TXOne Networks

2021
/Q4

Securing Autonomous Mobile Robots

txOne™
networks

TXOne Networks

Securing **Autonomous Mobile Robots**

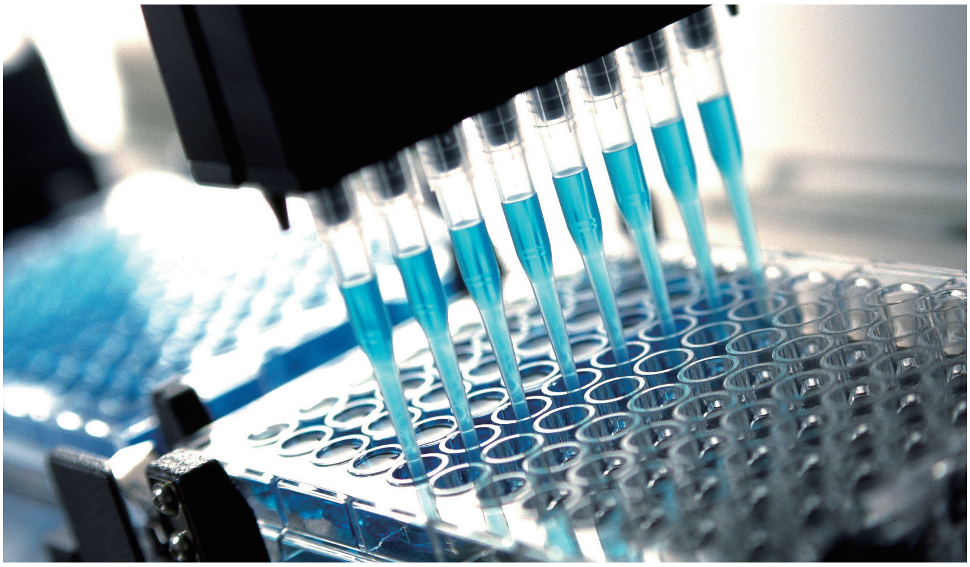
txOne™ networks

Securing **Autonomous Mobile Robots**

Executive Summary

Robots bring advantages that have long been crucial to the medical and pharmaceutical industries. For example, robots allow stakeholders to ensure that a recipe is 100% correct 100% of the time, and that the usage of precious substances can be maximized through this unerring precision. Medical applications for robotics have advanced even more rapidly since the onset of the COVID-19 pandemic.

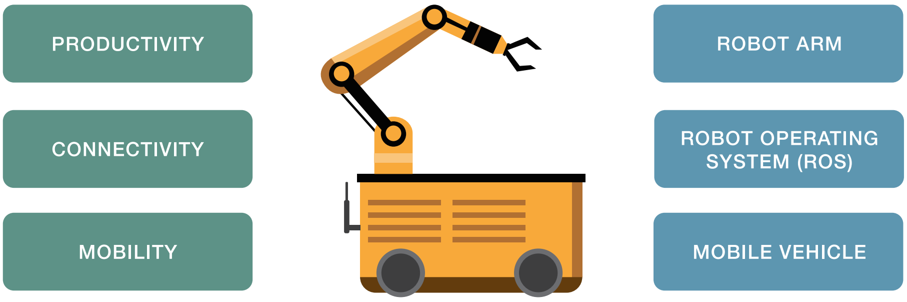
In Thailand, the robotic arm "AutoVacc" system is used to meter out COVID-19 vaccine doses so precisely that it can get 12 doses from a vial in 4 minutes – in addition to handling the process much faster, it also shows a 20% increase from the 10 doses expected when doses are drawn manually.[1] As of this writing, increasingly automated and mobile robots are being adopted across the front lines of the COVID-19 pandemic. These robots are able to sterilize environments, handle all phases of testing people for the virus, and transport supplies for doctors and nurses. When they take over these jobs they also streamline workflow, reduce the risk of transmission, and reduce exposure.[2]



[1] Juarawee Kittisilpa, "Thailand develops robotic system to squeeze out more vaccine doses", Yahoo News, Aug 25 2021

[2] Sai Balasubramanian, "Robots Have Become An Essential Part Of The War Against Covid-19", Forbes, Jan 26 2021

Autonomous mobile robots' (AMRs) range of work-saving and work-perfecting capabilities makes them as crucial to other forms of manufacturing as they are to the pharmaceutical and medical industries. They are able to autonomously navigate spaces with their wheels while using their multi-jointed robot arm to carry or manipulate objects, and their sensors allow them to maneuver or wait as necessary while moving, ensuring the safety and uninterrupted work of personnel and assets around them. However, to make this autonomous movement possible, they must have a fast wireless connection to the internet, and with connection to the internet comes the risk of cyber attack.



