What the EU's Cyber Resilience Act Means for Your Business

Adam Griffen

Product Manager, ei³
Digital Transformation Workgroup Leader, OMAC

Introduction

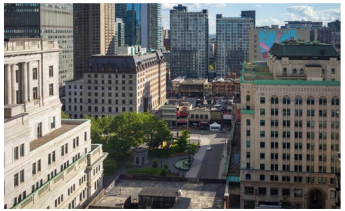
- Joined ei3 in March 2023, driven by a passion for Automation, IIoT, and AI
- 10+ years experience in industry:
  - Operator > Technician > Engineer > Product Manager
- Spent 8 years at Mettler-Toledo in Product Management, specializing in software engineering and SAP Variant Configuration. Also led Compliance efforts for Automation & Digital Security
- 9-years of involvement in OMAC, contributing to initiatives like PackML update and OPC UA Companion Specification

ei³ At A Glance

Trusted partner for Industrial IoT and AI for machine builders and manufacturers since 1999

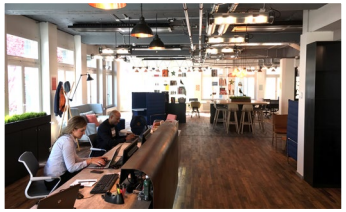
3 Locations, 3 Competencies

MONTREAL, CANADA
JAVA DEVELOPMENT



PEARL RIVER, NEW YORK
GLOBAL HEADQUARTERS

ZURICH, SWITZERLAND
DATA SCIENCE CENTRE



Data centres in: USA, Germany, China

Sales offices in: Japan, India

Trusted by leading brands

American Packaging Corporation · BOBST · BROWN Machine Group · coperion · DÜRR · ECOLEAF · kp klöckner pentaplast · INYX · MILACRON M POWERED · PROCENTEC Member of the HMS group. · STG · Shibaura Machine · SONOCO · WestRock · Graphic Packaging International · BROWN Machine Group · ORBIS · GESA

OMAC
The Organization for Machine Automation and Control

ei³ At A Glance

For machine builders:

- Proven, white-labeled solution to get started on your digital transformation journey immediately
- Reduce warranty costs and technican's travel time with secure remote access
- Drive new after-sales services to deliver fast support to customers and improve brand loyalty

For machine owners:

- Achieve maximum ROI from your equipment and save costs by measuring, monitoring and controlling your key performance indicators with our powerful suite of IoT Applications
- Reduce downtime, improve quality, increase yield and lower energy consumption

150,000
machines & devices being monitored

10,000
connected facilities

300 million
data points collected everyday

OMAC
The Organization for Machine Automation and Control

Organization for Machine Automation & Control

Why OMAC?

When manufacturers work together to create standards and share best practices whole industries benefit

The OMAC Mission

Provide collaborative thought leadership, standards and support to automation professionals enabling their organizations to save time, money and resources, creating room for innovation

OMAC
The Organization for Machine Automation and Control

Members

- Since 1994
- 60+ members and growing

End users

Nestle, P&G, Arla Foods, WestRock, etc.

System integrators

CONTEC, EOSYS, Rovisys, etc.

