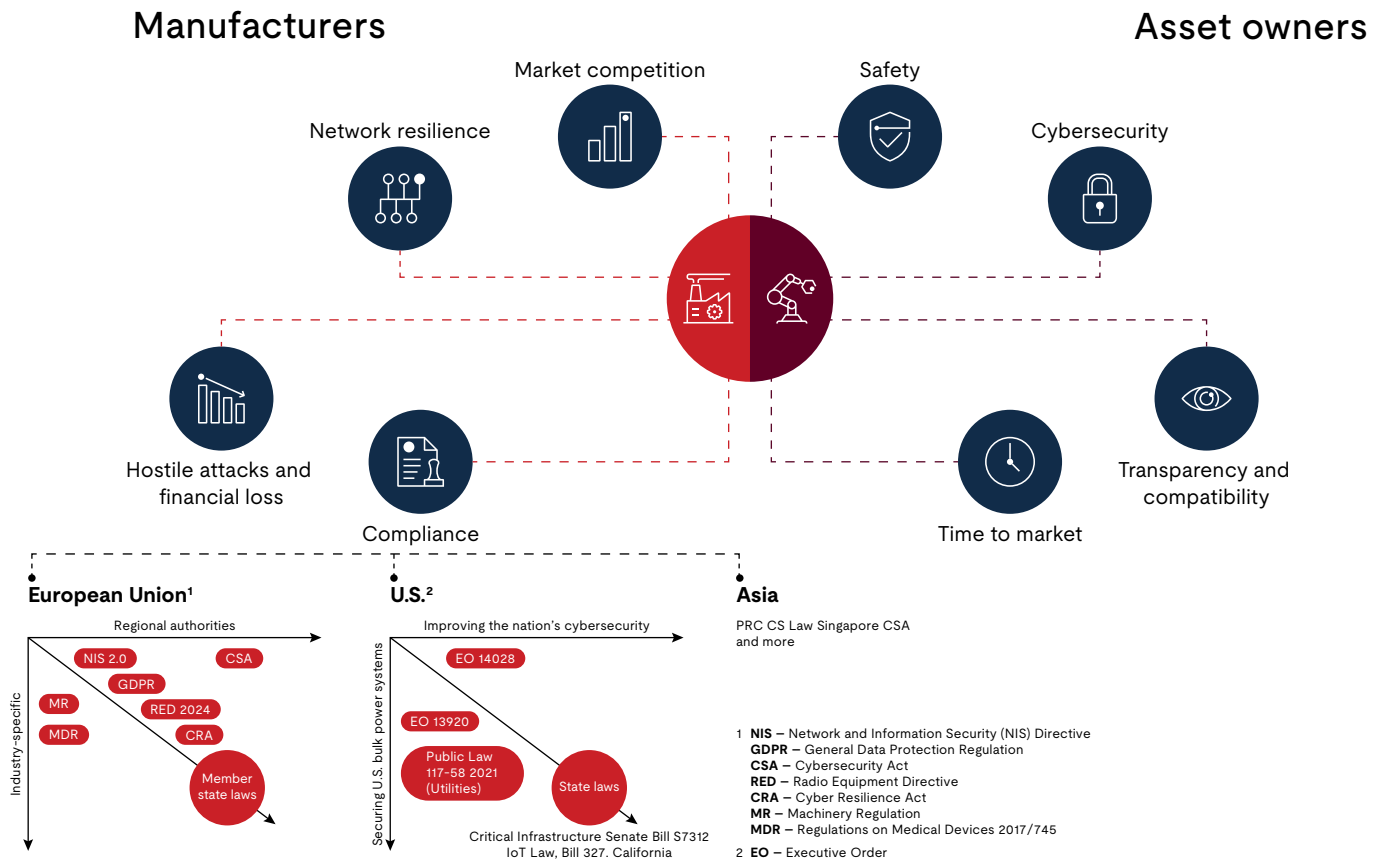# Industrial Cybersecurity

Industry 4.0 introduces increased cybersecurity risks

Smart manufacturing and smart factories depend on connectivity and data sharing to deliver Industry 4.0 benefits — increased operating productivity, enhanced safety, and reduced downtime and costs. However, critical connected systems are an attractive target for cybercriminals in search of a potentially profitable opportunity to exploit.
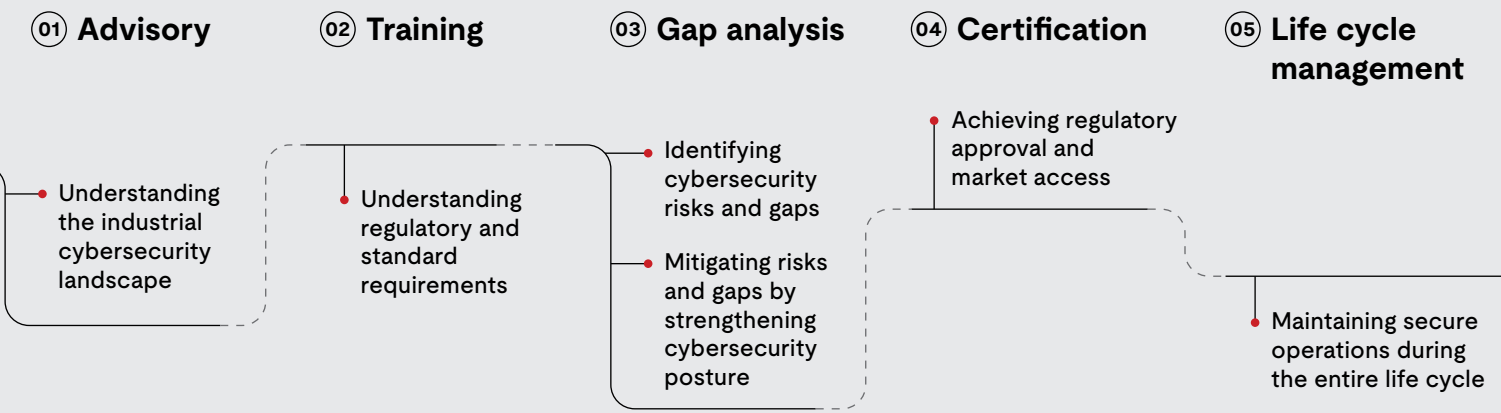
Industrial Internet of Things (IIoT) systems can prove particularly difficult to secure. Each device added to the network creates a new potential risk. Factor in the inherent complexity of large automated systems and the fact that malicious hackers potentially only need to find one vulnerability to gain access to the entire network, and the challenge becomes clear.

Industrial cybersecurity trends and challenges

Manufacturers

Asset owners

Market competition

Safety

