BERKSHIRE GREY

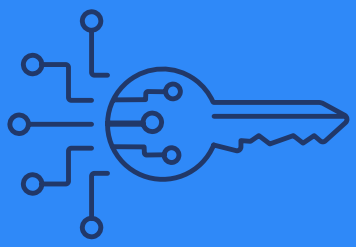
Cyber Security Considerations for Advanced Robotic Automation

Vigilance Starts with Layered Access

Cyber experts often say the weakest links for cyber security threats come from inside a company's four walls. For example, employees clicking on phishing links in emails, or networked machines like copiers and even air conditioners can be direct gateways through a firewall.

When it comes to warehouse automation, vendors often claim that because their machines are inside the customer's network, the systems on the warehouse floor present no greater cyber threat than the building had in the first place. Is this true? Not necessarily.

While a company's network may be secure, there is no guarantee that a cyber breakthrough won't happen. With that in mind, a better approach to warehouse automation is to moderate the type of electronic data that moves from the distribution center management systems to the automation systems. In other words, removing the chance of sensitive company information being compromised by assigning granular, layered access to each separately-secured part of the whole system — like a series of locked doors that a person would need to break through to get to an end destination.



MYTH

Installing automation inside a facility intranet is not a guarantee of overall security. In fact, it can make an automation system a greater threat.

Here we'll address some of the challenges of cyber security and how they relate to robotic automation in the warehouse.

Challenge #1

Wireless technologies, with or without autonomous mobile robots (AMRs) in the mix, present challenges when securing a logistics facility. With the right equipment, they can be targeted without direct physical access — typically from outside the facility.

It's particularly important that networks be protected with proven encryption protocols. In addition, it's good practice for AMRs and other mobile devices to authenticate the source of any information being received and/or shared.

Challenge #2

Cloud metrics collection and data warehousing are key components of advanced automation systems that enable remote support and machine learning. There are two main vectors that need to be secured — the link to the cloud itself, and the data stored in an offsite location.

The cloud link should be secured via strong authentication and encryption to ensure it cannot be exploited for access, and that data is only visible to the desired endpoint. Data leaving the network should be only what is necessary, with sanitization of as much business-sensitive detail as possible.

Challenge #3

Social-engineering attacks against logistics facilities can be particularly effective because of the sheer volume of traffic. With many people moving through them, tracking who has access to which resources is a constant challenge.

Consolidating identity-provider services and using role-based access control is critical when defending against these vectors. This centralizes access through specific routes that can be better protected (with layers like multi-factor authentication and geolocation) and more easily audited to keep necessary permissions up-to-date.

PRO TIP:

Facilities are often well-protected, with rigorous on-site security policies and access restrictions — both physical and virtual. When designing for interaction with people, whether remote-support or visualization dashboards, it's best to leverage this existing infrastructure.

Extending these same services to manage access control to automation both simplifies IT integration and eliminates manual access control steps where social engineering attacks can be targeted.

PRO TIP:

Separating out components of a network makes it easier to secure them. It's much easier to block or detect a vulnerability in a system that is only supposed to be doing a specific task. If an endpoint on your conveyor network suddenly starts trying to send faxes, it's easy to tell something is up.

Fact #1:

When dealing with automation, not every piece of software requires access to every piece of data. Modern systems decompose into many components, from PLCs controlling conveyance and safety equipment, to the application software that communicates with WMS and WES systems.

Fact #2:

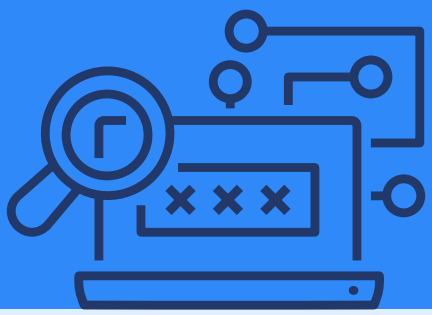
Good network security design splits components into multiple network segments — which not only helps with traffic monitoring and management, but also greatly simplifies security.

In summary, cyber security for logistics automation is not simple, but it should follow the same guiding principles already in place for company-wide data protection. While it's easy to lean on physical and external infrastructure access to assume a system is secure, that leaves systems vulnerable when those defenses are compromised, which happens constantly in the real world as new exploits are discovered and social-engineering attacks succeed.

Berkshire Grey designs every component of our automation systems with security in mind, because resistance to attack is measured in the composition of all layers of defense, not just the first one.

At Berkshire Grey, we employ a multi-layer approach to security — restrict information, restrict access, and encrypt data. This ensures that not only is it difficult to compromise the system, but if a component gets compromised, it's difficult to use that to get to sensitive information or exploit any other part of the system.

This redundant approach comes from practical experience defending our production systems against real-world social-engineering attacks, zero-day exploits, and data leaks. New vulnerabilities continue to be found or created, but the best defense is one that puts up a fight if any specific layer is compromised.



About Berkshire Grey

Berkshire Grey automates complex supply chain processes and optimizes fulfillment operations, accelerating business growth through AI-enabled robotic automation. Our modular and customizable solutions can be leveraged across eCommerce fulfillment, store replenishment, retail, grocery and convenience, 3PL, and package handling and logistics. **Contact us today to learn how we can help boost your business.**

 | +1 (833) 848-9900 | www.berkshiregrey.com

BERKSHIRE GREY