PRODUCTIVITY

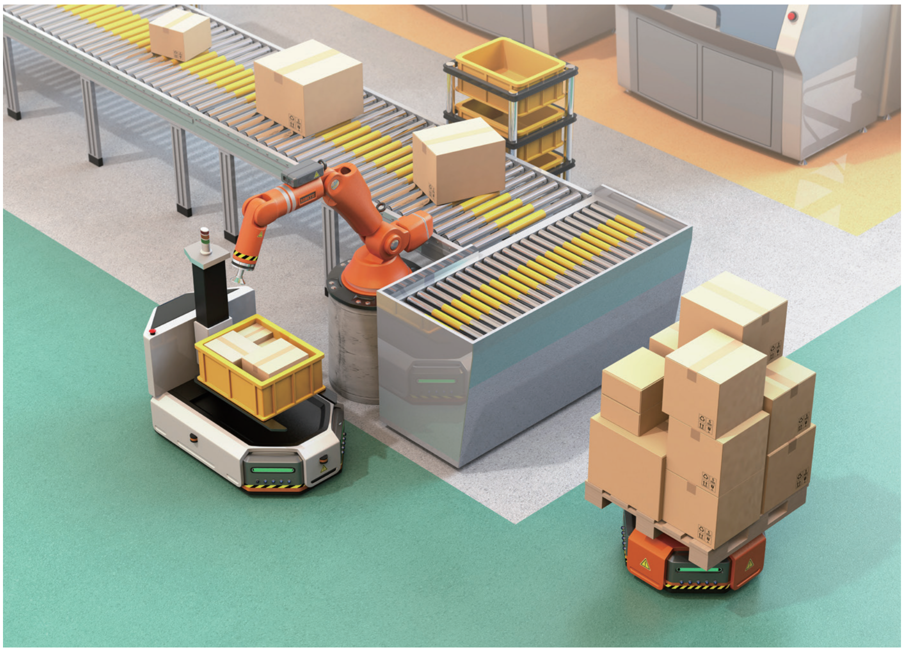
CONNECTIVITY

MOBILITY

ROBOT ARM

ROBOT OPERATING SYSTEM (ROS)

MOBILE VEHICLE



Cyber Attacks on AMRs

Computer numerical control (CNC) technology is often called 'the mother of industry', as it led to immediate massive advancements in many different verticals at the moment of its birth. Similarly, robot arm systems are 'the mother of automation'. Thanks to their precision, ability to work with extremely heavy objects, and ability to operate safely in situations dangerous to humans, robot arm systems have become essential to modern work.

However, robots like these cannot exist without data input and output over networks. Meanwhile, the last few years have shown the resourcefulness and dedication of attackers – if there is data flowing between assets, or back and forth between assets and the cloud, operations can be compromised and disrupted. The IoT readiness of autonomous mobile robots is a double-edged sword, able to provide convenience to stakeholders and attackers equally well if this functionality is improperly secured. Furthermore, robotic assets, like many modern operational technologies, were originally conceived to work in isolation without a modern network. This creates complications when we are securing them for an industrial IoT environment.

TXOne's experts predict that in the near future a wave of operational technology (OT) cyber attacks will be directed at robotic devices, and that it's just a matter of time before we see a major cyber attack in the news based on targeting robotic assets. According to Trend Micro's case study *Rogue Robots: Testing the Limits of an Industrial Robot's Security*, there are five potential types of cyber attacks on robotic devices:[3]

1 Production outcome alteration or abotage

2. Ransomware-type schemes

3. Physical damage

4. Production line process interference

5. Sensitive data exfiltration

It must be noted that this cyber attack classification for robotic devices was created during research on non-mobile robots. One or more compromised AMRs is capable of creating much more havoc than was possible with robots that were not yet autonomously mobile. AMRs normally have three main parts: the wireless communication device, the robotic arm and the automotive guidance vehicle (AGV) itself. The wireless communication device brings connectivity, the robot arm brings