Network resilience

Cybersecurity

Hostile attacks and financial loss

Transparency and compatibility

Compliance

Time to market

Collaborate with UL Solutions

Your cybersecurity journey along the industrial product development life cycle

01 Advisory

Understanding the industrial cybersecurity landscape

02 Training

Understanding regulatory and standard requirements

03 Gap analysis

Identifying cybersecurity risks and gaps

Mitigating risks and gaps by strengthening cybersecurity posture

04 Certification

Achieving regulatory approval and market access

05 Life cycle management

Maintaining secure operations during the entire life cycle

Time to market

Benchmarking

Brand protection

Risk and cost control
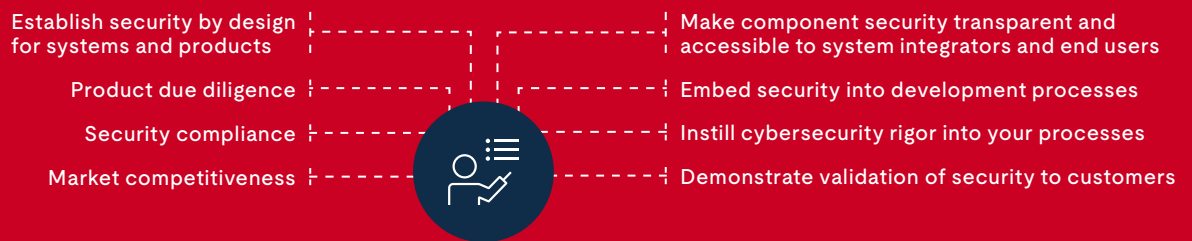
Industry 4.0 cybersecurity services

- Understand and mitigate the particular risks associated with Industry 4.0.
- Identify gaps and deploy a risk-based cybersecurity approach as an integral part of business strategy and operations.

