Industrial Cyber Security

Rockwell Automation

Navigating the OT Cyber Landscape

Start your journey to resilient operations today.

Grant Coffin – Software & Control Business Manager UK & Ireland

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

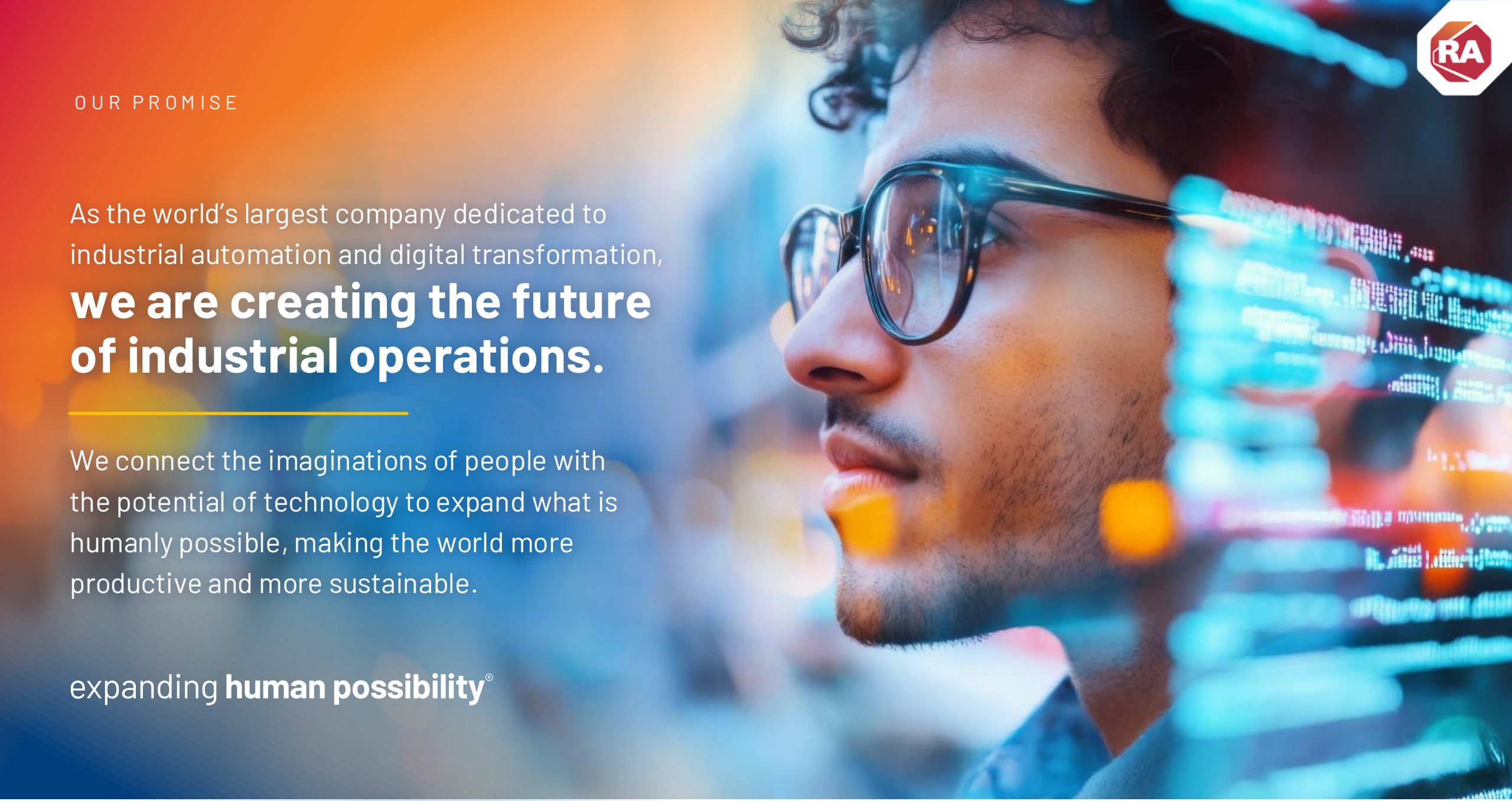
OUR PROMISE

As the world's largest company dedicated to industrial automation and digital transformation,

we are creating the future of industrial operations.