[3] Federico Maggi, Davide Quarta, Marcello Pogliani, Mario Polino, Andrea M Zanchettin, Stefano Zanero, "Rogue Robots: Testing the Limits of an Industrial Robot's Security", Trend Micro Forward-Looking Threat Research and Politecnico di Milano, May 3 2021

utility, and the AGV brings mobility. From the perspective of operational integrity, connectivity is the crucial factor because it allows the mobility and utility of one or more AMRs to be directed in concert, allowing them to be centrally managed as well as to perform advanced tasks. If this connectivity is compromised by an attacker, these mobile assets have the potential to cause catastrophic disruption.

When securing AMRs, defensive solutions are unusable if they cannot meet the baseline of being lightweight, scalable, and interoperable. Determining the needs of AMR cyber defense and configuring the ideal deployment to match it is a complex process involving input from many experts with differing specializations. To more effectively leverage their respective strengths, TXOne Networks and Joanneum Research have collaborated to assemble, test, and complete validation for a proof of concept for securing Joanneum Robotics' flagship AMR, the CHIMERA mobile manipulator, against cyber threats. TXOne's specialists have gone on to successfully deploy this proof of concept to defend a variety of other AMRs.

Goals for the Joanneum CHIMERA Proof of Concept

1. **Defend the AMR against DoS & brute force attacks.**
2. **Shield vulnerabilities in the AMR as well as in its AGV and robotic arm subsystems with virtual patching.**
3. **Create a reliable use case for applications in the healthcare and robotics industries**

Equipping an AMR to Repel Cyberattacks

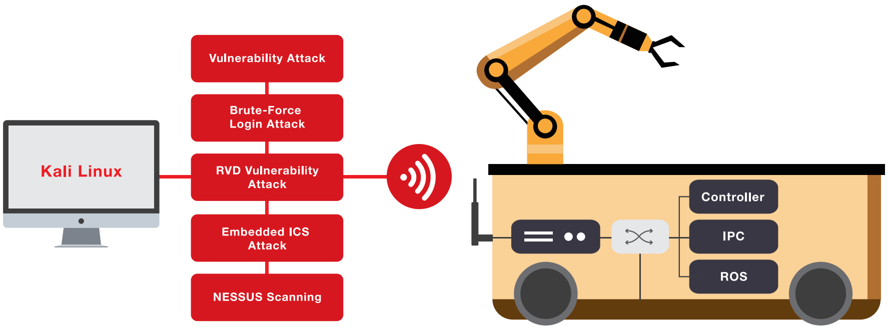
There are three crucial concerns for any solution that will be integrated into transporter-mounted robotic arms. First and foremost, vulnerabilities inherent to Robot Operating System (ROS) must be shielded, preventing intruders from taking advantage of them to disrupt or take control of the AMR. Secondly, running robotic hardware from a variety of vendors creates management and maintenance issues that must be solved – a complicated process unless a solution is available that can be adapted and customized to different assets. Finally, these assets also tend to have long lifespans, meaning that more and more vulnerabilities will be discovered over time, and any defensive appliance that will be viable must be supported by updates that can shield newly-discovered vulnerabilities from exploitation. The key point here is that securing the accuracy, safety, and integrity of AMRs requires a few different kinds of flexibility.

This set of defensive solutions must allow operation with full cloud connectivity. Robotics applications (advanced scenarios) for AMRs require supporting technologies that create cloud support, network infrastructure, and visibility. Authentication and authorization must be an overarching part of supporting technologies to protect the operational integrity of the device from interference, especially with regard to shielding the vulnerabilities inherent to ROS. After another decade, operations will commonly integrate AMRs into their DevOps procedures for ease of application deployment from the cloud, which will change the nature of how cost and scalability support ease of deployment and re-deployment. Deployed security solutions can harm the functionality of these supporting technologies if they aren't tailored for OT environments.

In addition to these technological and organizational concerns, there is also the practical issue of sizing. The AMR's interior is tightly packed with components and cabling and has very little unused space. Because of this tight fit, the solutions chosen for deployment within the AMR must be small, easy to install, and easy to maintain.

