Rockwell Automation

Attacking risk at its roots

Addressing brand-critical safety, security and obsolescence challenges with your automation infrastructure

Managing risk at the source

Managing risk is ultimately about protecting your company's brand and reputation. Incidents from tainted material or product recalls to data breaches and worker injuries have immediate consequences. These issues and how they are managed can impact your employees, facilities, intellectual property, product quality, revenue or customers. And in the end, they define your company and strongly influence the public's perception of you.

Risk management should be focused on the root causes of where problems originate. In many cases, that's your industrial automation infrastructure.

Managing risk with your automation infrastructure requires a focus on four key areas:

EQUIPMENT OBSOLESCENCE Modernizing your production systems using the latest control and information technologies can help minimize unplanned downtime, support compliance with the latest standards and regulations, and play a major role in managing the other three key areas of quality, safety and security.

QUALITY Harness the power of information that has long been buried within your operations to improve quality management and help confirm adherence to existing and emerging government regulations.

SAFETY For purposes of business continuity and risk management, safety must be addressed in three crucial areas – culture, compliance and capital. The upside: Companies that experience fewer safety incidents have also been shown to have improved operational performance.

SECURITY As more organizations embrace end-to-end connectivity across their facilities and enterprises, a comprehensive security approach is required to help protect their people, intellectual property and more.

WHERE IS YOUR RISK?

53% of industrial producers surveyed see maintaining product quality and reliability as their biggest operational risk over the next 5 years.

Source: TechValidate survey of Rockwell Automation customers, December 2015

Risk management should be focused on the root causes of where problems originate. In many cases, that's your industrial automation.

Equipment obsolescence

Challenges – both old and new

Manufacturers and industrial operators around the world are experiencing challenges at two different ends when it comes to their industrial automation control systems.

At one end are organizations relying on control systems from the 1970s and 1980s that are either near or past obsolescence. As a result, many vital component and subassembly replacement parts used in these systems are either hard to come by or no longer available. Decades-old control systems also are more difficult to support, especially as the skilled workers who are most familiar with them move on to retirement.

This can lead to significant downtime. Additionally, outdated equipment that falls short of today's regulations and standards can pose a threat to workers, the environment and product quality – critical risk areas for any company.

At the other end, many organizations in developing nations have launched greenfield facilities with the latest control technologies. Even with the latest equipment, a great number of these organizations have still found themselves being pushed past their capacity. Additionally, a lack of experienced designers and system integrators to develop these new systems means they can be riddled with risk.

This "obsolete at the onset" challenge can lead to operations that fall short of demand and miss out on revenue. Even worse, workers who push equipment beyond its limits or bypass standard operating procedures in order to meet productivity goals risk creating safety, security and environmental hazards.

Many end users are telling suppliers they need to keep their DCS running longer than the suppliers are willing to support them.[1]

[1] Automation and Software Expenditures in the Process Industries Global Market 2015 – 2020, ARC Advisory Group, January 2017

Assessing your assets

Managing equipment obsolescence begins with a thorough understanding of your existing industrial and IT assets. Before you embark on mitigation of obsolescence risks, you need to know where to begin.

Today, many organizations don't know the range of equipment operating throughout different facilities, where aging equipment physically sits or the specific risks associated with it as it ages. When companies do attempt to uncover this information, many find they must sacrifice an experienced engineer for several months simply to collect basic information on the hardware and software used in a single facility.

However, services such as installed base evaluations can collect hardware and software data across multiple sites in mere weeks. More than an audit, these services can provide reports that offer guidance on where critcal risk lies within your operations, areas or machines experiencing the most downtime or how to best mitigate risk based on ROI.

For example, a software inventory evaluation can help you identify potential compatibility risks between firmware and software versions as systems are connected and devices are updated, and confirm if software is being properly supported.

Industrial operators can sort reporting in a variety of ways, and share them across multiple functions. For example, a report comparing installed base equipment versus storeroom inventory can be shared with maintenance to improve spare-parts management. Reports can alert them of how many parts they currently have, and how many are recommended based on reliability, frequency of use and impact of part availability. Multiple site reports could be compiled to enable inter-enterprise inventory sharing.