We connect the imaginations of people with the potential of technology to expand what is humanly possible, making the world more productive and more sustainable.

expanding **human possibility**®



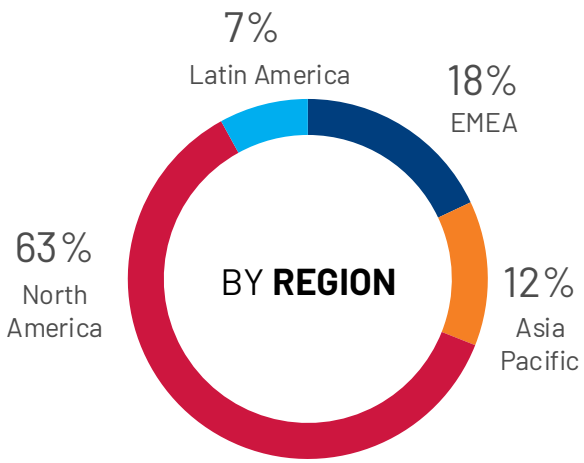
PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

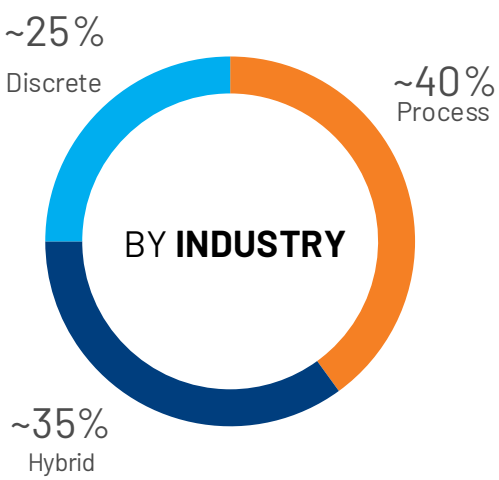
Rockwell Automation At A Glance

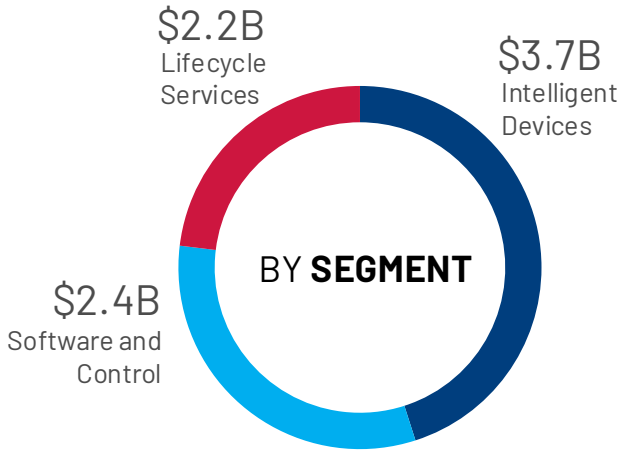
2025 GLOBAL SALES

8.3

BILLION USD







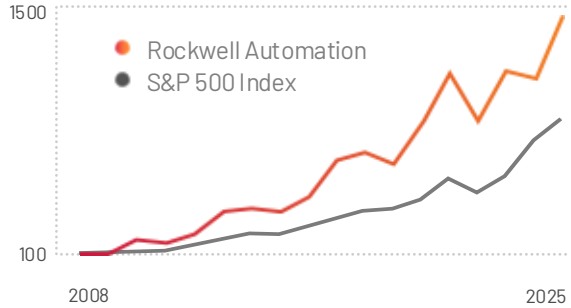
100+
Number of countries

26k
Employees: more than half outside the U.S.