The Joanneum CHIMERA Proof of Concept for Cyber Defense

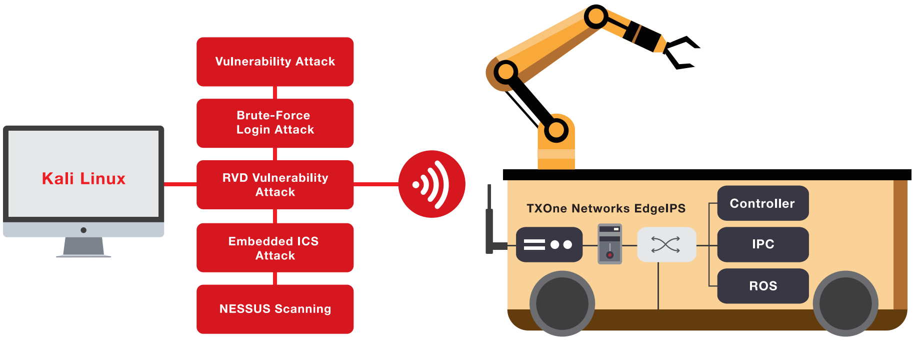
In a typical AMR, one switch connects two subsystems – an AGV and a robot arm system – in addition to connecting to an industrial PC (IPC) and a computer running ROS. The switch puts the AMR on the network and reaches the cloud via a connected wireless network (wi-fi or LTE) adapter, to which it is connected by a single cable. This allows the AMR's subsystems to connect with the centralized management system over the network. The single cable running between the switch and the wireless network adapter is the ideal deployment position for an appliance that can secure the AMR's operations.



5 Common Attack Strategies Likely to be Leveraged Against AMRs

1. **Attacks based on commonly-exploited CVEs for Linux and UNIX**
2. **Brute force login attacks**
3. **Common embedded and ICS attacks**
4. **Vulnerabilities documented in the Robot Vulnerability Database**
5. **Vulnerability scans with programs such as NESSUS**

Firstly, the solution needs to block attacks based on commonly-exploited CVEs for Linux and UNIX, brute force login attacks, and common embedded and ICS attacks before they reach the target, and any event that could be related to an attack must be logged for analysis. Secondly, it must secure vulnerabilities listed in the Robot Vulnerability Database, such as exploiting OpenSSH to conduct a remote denial-of-service attack. Attacks like this can be used to hit the key controller CPU and lock up 99.9% of an asset's resources, freezing the device and disrupting its functionality. Third and finally NESSUS, a vulnerability scanner commonly used in cyberattacks, must be blocked from successfully performing a scan, and after the detection the scan attempt must be logged. Every type of attack and attack-related behavior that AMRs are at risk to must be reliably repelled and documented.