An installed base evaluation should lead to the creation of a prioritized, obsolete-asset migration plan that takes into account:

- The criticality of a particular machine
- The obsolete parts on that machine
- The lack of available spares
- The complexity of moving the obsolete parts to current technology
- ROI of migration[1]

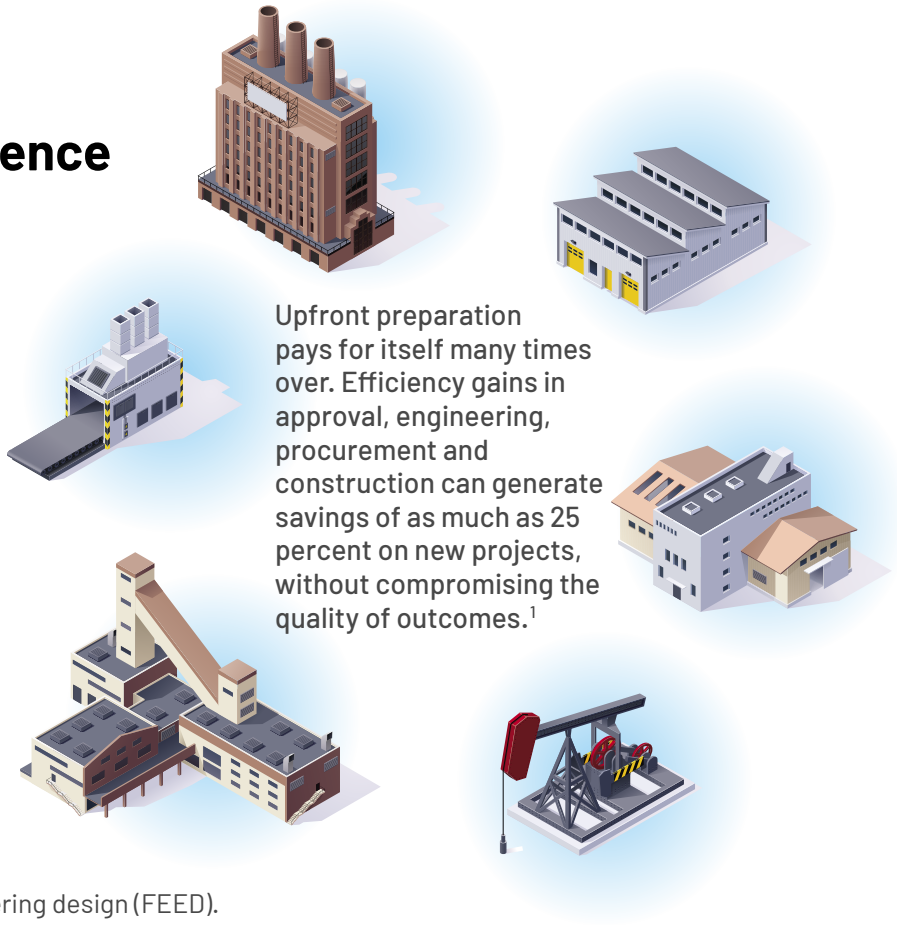
"Only 31% of industrial producers audit equipment for performance, age and obsolescence on a regular basis." [2]

[1] What's Your Obsolescence Plan? Rockwell Automation Blog, March 24, 2015
[2] TechValidate survey of Rockwell Automation customers, December 2015

Combatting obsolescence at the onset

Upfront engineering is critical to accurately define project scopes. Poor project planning, for example, can result in the wrong system being put in place and ultimately lead to missed production targets. Worse yet, poor planning can have detrimental effects on employee safety, the environment, IP security or product safety.