OEMs

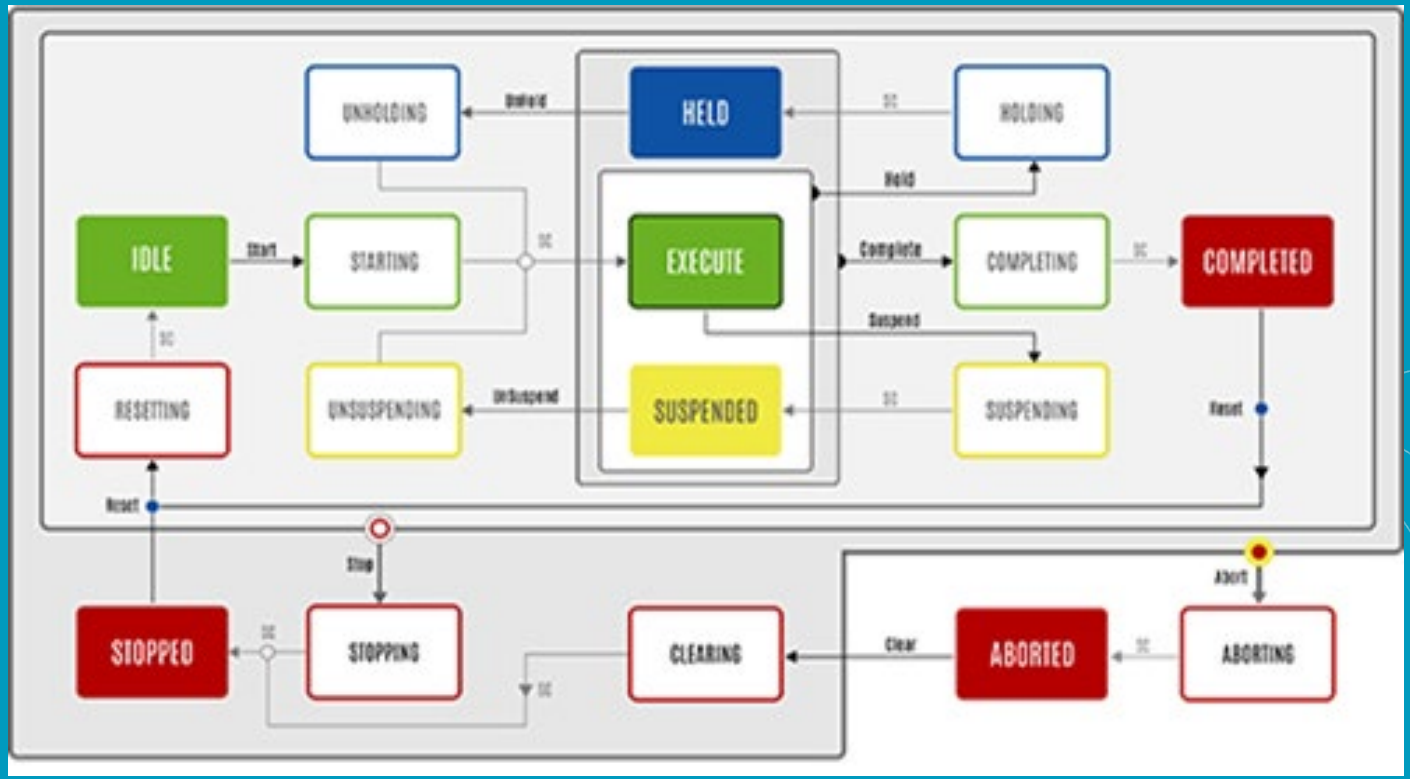
ProMach, Bobst, Milacron, Mettler-Toledo, etc.

Technology providers

Rockwell, Siemens, Mitsubishi, ei3, Cisco, etc.

Partner Organizations

PackML



OMAC
The Organization for Machine Automation and Control

OMAC
The Organization for Machine

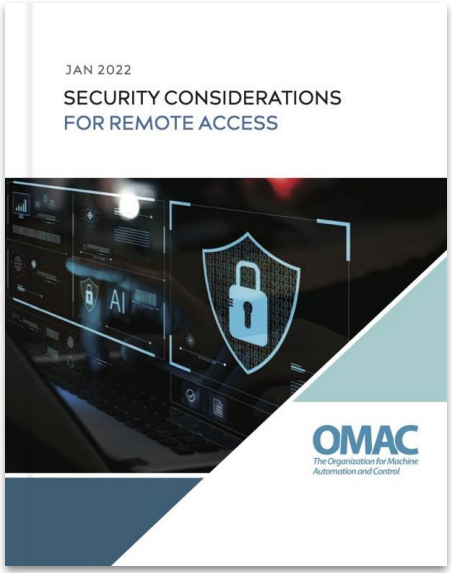
OMAC Workgroups

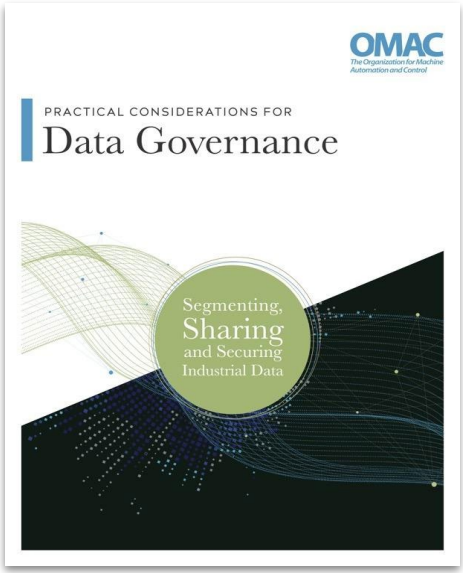
Shape the Future of Automation with the OMAC Packaging Workgroup (OPW)

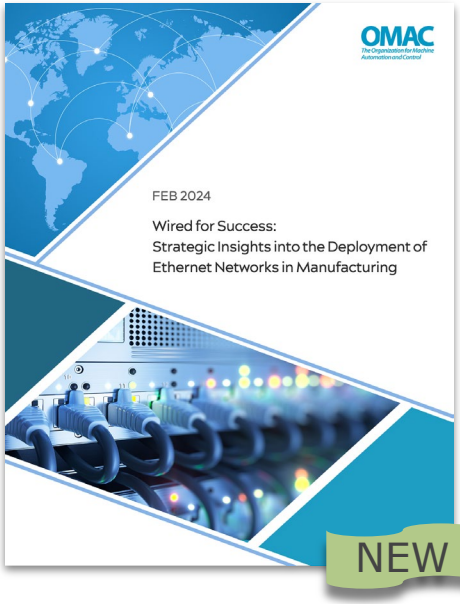
Drive Digital Twin Manufacturing with the OMAC Manufacturing Workgroup (OMW)

