THE REINFORCEMENT OF SECURITY FOR INDUSTRIAL OPERATIONS

Todd Rigby, Director of Sales at Rajant Corporation explores how to increase employee safety and efficiency in an era of automation

In the era of digitalization, countless industries are increasingly relying on advanced robotics and internet of things (IoT) systems for essential tasks. This burgeoning amount of digital assets presents new risks and challenges for industry professionals, underscoring the need for robust cybersecurity measures that surpass the current industry standards of today.

Let's evaluate how new physical and cybersecurity measures will be needed in future industrial spaces and how to best prepare for the dangers posing a threat to critical operations in the era of automation, machine learning and advanced robotics.

Well-planned security measures will be necessary

Just because a system is automated or reliant on robotics does not mean it's inherently secure. The increasing intelligence of these machines also means a growing susceptibility to security concerns. Therefore, integrating well-planned, robust security measures is not just advisable but absolutely necessary for industries to protect operations from potential threats. So, how can industries using robots for essential tasks solve security problems before they arise?

Threat to digital infrastructure and employee safety

Despite the efficiencies and advantages brought by emerging technologies, these assets also open up avenues for security breaches. Bad actors could not only compromise these machines' sensing and reporting capabilities but can also interfere with their physical operations. Such disruptions could significantly damage the infrastructure and in certain circumstances, pose severe dangers to employee safety.

Industry 5.0 facilities will operate with a hybrid automation style – robots, machines and humans all working harmoniously for the efficient excavation, manufacturing, transportation or refinement of materials and goods. Many industrial operations are already considered dangerous work environments; if machines and other assets are at risk of being compromised, these places could be too hazardous for human workers to be present altogether. Unless these risks are mitigated, the time it will take to realize the full productivity of these new technologies will be much greater.

Threat from outside interference – a greater risk than stolen property

Outside interference poses more than just the risk of stolen property. The repercussions of a security breach can extend far beyond the theft of intellectual property, finances or data. When robotic operations are compromised, the ripple effects can be deadly, disrupting critical functions within industries like mining, oil and gas, agriculture and heavy construction.

Undoubtedly, there will be an increasing need for strong cybersecurity measures for the systems performing the work and the software/network powering their cooperation. Companies will need to invest in robust and evolving antivirus firewalls, failsafe measures and emergency response plans to help mitigate the damage these threats pose.

Ensuring security without breaking the bank

While it's undeniable that robotic solutions and their corresponding security measures can be costly, organizations don't necessarily have to break the bank to ensure their systems function properly and with an adequate level of security. There are ways to deploy cost-effective solutions that strike the right balance between security and affordability.

One option, which will save a lot of money, is to look for communication networks with robust security integrated as part of the networking protocol. Ensure you have a strategy in place to address both wired and wireless security. Lastly, don't underestimate physical security. If your wireless infrastructure has a live Ethernet port, with no access control, you're likely inviting any passerby to tap into your sensitive data.

Infrastructure and security

One of the fundamental aspects of ensuring secure robotic operations is having the right infrastructure in place. This includes reliable connectivity, computing power and networking capabilities. Without these foundational elements, it will be challenging to implement robust security measures that can protect against potential threats. Encryption technology to guard against unwanted network intrusion or signal disruption will be essential.

To be more specific, you need to ensure your network is capable of encrypting device IP addresses as well as the data stream. This is necessary to prevent man-in-the-middle attacks and packet captures.

Furthermore, if your network relies on a cloud-based management platform, you should ensure it has security measures such as two-factor authentication. Locally run, network management applications are preferable. You should also regularly run diagnostics checks to identify vulnerabilities and to prevent bad actors from accessing internal databases and internet-capable assets. Additional stopgaps, like intelligent software that notifies administrators of unknown devices or potential breaches in the network, will help keep oversight aware of when threats may be manifesting.

Employee training

One of the most cost-effective and critical ways to ensure a robust defense is employee training and awareness. While high-tech solutions form the first line of defense, the human element can often be a weak link. Employees need to be educated on the best practices for maintaining the security and integrity of the systems they interact with. This includes limiting access to critical resources based on roles, understanding the importance of creating strong, unique passwords and using additional authentication factors for remote employees to access data, recognizing phishing attempts and following proper protocols when accessing confidential information.

Regular audits and updates

Routine audits of the existing security measures help identify potential vulnerabilities and address them before they can be exploited. These audits should be comprehensive, examining all aspects of the system, including the physical hardware, the network infrastructure, the firewall and antivirus systems, as well as software vulnerabilities.

It's also important to regularly update all systems and software. As cyber-threats continue to evolve, so too must the measures put in place to combat them. Regular updates can provide essential patches for known vulnerabilities and improve the overall performance and stability of the system.

Secure networks

Investing in a secure network infrastructure is another important way to protect robotic operations. This includes using encrypted connections, virtual private networks (VPNs) and other security protocols to ensure the transmitted data is protected from interception or tampering.

Organizations can also invest in intrusion detection and prevention systems. These tools monitor the network for any signs of a breach and either alert the appropriate personnel or take immediate action to thwart the threat. Disabling unused publicly accessible Ethernet ports can help.

> **"INTEGRATING WELL-PLANNED, ROBUST SECURITY MEASURES IS NOT JUST ADVISABLE BUT ABSOLUTELY NECESSARY."**

Reputable vendors

Partnering with reputable vendors can help ensure the security of your information systems. These vendors should have a proven track record in delivering secure solutions and provide ongoing support.

While it is true that the digitalization of industrial operations presents new challenges, these can be effectively addressed with the right strategies. By investing in a combination of the right infrastructure, employee training, regular audits and updates, secure networks and reputable vendors, organizations can ensure their operations are secure at an affordable price point. ▪