2025 WORLD'S MOST ETHICAL COMPANIES® ETHISPHERE 17-TIME HONOREE
World's Most Ethical Companies

SCIENCE BASED TARGETS
DRIVING AMBITIOUS CORPORATE CLIMATE ACTION
Committed: January 2024

Total shareowner return



Serving customers for **123 years**

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Our brands

Largest pure-play automation company serving a diverse set of end markets

Rockwell Automation

Allen-Bradley by ROCKWELL AUTOMATION

FactoryTalk by ROCKWELL AUTOMATION

LIFECYCLE IQ Services by ROCKWELL AUTOMATION

SERVING CUSTOMERS SINCE 1903



















PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Securing what the world relies on

Rockwell Automation helps organizations take a proactive approach to industrial cybersecurity.



THE CHANGING LANDSCAPE

Yesterday's strengths are not tomorrow's differentiators



Why secure operations matter

Delivering measurable business outcomes



Reduce Risk
Build a defensible IT/OT architecture to help protect critical assets

Maximize Availability
Keep production running and operations resilient amid evolving risks

Meet Compliance
Align with regulatory and corporate requirements for secure, safe, and stable performance

Scale Resources
Extend teams to fill skills gaps, unlock cost savings, and minimize disruption

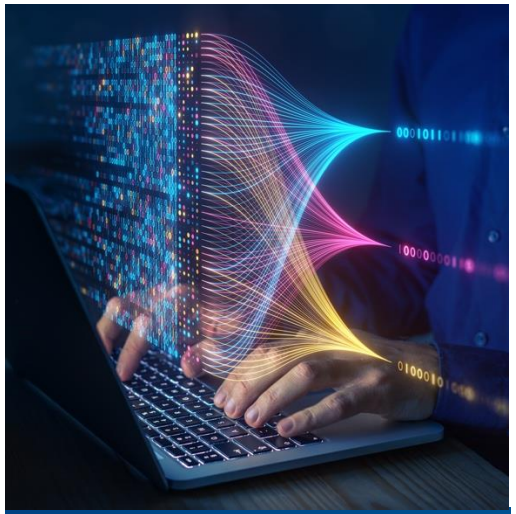
Limit Financial & Brand Impact
Avoid costly downtime and reputational damage

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Current Trends in Industrial Cybersecurity



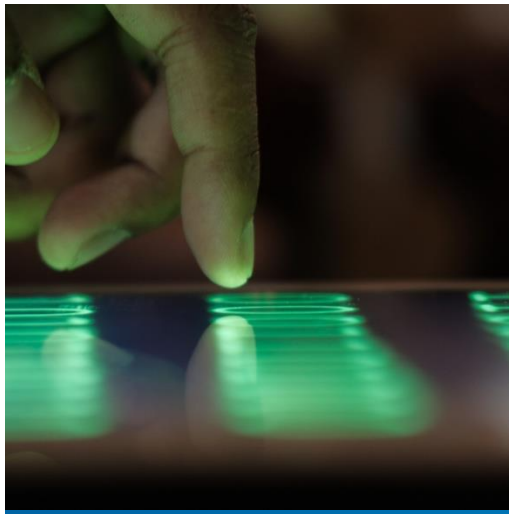
Expanding threat landscape



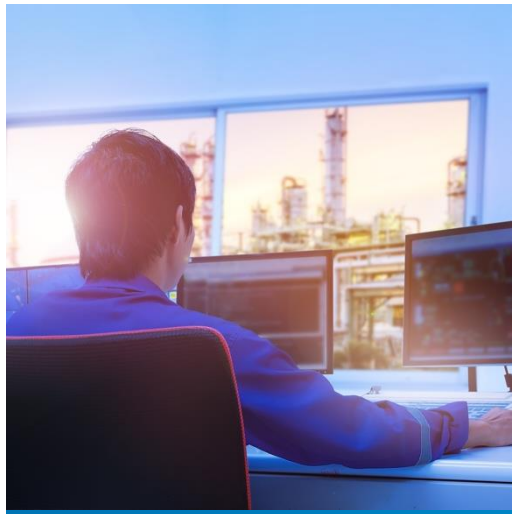
Vulnerability management



Geopolitical influence



Ransomware



Regulatory focus

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Industrial Security Challenges