Create Remote Access Best Practices with the OMAC Digital Transformation Workgroup (DTW)

Digital Transformation Workgroup







OMAC
The Organization for Machine Automation and Control

Digital Transformation Workgroup

- **March 12, 2024**: The European Parliament approved the Cyber Resilience Act
- The Cyber Resilience Act was approved with **517 votes in favour**, 12 against and 78 abstentions

OMAC
The Organization for Machine Automation and Control

Digital Transformation Workgroup

GLOBAL CYBERCRIME DAMAGE COSTS

- $6T a **year**
- $500B a **month**
- $16.4B a **day**
- $684.9M an **hour**
- $190,000 a **second**

Digital Transformation Workgroup

- High-level, non-technical 5-page summary of the act for executive leadership
- Helps understand the scope, impact, and timeline of the new legislation
- Offers practical first steps to begin the journey towards compliance

Products Affected by the Cyber Resilience Act

90% OF PRODUCTS

Default category

Self-assessment

Examples: domestic robots, smart speakers, toys, hard drives, photo editors, word processors

10% OF PRODUCTS

Class I - critical products

Self-assessment or third-party

Examples: IMSSs, browsers, passwords managers, anti-virus software, SIEM systems, microcontrollers, routers

Class II - highly critical products

Third-party assessment

Examples: operating systems, HSMs, industrial firewalls, CPUs, smartcards, smartcard readers, secure elements

Source: BLAZE

Status of the EU's CRA

Sept 2022

Commission proposed the first draft with a two-year provision to prepare for enforcement

Jul 2023

Council reached an agreement on changes to the legislation, updating the scope of products to comply, among other changes

Mar 2024

Final negotiations between member states and the European Parliament, followed by the establishment of the date the act goes into effect

Next Steps

Mapping industrial standards to legislative requirements and executing business changes to comply

OMAC
The Organization for Machine Automation and Control

OMAC Summary for Executives

Security properties in digital products

Collaborate with experts

Security vulnerability handling procedures

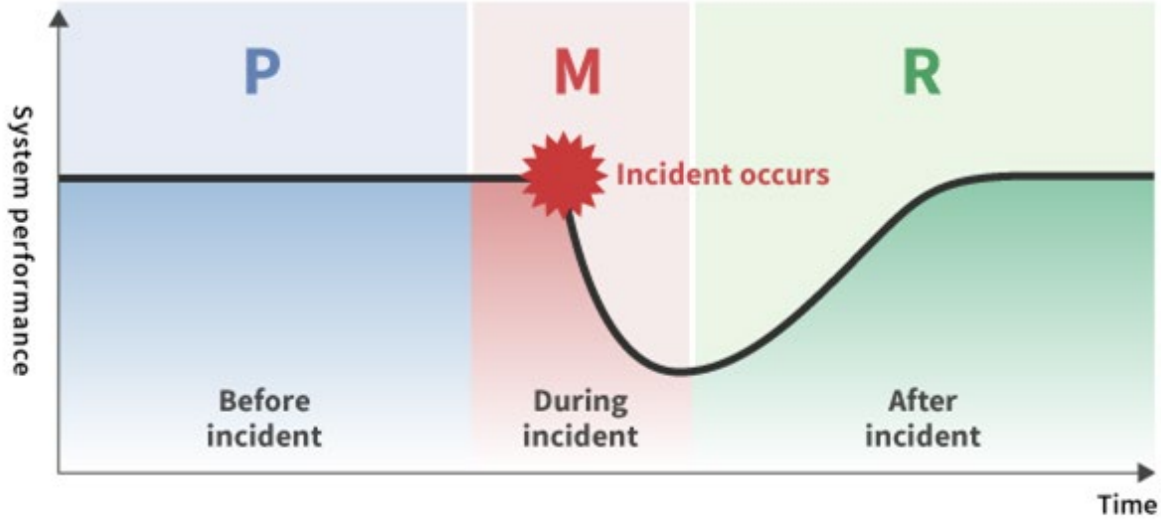
Comply with EU regulations

3rd party certification for critical products

Apply best practices for industrial cyber security

OMAC
The Organization for Machine Automation and Control

Cyber Resilience



Prepare (System operation time)	Mitigate (Losses caused by incident)	Response & Recovery (Response and recovery time)
Maximize system performance (extend P)	Minimize incident impact (decrease M)	Rapid recovery (shorten R)

