control systems. Industries with OT security teams may lack the resources and expertise to support the new technologies used in CPS. Most cybersecurity teams may also lack the ability to control security within the many IoT devices that are being used in CPS.

Critical infrastructure operators and suppliers need comprehensive security strategies to manage these growing CPS security risks. Every asset and communication path needs to be identified and a plan developed to ensure that the associated risks are appropriately mitigated. Organizations also need to address the cultural barriers that often develop around siloed cybersecurity programs to help ensure the efficiency and effectiveness of cybersecurity defenses. Development of governance and security agreements with suppliers in CPS ecosystems will also be needed to ensure that security policies are enforced across key lifecycle stages including:

- The design of cyber-physical devices and products.
- The manufacture and distribution of CPS.
- The integration of CPS into systems and ecosystems.
- The support of internal and external systems and services.

[1] NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things

Developing such a comprehensive program can be daunting, but its importance cannot be overstated. The risks for critical infrastructure operators are simply too large to ignore or be delayed by lack of resources.

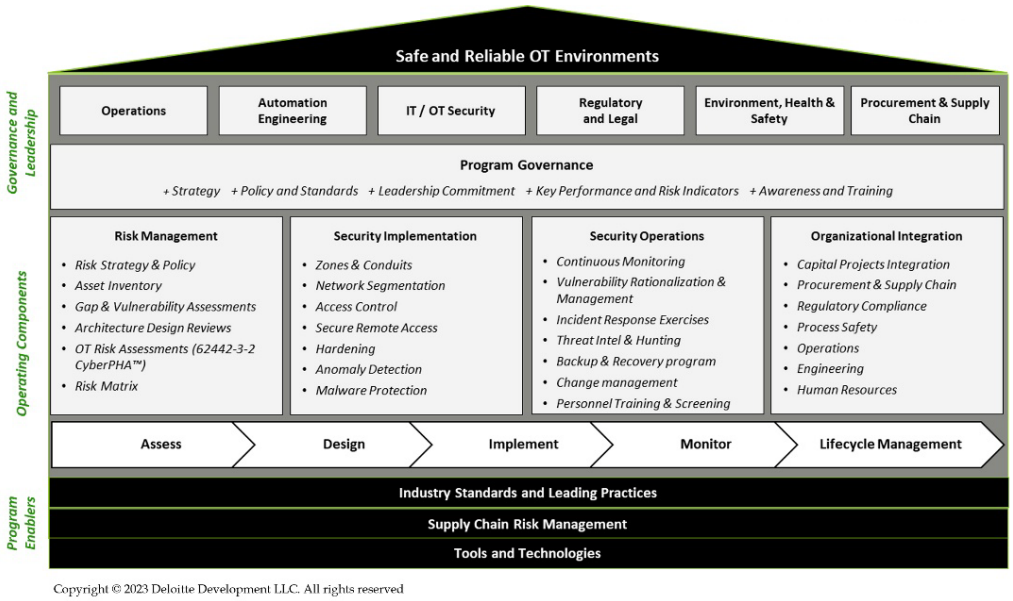
Deloitte CPS Security Offerings

Deloitte is well-known for their IT cybersecurity capabilities and the wide range of services they offer to help companies develop, maintain, and manage cybersecurity programs. What is less known is that Deloitte offers comparable cybersecurity capabilities for cyber-physical products and systems such as OT, IoT, and IIoT.

Deloitte's OT, IoT and Product Security practice is focused on helping clients identify and manage risks to CPS. Globally, this practice has over 400 CPS, OT, IoT and Product Security cybersecurity subject matter specialists with practical industrial control systems (ICS), product security and IoT experience across a variety of industries. Deloitte's CPS cybersecurity team members also act as leaders in OT and IoT cybersecurity standards development efforts, including ISA/IEC 62443, API 1164, and the NIST Cybersecurity Framework. They also actively participate in industry associations and conferences on product security, OT, and IoT cybersecurity.

The company advised ARC that they have executed over 1,000 OT or IoT cybersecurity projects in the last 5 years and OT/IoT visibility and monitoring solutions have been deployed at over 270 global sites. They also state that 95 percent of the Fortune 500 Energy companies are Deloitte clients and that they've established over 20 alliances with OT and IoT cybersecurity suppliers.

Deloitte's CPS cybersecurity practice is based on frameworks for developing enterprise-wide strategies to deal with the many challenges their clients are facing with cyber-physical system security. The following framework for OT Security is an example of the broad nature of Deloitte's frameworks. The company has similar frameworks for IoT and Product Security.



Deloitte OT Security Program framework

Deloitte offers a wide range of services that critical infrastructure operators and CPS developers can leverage to develop, implement and manage the security of their operations and products. This includes:

Users of CPS

- OT/IoT security program maturity assessment
- OT/IoT security program design, development, implementation, and operation
- OT/IoT monitoring technology selection, deployment, optimization, and management
- OT/IoT managed security services
- OT/IoT security risk assessments
- OT/IoT attack path analysis
- OT/IoT vulnerability rationalization and management
- OT/IoT regulatory compliance and readiness support
- OT/IoT system security testing

Developers of Cyber-Physical Devices and Products

- Product security program maturity assessment

- Product security program design, development, implementation, and operation
- Secure development support
- Product security risk assessment
- Product security testing
- Regional compliance support
- Product Security Manager™ customization, deployment, and support
- Regulatory submissions support
- Post market security risk management

Conclusion

Insufficient CPS security represents a serious threat to the safety and profitability of critical infrastructure around the world. The diversity of physical and cyber assets used in these systems have outpaced the capabilities of most internal cybersecurity programs. No company can afford to ignore these growing risks of serious cyber incidents.

This ARC report discussed the challenges of CPS security and the need for new, comprehensive strategies to ensure that security is properly addressed across cyber-physical supply chains. Operators may not control all the components, but they will suffer the brunt of any incidents.

As the discussion of Deloitte's IT, OT, IoT, and IIoT cybersecurity capabilities illustrates, there are companies that understand the full scope of risks and can help you build and implement an effective strategy. So, the biggest risk critical infrastructure operators face is to ignore the urgency of addressing these critical security issues.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. Specific questions for Deloitte may be directed to cyberiotandot@deloitte.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.