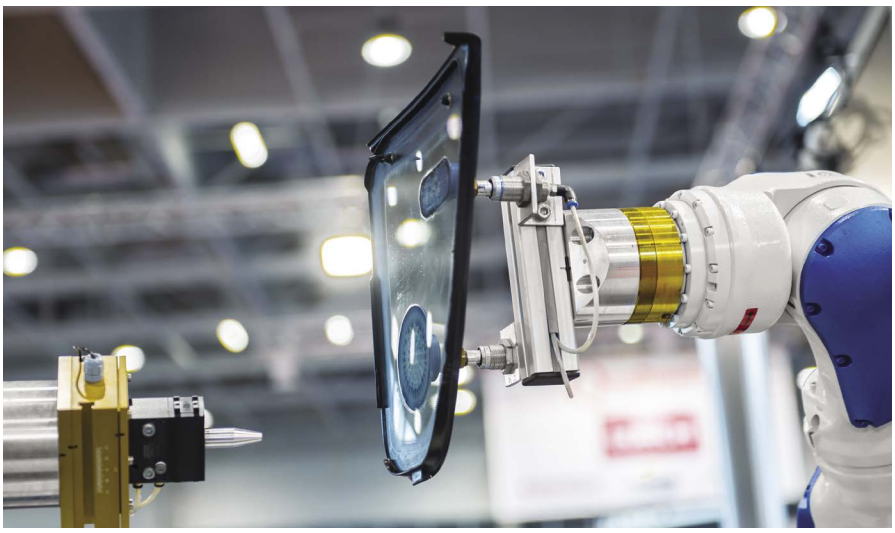
To help reduce this risk, industrial organizations and their EPC agency associates need the support and know-how of industry specialists. These specialists fully understand the many challenges surrounding greenfield and facility-expansion projects, from detailed engineering to system support and beyond.



Upfront preparation pays for itself many times over. Efficiency gains in approval, engineering, procurement and construction can generate savings of as much as 25 percent on new projects, without compromising the quality of outcomes.[1]

This support can include front-end engineering design (FEED). A good FEED is more than a project cost estimate. Rather, it is the foundation from which a project is built, and decisions made here will have an impact on every subsequent project phase.

A FEED should include detailed technical requirements, a well-defined project scope, a complete project budget, total cost of ownership, an implementation timeline and risk assessment – all of which can help reduce risk and uncertainty during the design, installation, commissioning and production phases. A good FEED also takes into account how your system will need to evolve as the plant evolves, which can reduce the likelihood of costly system replacements or upgrades.



[1]Megaprojects: The good, the bad, and the better, McKinsey & Company, July 2015

Risk lurking in information silos?

Reducing risk in your operations requires that you first know where it is, and that begins with better information.

For many manufacturers and industrial operators, the information needed to better help them understand different areas of risk – including compliance shortfalls, worker injuries, security holes, supply-chain gaps and more – has long remained hidden within their machines and processes. The Connected Enterprise is changing that.

While industrial organizations have traditionally used separate information technology (IT) and operations technology (OT) networks, The Connected Enterprise is built on a single, converged network infrastructure. This enables end-to-end, enterprisewide connectivity and secure, real-time information sharing between people, processes and technology.

Access to data, from your production equipment and smart devices in your facility and supply chain, can deliver unprecedented visibility into your operations to help better understand and address the most pressing risk areas.

RISK WAITS FOR NO PLAN

58% of industrial producers surveyed cite lack of information or priority planning as the primary issue preventing them from addressing a product quality or personnel safety issue.

Source: TechValidate survey of Rockwell Automation customers, December 2015

How can The Connected Enterprise help you better manage risk?

- Identify processes or raw materials that lead to quality issues
- Better understand where injuries, near misses and safety downtime events occur in your operations
- Uncover production inefficiencies that lead to missed production targets
- Monitor remote operations from a centralized location to reduce worker travel burdens and limit their exposure to dangerous environments
- Improve security through new technologies, such as RFID readers and cameras with video analytics
- Integrate genealogy and track-and-trace capabilities to achieve compliance with evolving anti-counterfeit and industry regulations

Quality

Modernize with MES software

Modern manufacturing execution system (MES) software integrates quality management and business analytics with production management to help you achieve the highest levels of quality and support regulatory compliance. An MES can play a crucial role within your Connected Enterprise for certain aspects of risk management:

- Automated collection of data from disparate sources replaces manual data-collection processes that can be prone to error and result in quality issues or even product recalls.
- Data-based insights enable you to compare finished-product quality against production conditions and individual suppliers' raw materials to identify the root cause of quality issues.
- Enforceable work flows guide operators through each production process and support products built to specification, helping verify product consistency while keeping your operations compliant with regulations and industry standards.
- Hold and quarantine capabilities help prevent the release of products that don't meet your quality requirements or are potentially dangerous.
- Security features such as role-based access can help ensure only authorized workers have access to production activities.