OMAC
The Organization for Machine Automation and Control

Cyber Resilience

Cyber Resilience

STEP 1
System Hygiene

Establish a proactive and systematic process for managing standard systems hygiene

STEP 2
Develop A Plan

Create a cross-functional team of senior management plan for cyber security events and consider hypothetical attacks

STEP 3
Map Out Risk Profile

Study cyber patterns and attack modes to develop a tailored approach to protecting company assets

STEP 4
Assess & Measure

Focus on rough figures, not precise estimates and avoid analysis paralysis

STEP 5
Mitigate Risk

Invest in risk mitigation measures to protect company assets at greatest risk

STEP 6
Cyber Insurance

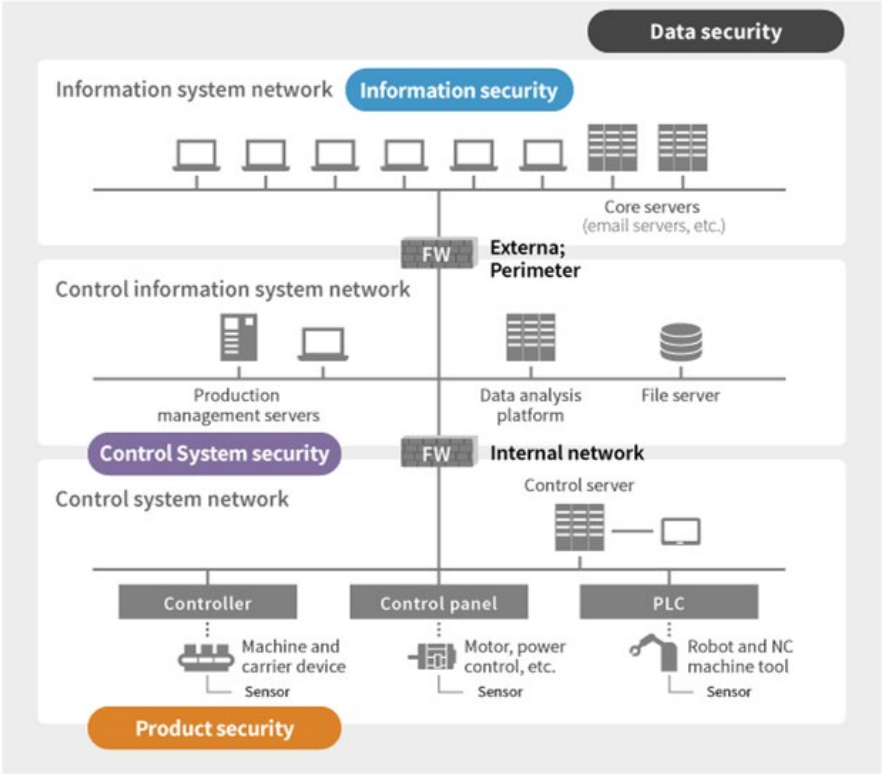
Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack

STEP 7
Get Started

A rough plan is okay - becoming resilient to cyber risk starts with a single step

OMAC
The Organization for Machine Automation and Control

Cyber Resilience in Automation



OMAC
The Organization for Machine Automation and Control

Business Analyst

CIO

IT Architect

vs.