AGING INFRASTRUCTURE



In 2023, the average age of industrial equipment was 8.1 years

LACK OF VISIBILITY



80% of vulnerabilities reside deep within the ICS network

OT CYBER SKILLS GAP



Cybersecurity is the #1 skill manufacturers are seeking

REGULATORY REQUIREMENTS



74% of executives expect regulatory pressure on OT security to increase

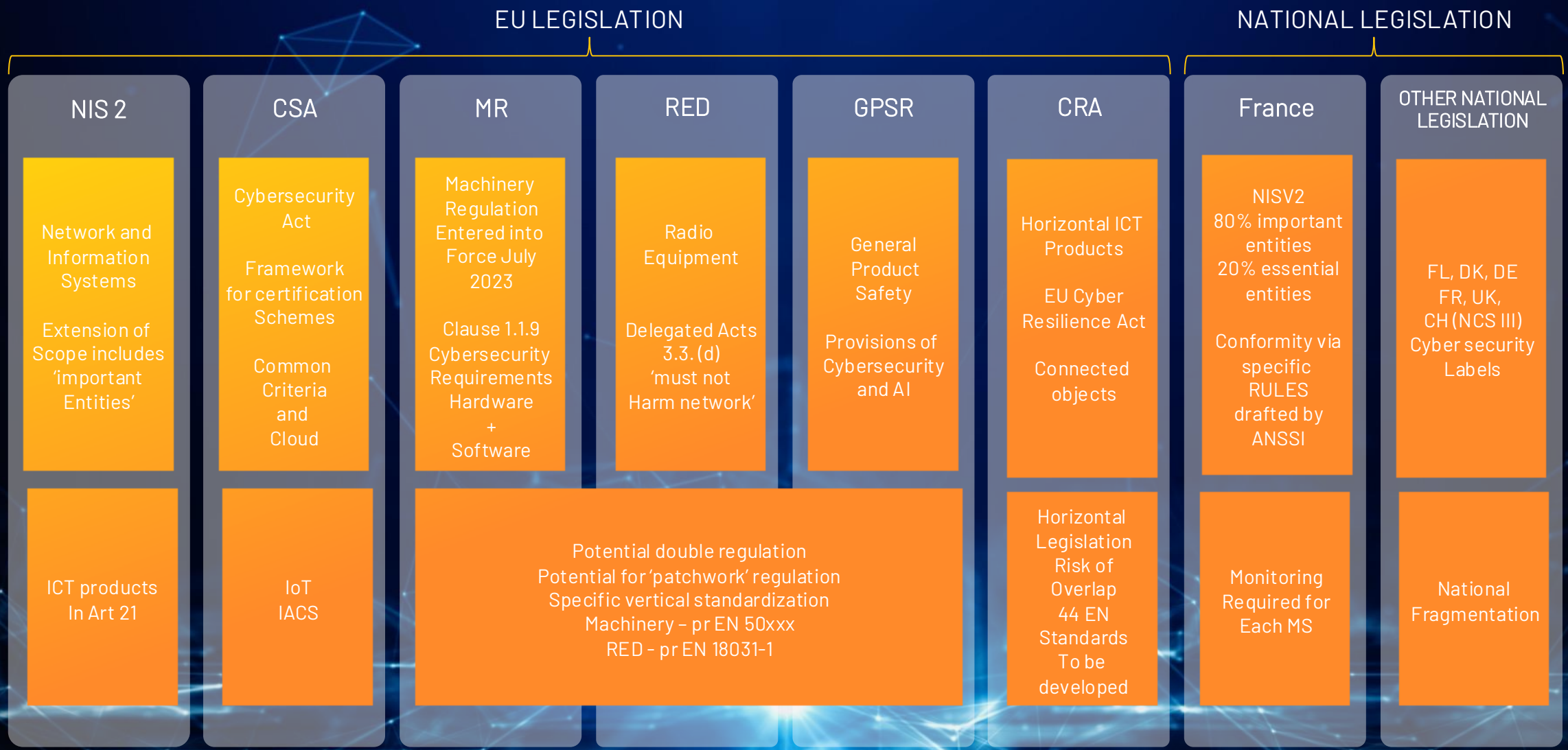
COMPLEX SUPPLY CHAINS



65% of attacks on manufacturers expand into supply chains

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Fragmented EU regulatory landscape for connected products



NIS2 directive: get ready now

What is the Network & Information Security 2.0 directive?

- The **NIS2 Directive** is legislation that aims to enhance the cyber resilience of critical infrastructure in the European Union by establishing a minimum set of cybersecurity requirements that **all member states** must impose on their respective in-scope entities.