How well are you mananging risk?

13% of industrial producers surveyed are impacted by product recalls.

Source: TechValidate survey of Rockwell Automation customers, December 2015

"By connecting sensors and other monitoring systems into a functional network, it will be possible for manufacturers to easily monitor the storage conditions of various raw materials to be sure that factors such as temperature and humidity are at their proper levels." [1]

[1] Is the Internet of Things the Food Safety Solution of the Future? Food Online, June 11, 2015

Safety

A holistic approach

Safety is about more than protecting your workers. It's also about living up to the ethical standards that you set as a company. It's about protecting the morale of existing workers and creating an appealing workplace for potential workers. And in an era where news spreads fast, it's paramount to protect your brand.

Many manufacturers and industrial organizations have long viewed safety as a costly burden that clashes with productivity. Today, however, leading organizations are proving otherwise.

Recent research has found that best-in-class manufacturers, defined as the top 20 percent of aggregate performance scorers, achieve 5 to 7 percent higher OEE and 2 to 4 percent less unscheduled downtime than average performers. These same producers also experience significantly fewer workplace accidents (1 in 2,000 employees) compared to average performers (1 in 111 employees).

These top performers share a common set of best practices that can be grouped into three core pillars of a safety program:

- **Culture** (behavioral)
- **Compliance** (procedural)
- **Capital** (technical)

"Safety became part of our global company culture when we labeled it a core value, instead of just a priority. Priorities can change over time, but our values remain constant."

Jeff Deel, electrical instrumentation and controls engineering manager, Clorox

Measuring the three Cs of safety

Before you can improve safety and profitability, you must first understand your current level of performance across culture, compliance and capital.

Culture is the measurement of behaviors within your organization, including values, priorities, attitudes, incentives and beliefs. It indicates how highly your company values safety and helps determine if your company "walks the talk" with behaviors that embrace safety as a core value.

Compliance is the measurement of policies and procedures within your organization, indicating whether you have implemented policies and procedures that help achieve compliance with appropriate standards. Compliance extends to your suppliers because preventable, industrial accidents and mistreated laborers increasingly represent substantial reputational risk to your brand and can result in supply-chain interruptions.

Capital is the measurement of technical aspects within your organization. Adoption of current machinery standards and contemporary technologies that integrate standard and safety control into one system has been clearly shown to improve both worker safety and productivity. This can provide alternative measures to lockout/tagout in certain situations, improved diagnostics and safety system designs that reduce scheduled and unscheduled downtime.

"Because safety is such a visible part of our everyday operations, employees feel empowered to report potential hazards at first notice. Management reviews all suggestions, so employees readily share safety ideas. The bonus is that, while mitigating risks, suggestions also help improve productivity, quality and efficiency."

Health and Safety Manager,
Dana Incorporated

Address workforce risk with integrated safety

A demographic shift in developed countries and the rapid industrialization of developing countries will leave producers of tomorrow responsible for the safety of a more diverse workforce. These workers – younger, male and female, tall and short, right- and left-handed, differently abled – will be exposed to less risk when companies replace traditional, hardwired systems with networked systems that can pull safety information into your Connected Enterprise. This can help reduce risk while also improving operating efficiency and productivity.

CAPITALIZE ON SAFETY DATA

Safety data can give you deeper insights into safety-related downtime events, including the number of safety events, who's interacting with the safety system, and why and when those interactions are occurring. This data can then inform follow-up actions, such as machine repairs, revised maintenance routines or additional worker training, to help reduce downtime.

UTILIZE ALTERNATIVE SAFETY MEASURES

Contemporary safety systems also enable the use of alternative safety measures to lockout/tagout in certain instances for minor, machine-servicing tasks that are deemed to be routine, repetitive and integral. Alternative measures include:

- Safe-speed monitoring: A safe-speed monitoring device allows machinery to be brought to a safe speed so operators or maintenance technicians can perform tasks without completely stopping the machinery.
- Zone control: A zone-control configuration allows operators and maintenance technicians to stop or slow down a single, specified zone within a production line while all other zones run as normal.