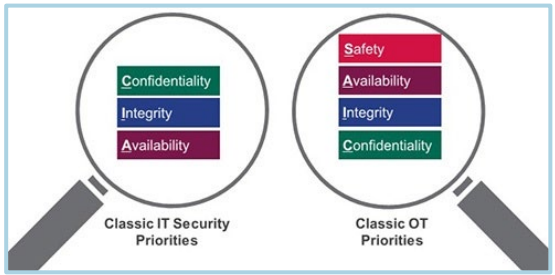
Plant Manager

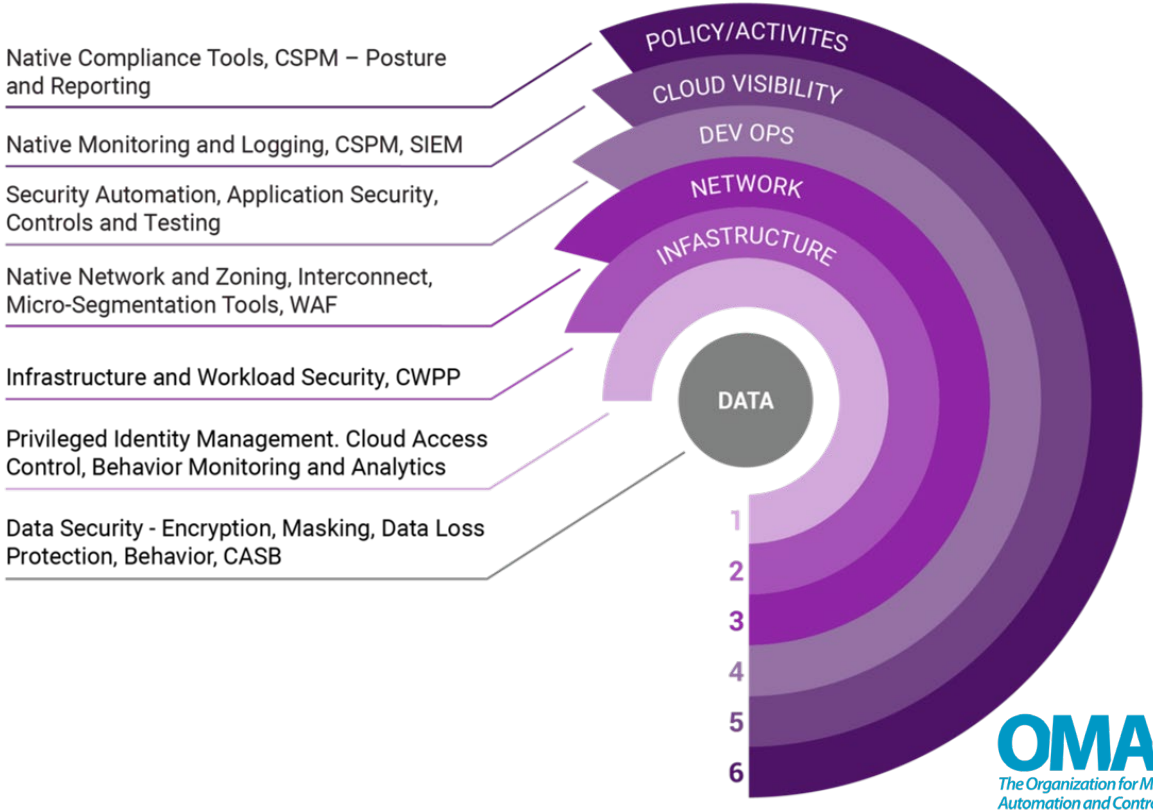
Control Engineer

COO

No. 1 Priority	Confidentiality	Availability
Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Target	Windows computers, servers	Industrial legacy devices, barcode readers
Environmental Conditions	Air-conditioned	Extreme temperatures, vibrations and shocks