- NIS2 replaces and builds upon its predecessor, the original NIS Directive (2016), with an expanded scope and additional requirements developed in response **to increases in the frequency and impact of cyberattacks against European Union critical infrastructure** in recent years

NIS2 impacts all entities that operate in the European Union

NIS2 became enforceable on **October 18 2024**



The Machinery Regulation - (EU) 2023/1230

Safety and Security – A Critical Relationship

Overview

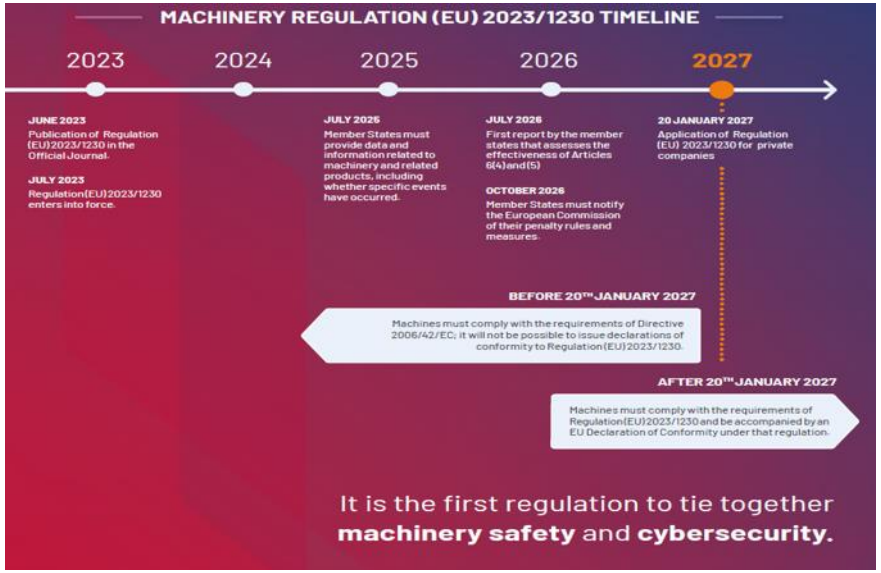
Applicable for the EU, EFTA countries & the UK

- Published in the OJ – 29th June 2023
- Entry into Force – 19th July 2023
- Transition period – 42 months.
- **Application date - 20th January 2027**

It is no longer a Directive it is a Regulation.

- Will be adopted by all member states without modification, or change to date of entry

Compliance continues to be based around the use of harmonised standards.
(WD EN50742)





With more machinery and products being integrated into SMART manufacturing lines, where industrial networks are commonplace, the need for **cybersecurity requirements** has been included in the Essential Health & Safety Requirements (EHSR"s).