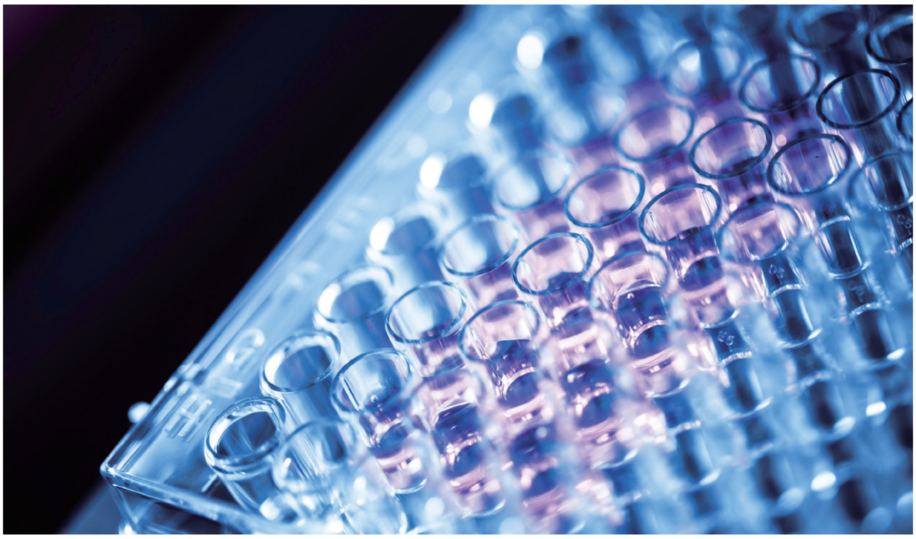


Taking these 5 types of attack strategies into consideration, it's necessary to find a solution tailored to an industrial setting. Basically in the protection of industrial assets it's crucial that the defenses will not interfere with asset functionality and can be deployed in potentially harsh environments. TXOne Networks' transparent security box, "EdgeIPS" (IPS - Intrusion Detection System) was developed with this in mind - it can adapt to secure customized operating systems without interfering in their operations, and it's ruggedized to work for a long time in industrial environments. After several rounds of testing both teams of experts were able to agree that the EdgeIPS is an ideal solution for defending AMRs from cyber threats.

Practical Industrial Defense

The proof of concept was based on TXOne Networks' EdgeIPS™ next-generation IPS security boxes, and this methodology has since been proven to work well with AMRs from other vendors too. For this proof of concept, an EdgeIPS was placed within the AMR between the control system and wi-fi adapter, where its small form factor makes it a convenient fit. Thanks to its convenient design, security engineers will be saved from much of the work of maintenance by being able to manage the deployed nodes from a single centralized console TXOne Networks' OT Defense Console.

AMRs for use in the development of COVID-19 vaccines were the focus of this proof of concept. There are three key challenges to this. First is the use of mixed hardware in robot fleets from different vendors including UR, ABB, Omron, MiR, Mitsubishi, Yaskawa, and Kuka, which results in different levels of access to robots and different vulnerabilities. The second challenge is the vulnerabilities inherent to ROS, which is the standard middleware used for hardware-agnostic interoperability in AMRs. Finally, because of the life-critical importance of this work there is a high risk of bad actors targeting vaccine- and healthcare-related work sites, so the cyber defense on these assets needs to be ironclad.



TXOne Networks' EdgeIPS is the only IPS that can provide native, authentic IT-OT integration. It protects the AMR from both denial-of-service (DoS) and brute force attacks, which are common methods of attempted disruption. Its virtual patching feature is a network-based behavior that allows it to put a shield around vulnerable equipment without requiring any alteration to the protected device, allowing it to vulnerabilities present in the AMR's subsystems or OS without disrupting productivity or the operational ecosystem. This protection for OT environments is native to TXOne's Edge series – EdgeIPS, EdgeIPS Pro, and EdgeFire.

Any solution is only as good as the research behind it. Each IPS that will be an effective cyber defense for AMRs needs to be backed with an understanding of the vulnerabilities inherent to the AMR itself as well as its AGV and robotic arm subsystems. As of this writing, TXOne Networks is the only team of cybersecurity specialists creating an appliance specifically maintained to mitigate these vulnerabilities, empowering the Edge series' virtual patch technology to cover most robot arm system and ROS vulnerabilities. TXOne's researchers are dedicated to continued ROS vulnerability research so that they can constantly output digital vaccines to protect vulnerabilities and seal them off from being used to launch attacks or disrupt productivity.

EdgeIPS' robustness combined with its small form factor was another factor that led us to this proof of concept. It is able to fit into and secure any system, even when that means fitting into a very cramped and already highly-utilized space. Finally, the appliance is easily maintained without requiring the engineer to open the AMR's body up and access it physically, and has a long mean time between failure (MTBF) of 700,000+ hours.

Lastly, a security solution that cannot work with the OT protocols in use can be almost as damaging as a cyber threat to work site productivity. EdgeIPS can work directly with OT protocols to provide security without disruption or delays to operations. It generates trust lists and special controls based on these protocols, and outputs detailed, easily-referenced logs of activity and incidents. After rigorous testing, TXOne Networks and Joanneum Robotics concluded that EdgeIPS is the ideal solution to balance the inextricably linked needs of AMR protection and work site productivity.

Conclusion

Robot arms have long been known as one of the keys to the next generation of industry, and manufacturers are moving more and more into this highly-automated style of deployment every day. Equipping robotic arm systems with mobility increases their work potential many times over, but also creates an urgent need to secure them effectively. As the technology improves, robotic assets will continue to take on more unique, complex, or sensitive jobs. Keeping this 'mother of automation' safe from cyberattacks will be crucial to the next wave of operational development.

www.txone-networks.com
support@txone-networks.com

txOne™
networks