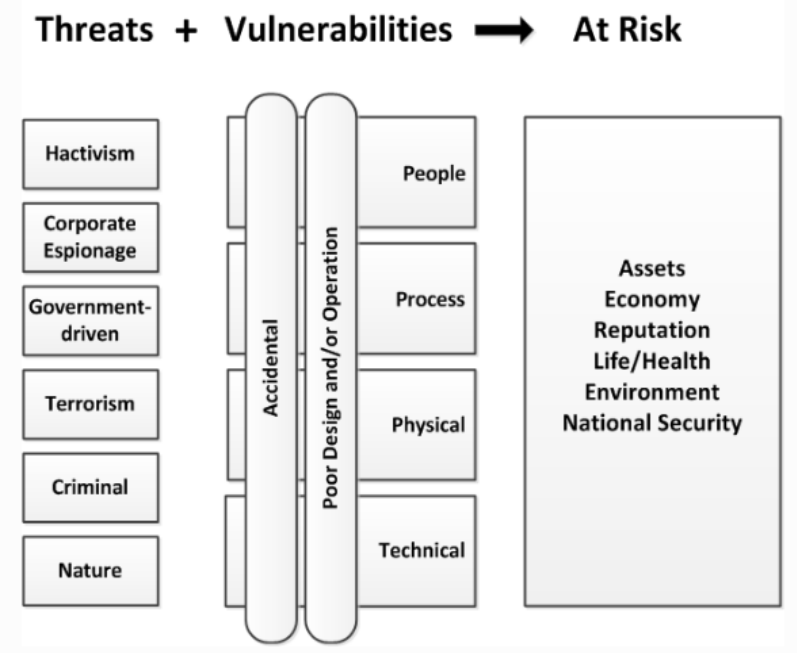
Cyber Resilience in Automation





OMAC
The Organization for Machine Automation and Control

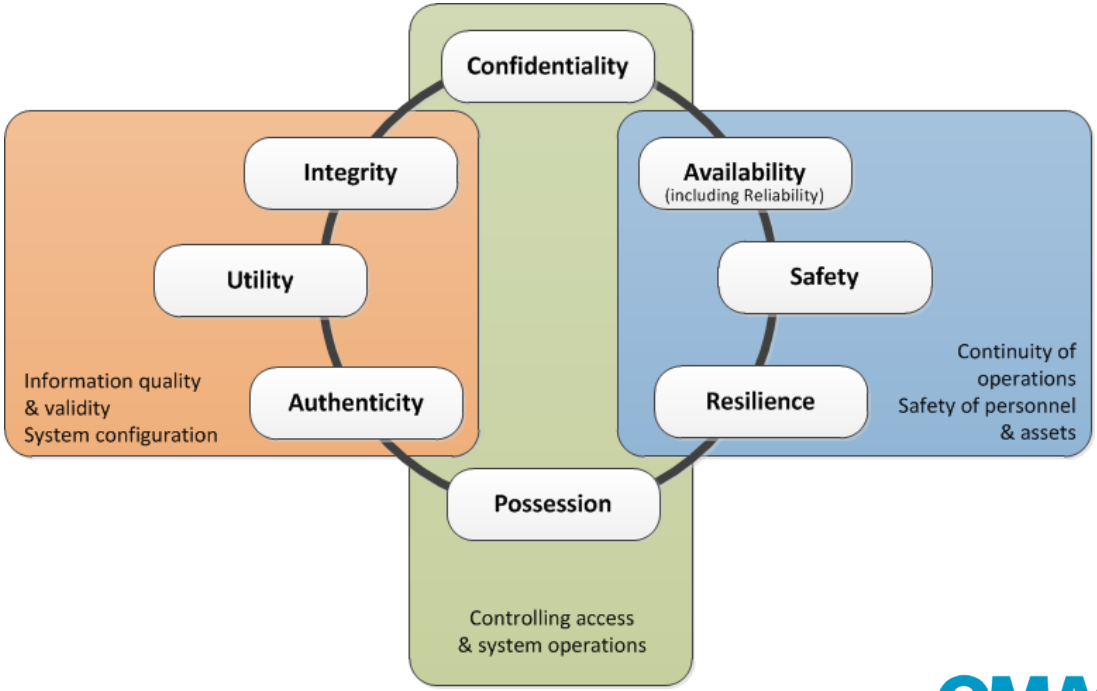
Cyber Resilience in Automation



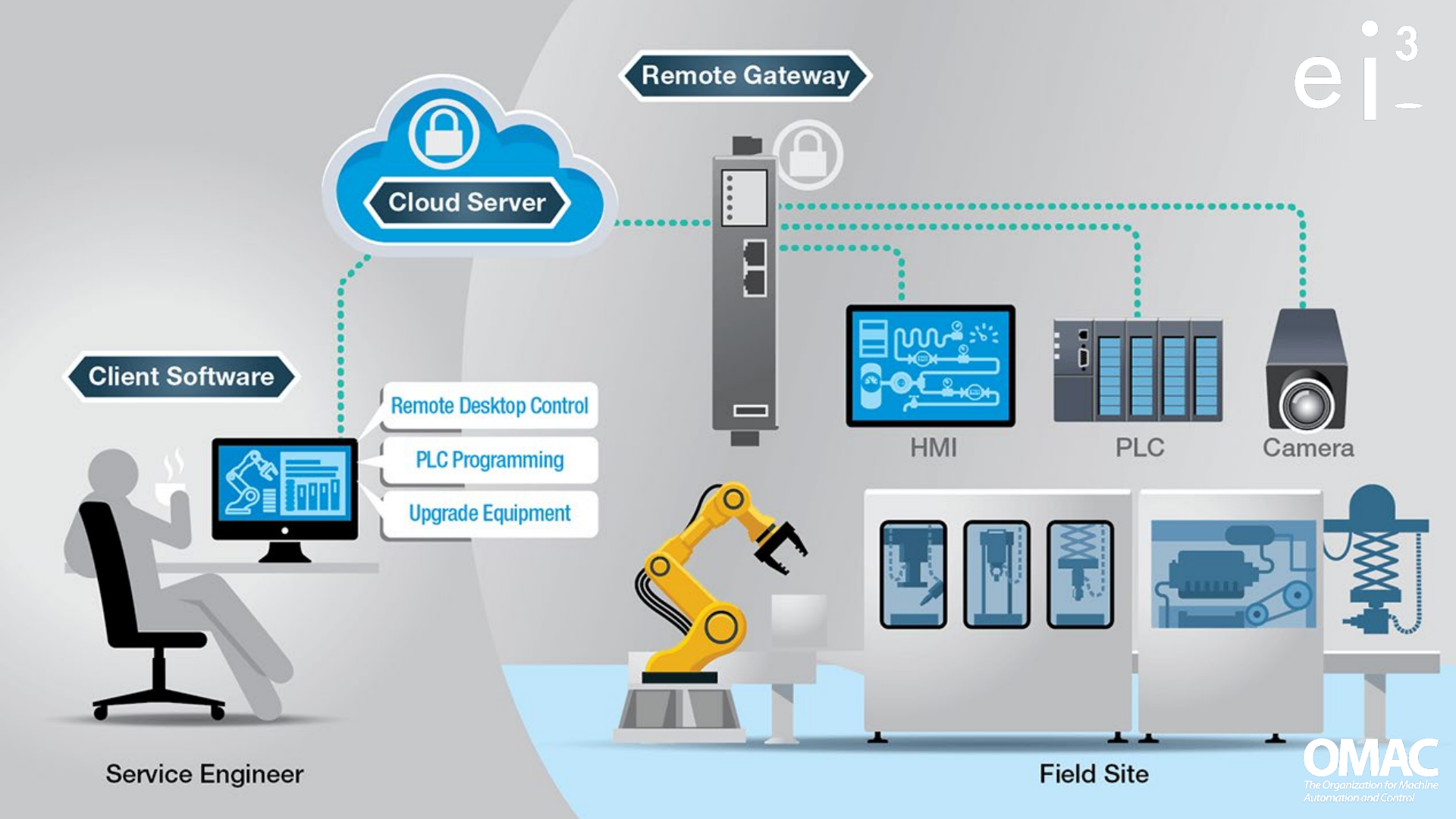
OMAC
The Organization for Machine Automation and Control