REDUCED DESIGN BURDEN

An integrated safety system uses a single software environment to program discrete, process, batch, motion, safety and drive-based systems, eliminating the need to write programs on multiple controllers. Fewer overall components also allow for smaller panel enclosures to help reduce cabinet size and cost.

Several studies show that younger workers (under age 25), and in particular those with less than one year on the job, have much higher injury rates.

Security

CONNECTED OPERATIONS REQUIRE COMPREHENSIVE SECURITY

Security requirements have vastly changed in recent years as more organizations have adopted smart manufacturing and a connected-operations approach. More connections throughout the enterprise create more potential entry points for a wide range of security threats, be they physical or digital, internal or external, malicious or unintentional.

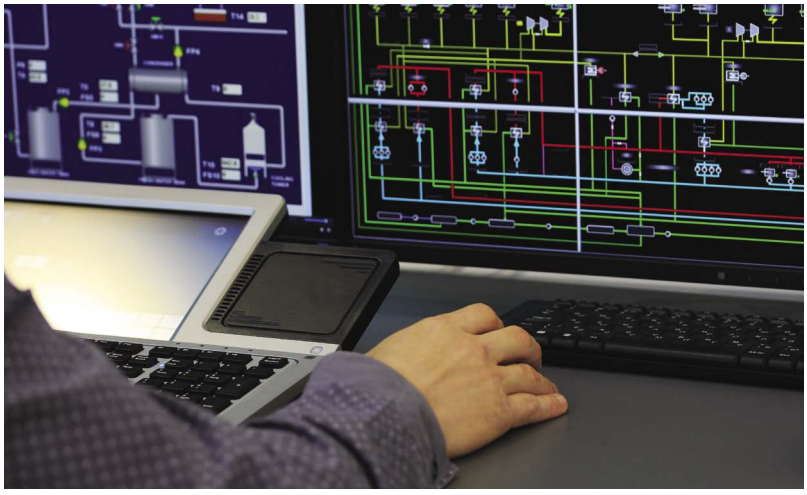
THE RIGHT APPROACH

Given the vastness of today's threat landscape, no single security product, technology or methodology will suffice. A security-through-obscurity approach also cannot be relied upon because it lacks meaningful security measures. Proprietary networks rely on a single vendor and fall short when they don't take advantage of the plethora of other IT tools, security features and innovations available from the marketplace.

Protecting your people, property and proprietary information requires a comprehensive, industrial-security program. It should extend from your enterprise, down to the plant level, and out to end devices.

UNDERSTAND YOUR RISKS AND VULNERABILITIES

A security assessment should be the starting point for any security policy implementation. It will help you understand your current security posture regarding your software, networks, control system, policies, procedures and employee behaviors. It also will identify the mitigation techniques needed to bring your operation to an acceptable risk state.



"Attacks that target [industrial control system] infrastructure continue to evolve and mature. Through a variety of methods, malicious threat actors are introducing sophisticated malware into control systems at growing rates." [1]

[1] ICS Cybersecurity for the C-Level, U.S. Department of Homeland Security, September 2015

Defense in depth

Defense in Depth (DiD) is a multilayered security approach that creates multiple fronts of defense throughout your manufacturing or industrial enterprise. It is based on the notion that any one point of protection can and likely will be defeated and therefore establishes multiple layers of protection through a combination of physical, electronic and procedural safeguards.

Your DiD approach should address security at six levels:

1. POLICY: Your policies and procedures play a central role in shaping workers' behaviors to follow good security practices and confirming the appropriate security technologies are used.

