



**Rockwell
Automation**

CYBERSECURITY SOLUTIONS FOR LIFE SCIENCES

Mitigate risk with secure industrial network connectivity

```
<img alt="Background image of a woman in a server room working on a laptop, with a semi-transparent overlay of HTML code." data-bbox="0 0 1000 1000"/>

```


```
<img alt="Background image of a woman in a server room working on a laptop, with a semi-transparent overlay of HTML code." data-bbox="0 0 1000 1000"/>
```


```


```

Importance of **cybersecurity** in Life Sciences

The cybersecurity risk to Life Sciences companies has grown exponentially since the start of the pandemic. Right when Life Science companies became even more important to us and were operating within a highly validated environment close to 24/7.

Life Science processes don't follow standard lifecycle timelines and these systems typically can't implement security updates quickly, which leaves a process vulnerable to cyberattacks.

Facing the threat to mission-critical systems, many of which are legacy systems running older operating systems, can be done with a strong partner. Rockwell Automation has over 100 years of industrial automation and specialized OT cybersecurity knowledge.

Our portfolio of solutions and managed services align to the NIST Cybersecurity Framework for 360 protection



ASSESS
& DESIGN

Network

- Industrial demilitarized zone (IDMZ)
- Firewall
- Risk assessment
- Security posture survey
- Penetration testing



IMPLEMENT

Network*

- Industrial demilitarized zone (IDMZ)
- Firewall
- Virtual infrastructure*
- Threat detection
- Endpoint security
- Secure remote access



MANAGE

Network*

- Industrial demilitarized zone
- Firewall*
- Virtual infrastructure*
- Threat detection
- Endpoint security
- Incident response

Assess & design a cybersecurity system

To design a strong and lasting cybersecurity system the first step is to assess what's needed. Up until recently OT networks used to be air-gapped for security, which made it more challenging for IT. Establishing homogenous point-to-point security while meeting the latest in IEC 62443 certification standards is the next level.



Assess along networks
in digital infrastructure



Review virtual infrastructure
the company is assessing

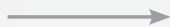


Detailed risk assessment,
firewall needs, security
posture survey, and
penetration testing

Assess & design

NETWORK DESIGN

- **Topology, performance, and remediation planning** for current-state and comprehensive future-state logical or physical design blueprint meeting IEC 62443 standards
- **IDMZ design** - Functional specification, policies, procedures, rule sets, security appliance selection, and architecture drawings for an industrial segmented demilitarized zone



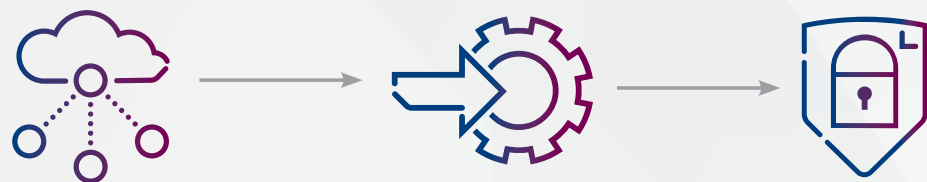
SECURITY DESIGN

- **Firewall design** with selection of security appliances based on existing IDMA rule sets or pre-defined parameters for secure information exchange
- **Qualitative or quantitative impact assessment** of vulnerability, threat, or consequences based on global framework standards
- **Security posture survey** for simplified cybersecurity hygiene score and report to prioritize remediation plans for found or known vulnerability

Implement a cybersecurity solution

Implementing a network involves deployment of the logical and physical OT network topology design. Hardware must be procured along with engineering commissioning services and delivery of standardized documentation packets.

Rockwell Automation offers a portfolio of solutions and managed services that align with the NIST Cybersecurity Framework for around the clock, end-to-end protection with cloud security. Finding a partner in cybersecurity who can handle every element brings added peace of mind along with reduced costs and time spent.



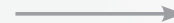
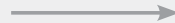
Network implementation

IDMZ IMPLEMENTATION

Deployment of design specifications, microservices, security appliances, engineering commissioning services, completed documentation packages, and finalized policies and procedures.

IDMZ PRE-ENGINEERED

Procurement configuration, deployment, and commissioning of pre-engineered **industrial demilitarized zone** solutions.



Virtual infrastructure **implementation**

VIRTUAL INFRASTRUCTURE

Virtual infrastructure implementation pertains to selections, sizing, configuration, deployment, and commissioning of pre-engineered **Industrial Data Center Solutions**.



The Industrial Data Center (IDC) can greatly ease your move to a virtualized environment. The IDC is a scalable architecture allowing you to easily scale up and out as needed. It includes all of the hardware, software, and installation services needed to deploy a large environment quickly.

Security implementation

FIREWALL

Implementing a firewall for security requires procurement, deployment, startup, and commissioning services of firewall appliances with optional documentation packages for architecture drawings, documented rule sets, and policy and procedures.

ENDPOINT SECURITY

Anti-malware management solutions are deployed along with software or third-party services for end devices.

THREAT DETECTION

Scaled site or enterprise-wide deployment of threat detection with on-site or off-site engineering services for configuration and optional enterprise management council (EMC) configuration.

SECURE REMOTE ACCESS

On-site or remote engineering services provide configuration and testing for remote user system access.

Manage a cybersecurity solution

Managing a cybersecurity system involves real-time monitoring and administration services for OT network switches, warranty management, firmware updates, and network configuration changes. A trusted partner with verifiable experience, like Rockwell Automation, can provide the management needed.

With our proven approach, on average, there is a 90% decrease in troubleshooting time, virtually eliminating network and server issues leading to improved productivity.

When a cyber incident occurs, you don't have time to figure out who to call. Rockwell Automation can assist, whether on-site or through remote support.

Leveraging the Rockwell Automation **Security Operations Center (SOC)** and connecting with yours, we can help you develop and maintain and OT SOC and train IT experts in how cybersecurity in the manufacturing space works. The Rockwell Automation SOC functions as a temporary intermediary between you OT stack and your IT SOC.



Why choose Rockwell Automation?

Today, **95% of Fortune 500 Life Sciences companies** rely on Rockwell Automation to improve product quality, reduce losses and risk, and optimize production operations. Cybersecurity is an important piece of operations today.



Learn how Rockwell Automation can help you **design, implement,**
and manage a secure cybersecurity system for your Life Sciences business.

Connect with us.    

rockwellautomation.com — expanding **human possibility**[®]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600

ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608

UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44)(1908) 838-800

Allen-Bradley, AutoSuite, ControlLogix, FactoryTalk, expanding human possibility, Integrated Architecture, Kinetix, PanelView, PartnerNetwork, and PowerFlex are trademarks of Rockwell Automation, Inc.
EtherNet/IP is a trademark of ODVA, Inc. All other trademarks are property of their respective companies.

Publication LIFE-SP006A-EN-P - February 2025

Copyright © 2025 Rockwell Automation, Inc. All Rights Reserved. Printed in USA.