- For component and product manufacturers, system integrators, and asset owners - from product security to operational technology security

---

I want to level up my industrial cybersecurity knowledge.

ISA/IEC 62443 training for product and system manufacturers – Secure industrial products and components with cybersecurity training for engineers based on ISA/IEC 62443 2-4, 3-2, 3-3, 4-1 and 4-2.

Establish security by design for systems and products

Product due diligence

Security compliance

Market competitiveness

Make component security transparent and accessible to system integrators and end users

Embed security into development processes

Instill cybersecurity rigor into your processes

Demonstrate validation of security to customers

IEC 62443 training
Manufacturers, system integrators | Three days | Online/classroom | Certificate (optional)

I want to ensure that our cybersecurity processes and product life cycle are truly secure.

ISA/IEC 62443 services – Accelerate your cyber-readiness and gain visibility into your security posture with comprehensive ISA/IEC 62443 advisory, testing and certification services.

Market enablement

Operational technology (OT) risk assessment

Documentation review and support

Building a control system cybersecurity management system (CSMS) for IACS

Training workshops

Gap analysis for certification readiness

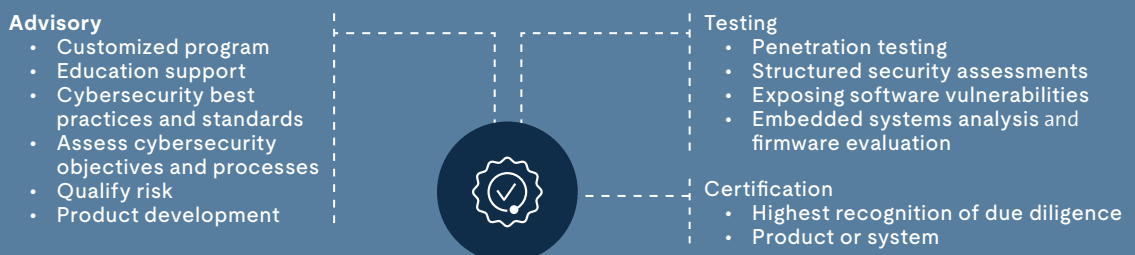Penetration testing

Certification

IEC 62443 services
Component and product manufacturers | ICS integrators | Control system users

---

I need comprehensive cybersecurity services.

UL Cybersecurity Assurance Program (UL CAP) – A full suite of advisory, testing and certification services designed to help organizations manage their cybersecurity risks and validate their cybersecurity capabilities to the marketplace

Advisory
- Customized program
- Education support
- Cybersecurity best practices and standards
- Assess cybersecurity objectives and processes
- Qualify risk
- Product development

Testing
- Penetration testing
- Structured security assessments
- Exposing software vulnerabilities
- Embedded systems analysis and firmware evaluation

Certification
- Highest recognition of due diligence
- Product or system

UL CAP Cybersecurity Assurance Program
Based on the UL 2900* series of Standards

*UL 2900, the Standards for Software Cybersecurity for Network-Connectable Products

Why UL Solutions for cybersecurity?

- Independent, trusted third party

- Hardware- and software-based security evaluations

- Cybersecurity expertise

- Cybersecurity and safety

- Full life cycle solutions

- Assessment of security development practices

- Industry knowledge

- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

Learn more and speak to one of our experts today at UL.com/industry40-cybersecurity.

UL Solutions

UL.com/Solutions