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Cyber Resiliency Act: Start to Prepare

The European Union Cyber Resiliency Act will go into effect **11th December 2027**

Reporting obligations will go into effect **11th September 2026**

The CRA has **four specific objectives** to improve the approach to security in Europe

End-to-end security

Once in force, the CRA will **impose security improvements for products** with digital elements at every stage of their life cycle, including design, development, and maintenance.

Compliance

Using a coherent cybersecurity framework, the CRA will facilitate **compliance for hardware and software manufacturers** with consequences for violations.

Improved Transparency

New rules and standards that improve the **communication** around cybersecurity properties of products with digital elements will make information more accessible to users, helping them make more **informed decisions**.

Safer use of products

Comprehensive measures outlined by the CRA will make it easier for organizations and consumers to use products with digital elements securely, therefore, **minimizing exposure to risk**.

Cost of Non-compliance

For **security requirements and vulnerability** reporting: penalties of up to €15 million or 2.5% of global turnover for non-compliance

For accompanying articles (Obligations of importers and of distributors): penalties of up to €10 million or 2% of global turnover for non-compliance

Incorrect, incomplete or misleading information: penalties of up to €5 million or 2% of global turnover for non-compliance

CYBERSECURITY FRAMEWORKS FOR IACS

A practical stack for governing risk, engineering controls and validating resilience

THE OT / IACS ENGINEERING ANCHOR

IEC 62443

Purpose-built for industrial automation and control systems across the full lifecycle.

ROLES	Asset owner • Integrator • Supplier
ARCHITECTURE	Zones, conduits & defence-in-depth
ASSURANCE	Security levels & secure development

GOVERN

NIST CSF 2.0

Enterprise outcomes across Govern, Identify, Protect, Detect, Respond and Recover.

IMPLEMENT

NIST SP 800-82

OT-specific guidance that balances cyber controls with safety, reliability and availability.

INTEGRATE

ISO/IEC 27001

ISMS governance, risk treatment and auditability connected to the wider enterprise.

UK RESILIENCE

NCSC CAF

Outcome-based assessment of essential functions, using evidence and indicators of good practice.

THREAT-INFORM

MITRE ATT&CK for ICS

Adversary tactics and techniques to shape detection, exercises and control validation.

SECTOR OVERLAYS

Regulatory / sector sets

Apply where relevant: NIS / NIS2, NERC CIP, IEC 62351 and sector regulator profiles.

HOW THEY WORK TOGETHER

01 ORGANISE RISK	02 ENGINEER CONTROLS	03 IMPLEMENT SAFELY	04 VALIDATE THREATS
CSF • CAF • ISO 27001	IEC 62443	NIST SP 800-82	ATT&CK for ICS

Use one integrated control model, not six parallel compliance programmes.

Prioritise safety, availability and recoverability alongside confidentiality and integrity.

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Key Takeaways

- Education and awareness:
  - Within your organization, for your customers or trusted partners
- Establish an open dialog between Industrial Automation and IT groups
- Establish an Industrial security policy, unique from and in addition to the Enterprise security policy
- Holistic Defense-in-Depth approach: no single product, methodology, nor technology fully secures IACS networks
- Be aware of and align with Industrial Automation and Control System Security Standards
  - **IEC-62443 (Formerly ISA99), NIST 800-82, ICS-CERT, CPNI, etc. Recommended Practices**
- Utilize standards, reference models and reference architectures
- Work with trusted partners knowledgeable in industrial automation and security
- "Good enough" security now, is better than "perfect" security … never. (Tom West, Data General

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.

Rockwell Automation

expanding **human possibility**®

Allen-Bradley by ROCKWELL AUTOMATION

LIFECYCLE IQ™ Services by ROCKWELL AUTOMATION

FactoryTalk by ROCKWELL AUTOMATION

PUBLIC • Copyright ©2025 Rockwell Automation, Inc.