Cyber Resilience in Automation

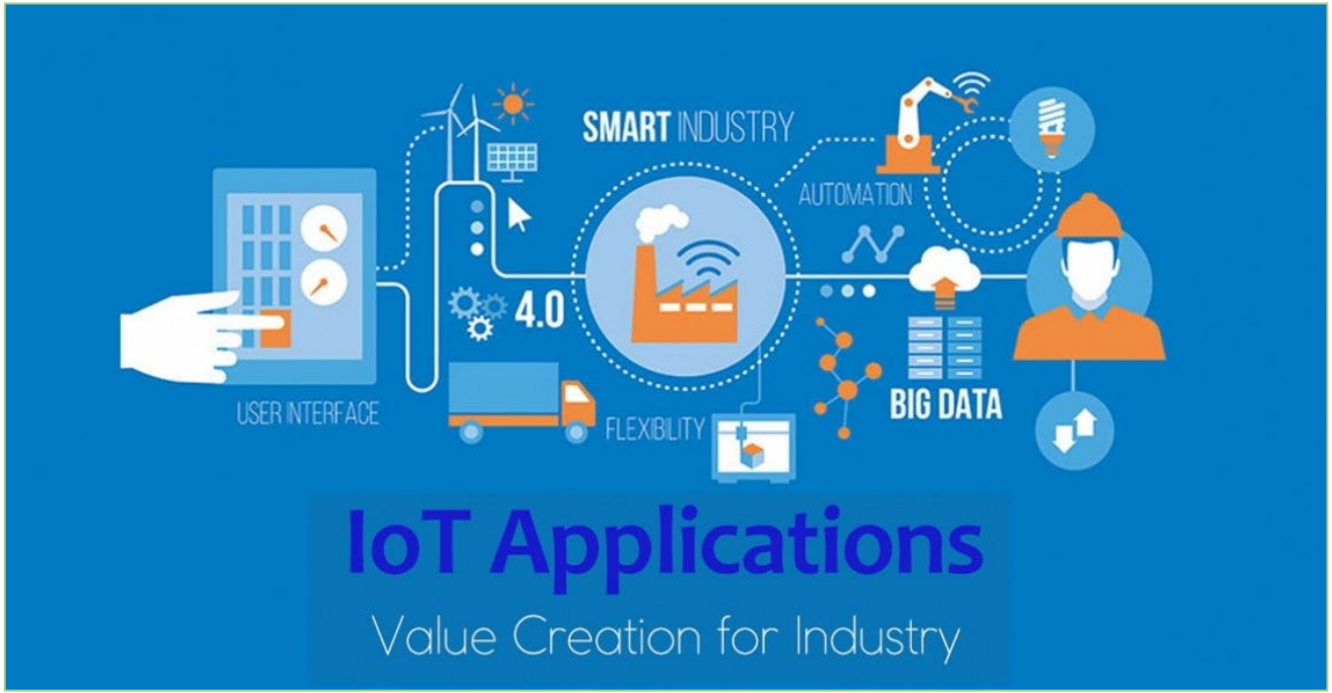
- Legacy systems
- Compatibility with existing IT security
- Collaboration with 3rd parties (system integrators, OEM service technicians)
- Workplace safety is paramount

