Next-Generation Safety Strategies

Managing functional safety and cybersecurity at the system level in industrial manufacturing environments

Better together
Industrial manufacturing is undergoing a revolution. Powered by new levels of connectivity, this revolution offers exponential enhancements in efficiency and flexibility.

While the application of modern, connected devices has created new opportunities for industrial manufacturers to optimize their operations and better meet customer needs, it has also created an array of new safety and security risks.

In this era of interconnected electronics and the Industrial Internet of Things (IIoT), we need a new lens to address these safety risks — a lens that considers functional safety and cybersecurity strategies together at the system level to optimize safety and uptime across modern industrial operations.

We highlight the six key things you need to know about how functional safety and cybersecurity can work together to improve operational safety.

HOW WE HELP

UL Solutions helps asset owners, system integrators and manufacturers navigate the complex technical and regulatory challenges of today's industrial operations. From preventing vulnerabilities in components to finished products to systems, UL Solutions offers customers effective system-level safety and security expertise across the value chain of automated systems.

UL Solutions

Everything is connected

You can’t think about safety and vulnerability on an individual component level. It’s important to consider the role each will play in the interconnected system.

Each separate component may have separately undergone thorough testing and certification, but what happens once it integrates into the wider operating environment? Connecting industrial machinery parts and devices creates new sets of risks. By adopting a system-level approach, functional safety and cybersecurity can more effectively model and assess the impact of installation. Consider all the information coming into each device and all the information coming out of it, as well as the devices’ interdependencies. Multiple elements combine to create new interactions, and these different functionalities generate different responses that require both identification and evaluation.

The systems integrator plays a key role in this respect. Broad knowledge of available technologies is essential for integrating different interfaces successfully. Good products that are poorly integrated at the system level introduce weak points. This negatively impacts both safety and security, as well as overall factory performance.

Your system is only as safe as its weakest link. By establishing a system-level view that reflects hyperconnectivity, industrial operations can better identify potential risks and vulnerabilities early on and make adjustments. This lowers the risk and reduces the need for remedial work later on.

A system-level approach improves safety and security by identifying potential risks early on.

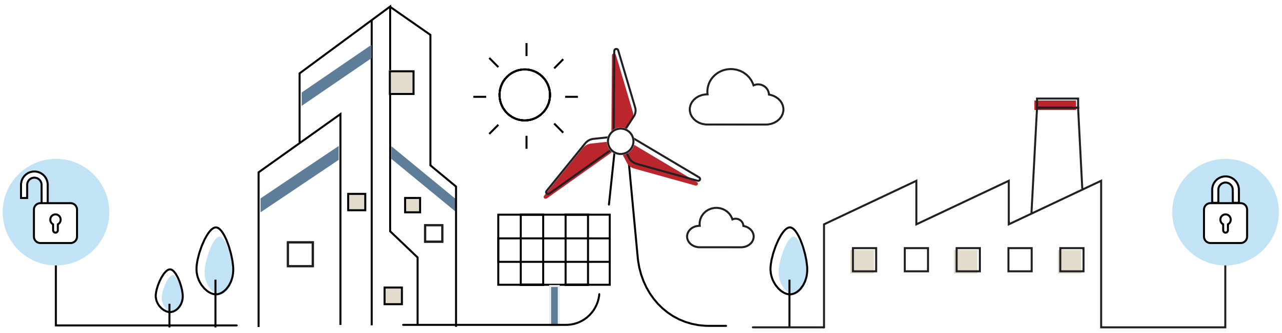
Integrating functional safety and cybersecurity

Industry 4.0 operates on connectivity. Whether they’re fully automated industrial processes or the specific devices controlling individual cobots, electronics underpin enhanced functionality, efficiency and safety.

Within this cyber-physical system, a functional safety strategy must evaluate potential dangers arising from system malfunctions. At the same time, these connected devices now face malicious security threats. This is where the need to think about functional safety and cybersecurity together optimizes the safety and security of your operations. Downtime due to a distributed denial of service (DDOS) or an electronics failure may have the same outcome in terms of health and safety — just a different cause.

Functional safety and cybersecurity can work together to address and prevent these failures more effectively. Establishing a process that integrates functional safety and cybersecurity considerations from the outset lends momentum to the drive toward a common architecture. It’s about looking at what functionality you desire, creating the architecture to achieve that, then systematically evaluating the risk at each stage, whether that’s through external attack or internal malfunction. At both the implementation and operation stages, security controls must never prevent the execution of safety functions.

UL Solutions leads the way in integrating functional safety and cybersecurity.



UL Solutions

Consider safety from the outset

As innovation in manufacturing plows forward, it's critical to integrate safety considerations throughout the process.

As designers create systems, they need to focus not just on how a system can meet its requirements, but also model safety cases at each stage with each component and with each interaction. To avoid remediation costs and needing to make changes to established manufacturing processes post-installation, you need to scope these safety considerations and carry them out at the outset of a project.

Processes are important; good processes are critical. It's about taking the time to think through the proper steps to produce the correct architecture before developing the software and hardware. Modeling, simulation and testing are essential tools in understanding how the different elements interact, as well as identifying and mitigating risks. Increasingly complex automated systems should take advantage of partitioning to optimize scenario testing so that you model only the relevant parts.

