Deloitte.

Future forward readiness

Cyber Physical Systems (CPS)

Securing Internet of Things (IOT) and Operational Technology (OT) - Products, Systems and Ecosystems

What do medical devices, autonomous vehicles, smart buildings, and industrial control systems have in common? They are smart devices or systems that interact with or control the physical world. This interaction makes them vulnerable to cyber incidents and the consequences can have serious health, safety, environmental, or business implications.

CPS are smart systems that include engineered interacting networks of physical and computational components. They go by a lot of other names depending on the industry and the application so it can get quite confusing. In the big scheme of things, there are IT systems, OT systems, and IoT systems.

Current Trends

Connected device visibility and security will be a major area of focus for many organizations

"Leading organizations will focus in the year ahead on connected device cyber practices by establishing or updating related policies and procedures, updating inventories of their IoT-connected devices, monitoring and patching devices, honing both device procurement and disposal practices with security in mind, correlating IoT and IT networks, monitoring connected devices more closely to further secure those endpoints, manage vulnerabilities, and respond to incidents."
— Deloitte's US Cyber IoT leader, Wendy Frank

Security in emerging technologies will be critical for their adoption

"Adoption of these technologies will be instrumental to manage an organization's strategic growth initiatives, however, their sustained success will be based on the organization's ability to navigate and implement appropriate technology security measures."
— Deloitte's US Transformation & Emerging Technology leader in cyber & strategic risk, Kieran Norton

Complex supply chain security risks will continue to emerge

""Today's hyperconnected global economy has driven organizations to heavily depend on their supply chains — from the components within their physical and digital products to the services they require to run their day-to-day operations. This critical interdependence makes supply chain security and risk transformation an imperative for today's globally connected businesses.
— Deloitte US Cyber Risk Secure Supply Chain leader, Sharon Chand

Desired outcomes

Cyber-physical security can yield several benefits, including:

Reduced risk of security incidents that could lead to health, safety, or environmental impacts, business interruption, or loss of data (e.g., personal data and intellectual property) which could result in damage to your organization, as well as regulatory and legal penalties.

Improved compliance with regulations and security standards requiring that organizations have cyber risk measures and mitigation plans in place.

Increased market acceptance meeting customer demands where they are going and not just where they are at today.

Increased perception as a CPS market leader through early adoption and preparedness against emerging threats and sharing of information.

Improved visibility into the assets you have, their location and security posture, and the software components that they comprise.

Future Forward Readiness

Deloitte can help you achieve an enhanced security posture as threats and disruptions grow. With services across the advise, implement, and operate spectrum, Deloitte can help forge a better balance between safety, security, quality, and usability to maintain the security of the products you manufacture and the environments you operate.

Cyber IoT in action

Medical Device Security

Deloitte works with medical device manufacturers for devices ranging from small glucose monitors or software as a medical device to implantable devices to large image and diagnostic equipment to embed security throughout their product lifecycle, both in development and in operations.

Vehicle Security

Deloitte works with vehicle Original Equipment Manufacturers (OEMs) and suppliers to embed security throughout development lifecycle of sourced vehicle parts and into the integration and customization of those parts by the OEM. Deloitte also works with suppliers to embed security into the products that they sell to OEMs, which are used within a vehicle.

Industrial Controls Systems (ICS)

Deloitte works with manufacturers of ICS that are used across industrial environments (e.g., factories, distribution, refineries, pipelines) to secure the equipment by design. In addition, Deloitte works with companies" ICS-to securely govern, architect, implement, and operate environments.

OT Security

Deloitte works with companies across industries that own and/or operate industrial facilities to help them securely govern, architect, implement, and monitor their operations to remain online, resilient, and secure.

Smart Buildings and Campuses

Deloitte works with IoT product manufacturers for devices ranging from HVAC and physical security to digital twins to embed security throughout their product lifecycle, both in development and in operations. In addition, Deloitte works with companies that operate IoT to securely govern, architect, implement, and operate the IoT environment.

Smart Cities and Agriculture

Deloitte works with smart city and agriculture product manufacturers to embed security throughout their product lifecycle, both in development and in operations. In addition, Deloitte works with companies that operate smart city and agriculture equipment to securely govern, architect, implement, and operate the environment.

Turn complex challenges into opportunities

Our industry-tailored approach enables us to apply the right solutions to your precise business challenges.

When you're looking for global leadership

Deloitte is recognized as a global leader in the OT and IoT cybersecurity market. With our strong experience, we support the world's largest companies with their product security, OT security, and IoT security needs.

When you need a strong ecosystem of collaborators and alliances

We have strong alliances with leading technology vendors, and work with industry associations, academia, and government agencies to provide leading insights, share intelligence, and collaborate.

When you need a one-stop shop

While navigating the uncertainty of cyber-physical security, the breadth of our services allows us to provide you with an expansive solution to help you move forward and achieve the outcomes most critical to your organization.

We're well positioned to help you achieve your objectives

Wherever you are in your journey, we have the experience, knowledge, and tools to help move your organization forward.

Outcomes-driven

In the face of growing complexity, we make finding a cyber physical system provider easy. Our breadth and depth allow us to provide the outcomes (and value) you seek as a trusted advisor, a technology-savvy pioneer, a visionary integrator, and a dependable operator. We connect the dots, so you don't have to—helping you to improve security, trust, and resilience.

Quality-oriented

We bring together a powerful combination of proprietary technology, domain experience, leading alliances, and industry knowledge to deliver better. Our obsession with quality means we consistently work to help you realize your vision, because preventing and mitigating cyber physical system risks are mission critical.

Value-focused

We act as a leader in times of crisis, a teammate to help you navigate change, and a force to have your back when you are on the front lines. We create value for our clients beyond the deal, pioneering cutting edge resources and innovation, paving the way for forward leaning collaboration, and leading bold thinking on tomorrow's emerging technologies so you can turn risks into opportunities.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.
As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Future forward readiness

Cyber IoT in action

Product Security

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

OT Security

- OT security program design, development, implementation
- OT security program maturity assessment.
- OT security vulnerability rationalization and management
- OT security design and implementation
- OT Security regulatory compliance and readiness
- OT security tool evaluation
- OT security detection tool architecture, deployment, and configuration
- OT security training
- OT managed security services

IoT Security

- IoT security program design, development, implementation
- IoT security program maturity assessment
- IoT security vulnerability rationalization and management
- IoT security design and implementation
- IoT security regulatory compliance and readiness
- IoT technology and support
- IoT system security testing
- IoT managed security services

Engineered for

- Organizations that design cyber-physical devices and products
- Organizations that manufacture, distribute and maintain CPS
- Organizations that integrate CPS into systems and ecosystems
- Organizations that rely on ICS and OT for safe and reliable operations
- Organizations deploying IoT or Industrial Internet of Things (IIoT) to transform and optimize their business
- Organizations responsible for management of smart facilities

Start the conversation

Wendy Frank
Principal, Cyber IoT Practice Leader
Deloitte and Touch LLP
wfrank@deloitte.com

Russell Jones
Partner, OT Security Leader
Deloitte and Touch LLP
rujones@deloitte.com

Veronica Lim
Principal, Product Security Leader
Deloitte and Touch LLP
vlim@deloitte.com

Ramsey Hajj
Principal, OT Security Leader
Deloitte and Touch LLP
rhajj@deloitte.com

John Cusimano
Managing Director, OT Security Leader
Deloitte and Touch LLP
jcusimano@deloitte.com

Sara Weiland
Managing Director, IoT Security Leader
Deloitte and Touch LLP
sweiland@deloitte.com