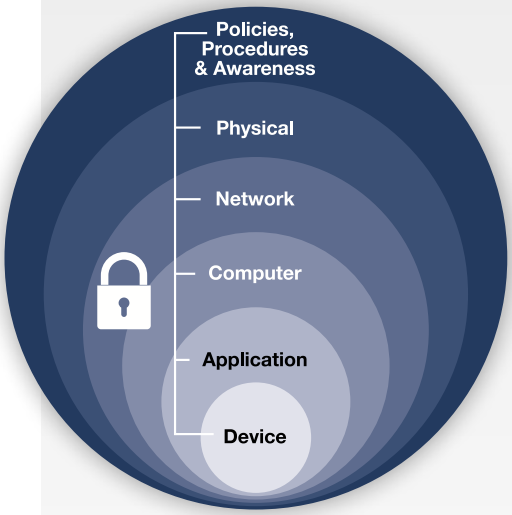
2. PHYSICAL: Physical security should limit personnel access to not only areas of a facility but also to physical network entry points, such as on control panels, cabling and devices.

3. NETWORK: Network security uses safeguards – such as an industrial demilitarized zone (IDMZ), virtual local area networks (VLAN), and firewalls with intrusion detection and prevention systems (IDS/IPS) – to help protect your network infrastructure against cyberattacks.

4. COMPUTER: Software vulnerabilities are the No. 1 means of intruder entry into automation systems. Computer security should include security patch management, antivirus software, application whitelisting and host, intrusion-detection systems. Unused Windows programs, protocols and services also should be removed.

5. APPLICATION: Security measures – such as role-based access and authentication, authorization and accounting (AAA) software – are valuable safeguards at the manufacturing or industrial application level.

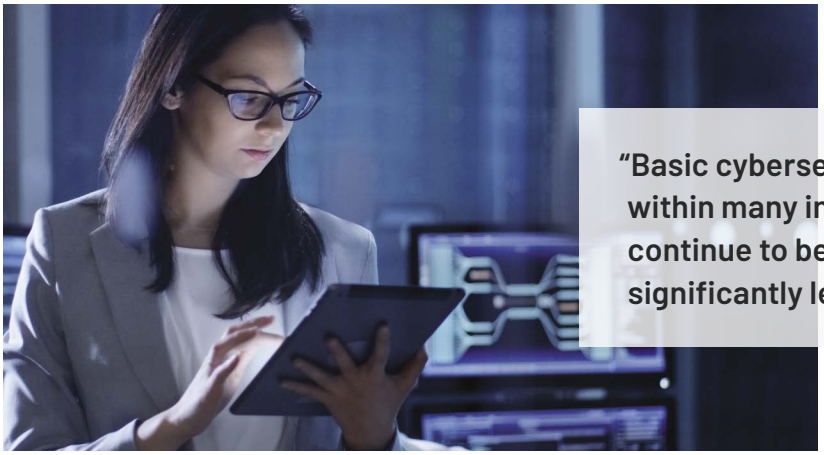
6. DEVICE: Changing the out-of-the-box default configurations for embedded devices can help make them more secure in areas, such as restrictive access and change management.



A security best practice

The Defense-in-Depth security approach is recommended in:

- IEC 62443 standard series (formerly ISA-99).
- NIST Special Publication 800-82.
- U.S. Department of Homeland Security/Idaho National Laboratory Report INL/EXT-06-11478.



"Basic cybersecurity practices within many industrial organizations continue to be an afterthought or significantly less than needed." [1]

[1] ICS Cybersecurity for the C-Level, U.S. Department of Homeland Security, September 2015

Trusted vendors

Your automation vendors are just as integral to helping you meet your security goals as they are your production, quality and safety goals.

Before selecting vendors, request they disclose their security policies and practices. Consider if they follow five core security principles – defined by Rockwell Automation – for designing products used in a control system, including:

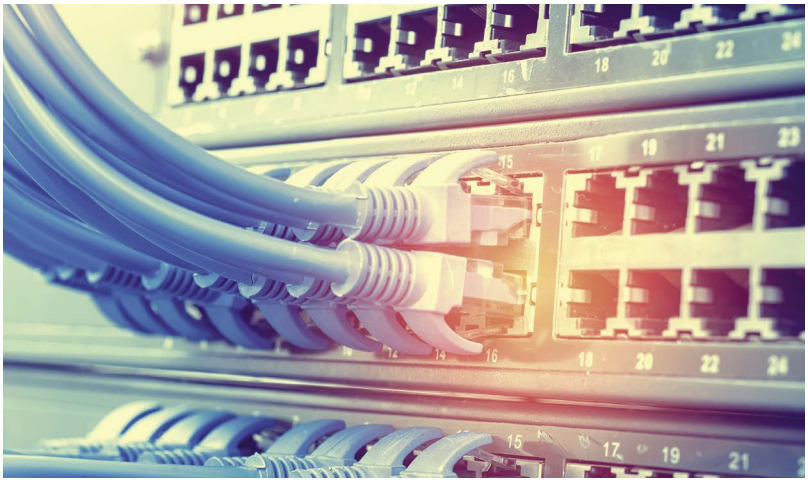
1. SECURE NETWORK INFRASTRUCTURE: Vendors can help keep information in the automation layer secure and confidential. For example, embedded technology can validate and authenticate devices before they are granted access to a network.