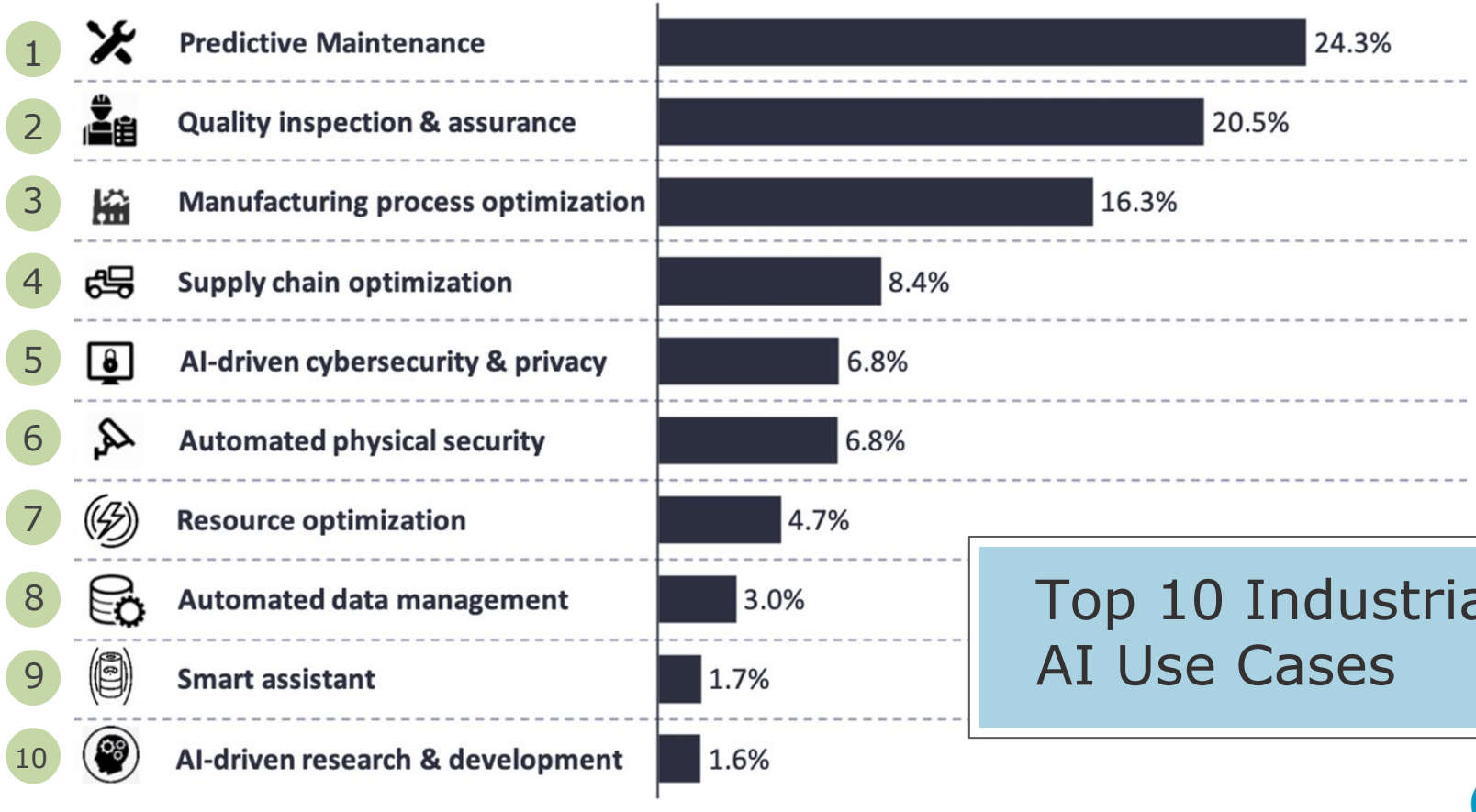


OMAC
The Organization for Machine Automation and Control


Remote Gateway
Cloud Server
Client Software
Remote Desktop Control
PLC Programming
Upgrade Equipment
HMI
PLC
Camera
Service Engineer
Field Site
OMAC
The Organization for Machine Automation and Control

Costs of Risk Mitigation vs. Reward





Top 10 Industrial AI Use Cases

Source: IoT Analytics

Start Your Cyber Resilience Journey

- Prioritize cyber resilience as a crucial business cost
- Allocate resources proportionate to the risks to mitigate them
- Seek expert guidance early in the process
- Partner with the right technology and service providers
- Conduct cyber risk assessments for products and systems
- Involve all stakeholders: Engineering/Development, IT, Production, Quality, Service, and Legal Counselors
- Apply best practices in remote access, cybersecurity for industrial systems, and data governance

OMAC
The Organization for Machine Automation and Control

OMAC
The Organization for Machine Automation and Control

ei3

Thank you!

Adam Griffen
Phone Number
agriffen@ei3.com