Modeling, simulation and testing are essential tools to help reduce risk.

- Identify potential areas of concern
- Break down each concern into a system view
- Break down the system view into hardware and software safety cases
- Write traceability requirements
- Perform a safety analysis of each requirement

Think beyond the human

As the role of automation increases in manufacturing, product designers and safety engineers can no longer rely on the human operator within their safety strategy. Electronics make decisions faster, which means the IIoT-driven environment requires different safety and security considerations. The electronics must now feature built-in safety, and as advanced robotic systems and cobots increasingly proliferate, functional safety must also shift to a system-level approach to reflect this interconnectivity and ensure holistic evaluation. IIoT introduces new cybersecurity considerations around cloud services and the need for evolved individual and system-wide device management.

As the Industry 4.0 ecosystem enables more and more automation across a diverse range of sectors, from energy and utilities to chemicals and materials, a phased approach will transition industrial operations safely and securely to a fully automated future. This works for both retrofitting legacy systems and new capital expenditures. It's about starting with tighter guidelines then gradually widening them as part of a flexible system that can scale and expand as new opportunities emerge. Looking to other industries to learn, work collaboratively and share learnings and knowledge plays an important role in safely advancing automation. Related technology may already exist in a different sector — think sensor technology and automotive — so access to cross-industry expertise can accelerate progress.

System-level functional safety is essential in the Industry 4.0 ecosystem.

Security is not a product

In a dynamic environment, it's not just about a product complying with a safety test; it's about effective system-wide integration to prevent vulnerabilities and enable safer, more secure and uninterrupted daily operations.

The information security management system (ISMS) serves as the foundation that underpins this notion, and getting it right is critical. A comprehensive ISMS ensures that cybersecurity measures have been properly assessed, structured and implemented to minimize the risk from external malicious threats. The ISMS gives asset owners full visibility by bringing together relevant security information for all elements of the industrial operations under a single framework. This complete picture helps asset owners maintain continuous, cost-effective operations by preventing vulnerabilities and reducing the need for remediation — as well as potential liabilities — later on.

Security is also about a product's software development life cycle (SDLC). The threat landscape changes constantly. Ensuring that all component manufacturers have the right development processes in place is key to maintaining ongoing resiliency and protection. System integrators in particular need to be aware of a manufacturer's development processes and to actively interrogate SDLCs, encouraging transparency that in turn will build trust. They need to ask how readily a vulnerability can be addressed and what processes they have in place to ensure consistency (including regression testing, etc.) with new hardware and software releases.

Software development life cycles are a key element in a system-level cybersecurity strategy.

Continuous process optimization

Supporting the long life cycles of industrial machines is critical to maintaining uninterrupted operations and SDLCs, and supplier transparency plays a part in this. Over time, processes degrade, operating systems change, regulations evolve, and continuous updates and patches must be implemented to support the 20+-year life cycles of industrial machinery.

Each stakeholder has a role in optimizing the process (see visual) and implementing improvement cycles to maintain cybersecurity and functional safety. Continuous testing facilitates the transition from one product iteration to another, which builds resilience into the system maintaining security and safety and facilitates the smooth running of industrial operations.

Ongoing process maintenance involves implementing a plan, do, check, act (PDCA) model along with regular audits to support the key business priority of continuous availability. Maintenance service providers play a key role in this process's ongoing success. A flexible approach creates a scalable and future-proof system that incorporates continuous learning to enable expansion as new opportunities and innovations emerge.

Building a resilient system across the stakeholder segments

Asset owner/operator	Has ultimate responsibility for both safety and security, including deploying ISMS.
Service providers/ system integrators	Must consider a range of available technologies to optimize integration and security architecture.
Product manufacturers	Component development processes and component security impact functional safety as well as system security and safety.

UL Solutions

Next-generation safety strategies

In today's era of advancing connectivity, functional safety and cybersecurity need to be considered together at the system level to optimize safety and uptime across modern industrial products and systems.

- **Everything is connected** – Your interconnected system is only as safe as its weakest link. Adopt a system-level approach to functional safety and cybersecurity.
- **Integrate functional safety and cybersecurity**– Highly automated, cyber-physical industrial operations necessitate a more joined-up approach.
- **The earlier, the better** – Consider safety and security at the outset and follow a rigorous process to diminish costly remediation and downtime later on.
- **Think beyond the human** – Build safety into your electronics from the component level up to create an effective, system-level approach to safety and security.
- **Security is not a product** – Interrogate each product's secure development life cycle to minimize the impact of dynamic threats to your operations.
- **Continuous process optimization** – Make sure all stakeholders contribute to life cycle optimization and operational resilience.

With the ever-increasing number of new technologies and devices on the market, we will continue to see a large demand for device certification, systems integration and testing. There is also potential to offer performance verification services related to product lifetime and cybersecurity, which are growing and evolving areas of business.

To learn more about functional safety and cybersecurity key offerings from UL Solutions, please visit UL.com/Solutions.

UL Solutions