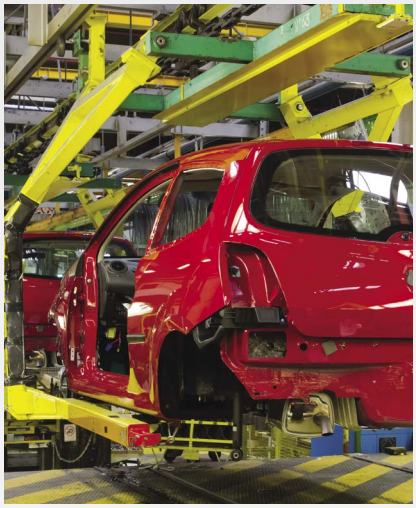
2. AUTHENTICATION AND POLICY MANAGEMENT: Company policies dictate data access levels for employees. Automation products can support these policies using access control lists to manage user access to devices and applications.

3. CONTENT PROTECTION: Intellectual property is the lifeblood of your operations. Your automation solutions can help protect it by assigning passwords to routines and add-on instructions, and by using digital rights management (DRM) to limit users' ability to view and edit device data.

4. TAMPER DETECTION: Built-in tamper detection can detect any unauthorized system activity and alert the right personnel. It also can log key details, such as where the attempted intrusion took place, how it occurred and if anything was modified.

5. ROBUSTNESS: Design-for-security development practices can help confirm vendors' products are secure, resilient and trustworthy. Vendors also should follow the latest security standards, collaborate with other industry leaders in security, and verify products are authentic and free from modifications.





How can The Connected Entetprise help you better manage risk?

During a plant upgrade, Daimler Trucks North America (DTNA) used aspects of the Converged Plantwide Ethernet (CPwE) validated design guides from Cisco and Rockwell Automation to jumpstart the network architecture design and deployment.

The new network provides secure and reliable Wi-Fi connectivity everywhere on the shop floor and in office areas.

Bringing its IT and OT departments more closely together helps DTNA meet its security and compliance requirements.

Now, one converged, plant-to-business network provides secure, reliable connectivity everywhere.

Resources

Rockwell Automation can help you improve risk management in several key areas. To learn more about these solutions, contact a Rockwell Automation sales representative or visit the **risk management page** on our website.

EQUIPMENT OBSOLESCENCE

As much as we invest to extend the life of our products and technologies, no technology lasts forever. If you are ready to modernize or need to develop a modernization plan, **Rockwell Automation tools and services** are available to help you understand and mitigate your risk from outdated equipment.

QUALITY

MES solutions enable more informed decision-making and better quality management throughout the production process and can help ease the burden of compliance.

SAFETY

Free tools can **measure and evaluate your safety program** and **guide you through the development** of your safety system.

Safety assessment services help you comply with current and emerging standards and provide remediation suggestions.

SECURITY

The **Security Assessment Tool** is a free and confidential tool that can help you identify your current, industrial-security risk level and begin to identify methods to mitigate potential security risks.

Network and Security Services cover the full range of security needs from assessments and design considerations to implementation and security monitoring.

PLEASE CONTACT THE FOLLOWING PERSON FOR MORE INFORMATION.

Rockwell Automation

Steve Ludwig
Commercial Programs Manager
swludwig@ra.rockwell.com

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, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SAFETY-WP011C-EN-E – February 2020 | Supersedes Publication SAFETY-WP011B-EN-E – April 2017