TECHNOLOGY AND IIOT > INFORMATION TECHNOLOGY

New RFID Forklift System Can Improve Material Handling

The system utilizes an acoustic sensor, broad beam antenna and controller logic to identify an RFID pallet tag after it has been loaded onto the forklift

Compiled Adrienne Selko

JAN 22, 2009

M/A-COM Technology Solutions, Inc., a provider of microwave and RF design solutions and products, recently announced the introduction of a its new sensor-based RFID Forklift System. The system automatically records an RFID tagged pallet's exact storage location during handling and slotting processes, without requiring the operator to initiate traditional manual data collection methods.

"Our sensor-based RFID Forklift System automates and streamlines materials movement and management tasks," said Kevin Anderson, Product Line Manager, M/A-COM Technology Solutions. "From increasing inventory accuracy and reducing material losses to processing more pallets per shift while reducing labor costs, this forklift system brings immediate and significant cost savings to the material handling and inventory management operations."

The system utilizes an acoustic sensor, broad beam antenna and controller logic to identify an RFID pallet tag after it has been loaded onto the forklift. The system then identifies a pallet storage location, utilizing a narrow beam antenna, laser-height sensor and controller logic to confirm that the specific pallet has been picked up or dropped off at that location. These slotting transactions are fed to the enterprise system via WiFi connectivity. The RFID Forklift unit employs a high-performance Impinj Speedway reader loaded with fully released and supported forklift firmware.

LATEST IN INFORMATION TECHNOLOGY

Changing Requirements and Security Concerns During COVID-19

APR 30, 2020

COVID-19 Crisis

Department of Commerce Extends Comment Period for Huawei TGL

MAR 25, 2020

Cybersecurity

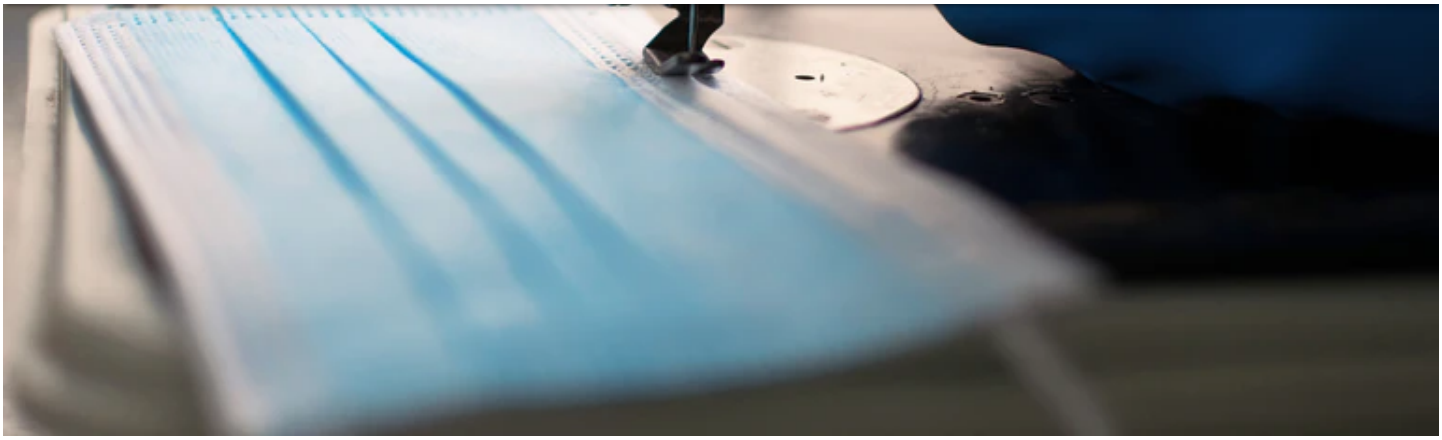
Webinar: Leveraging Analytics to Survive Manufacturing's Current Economic Crisis

Webinars

Webinar: Industrial Transformation Done Right – Avoid Pilot Purgatory

Webinars

David Moreno | Dreamstime.com



COVID-19 CRISIS

Changing Requirements and Security Concerns During COVID-19

Successfully pivoting and working remote mean understanding and addressing qualifications and security concerns.

Peter Fretty

APR 30, 2020

Operating within this temporary new norm isn't easy for anyone. And, numerous considerations exist for manufacturers keeping the lights on during today's new norm. This is true whether the business is pivoting to help address urgent needs resulting from the ongoing pandemic or actively leveraging a mix of on-premise and remote technologies to effectively operate.

While digital technology has proven empowering as increasingly more manufacturers leverage remote technology, navigating the new broader threat landscape is rightfully a viable concern. And, as a result, manufacturers need to plan and properly secure devices that are fast becoming more complex machines with complex functions, explains Ellen Boehm, senior director of IoT product management at Keyfactor.

"Any new connected device expands IoT attack vectors; cyber-attackers are exploiting the global crisis, and hardening device security is critical. In the case of connected medical devices, security risks can be life impacting," says Boehm. "The pandemic is changing the way we work today, but it will also shift the industry moving forward. Manufacturers must

control systems that reduce human interaction. This is the reality today, and companies will have to accept it as a long-term scenario."

Andy Riley, executive director at Nuspire tells IndustryWeek, the move to broader mobile device and remote access usage during this pandemic will highlight the continued erosion of the network perimeter and focus attention on endpoint security. “Companies are sure to find gaps in their remote access and mobile device strategies through this increased attention resulting in improved configuration standards that will provide benefits well after the emergent operations period is over,” he says.

Unfortunately, unsavory characters recognize the opportunity to exploit the current environment. And, as such, COVID-19 phishing emails are everywhere. According to the latest Bitdefender research, the curve of coronavirus-themed cyber threats has not flattened, and the manufacturing vertical is one of the hardest hit.

“The global daily evolution of COVID-themed threats shows consistent effort from cybercriminals and a continued interest in exploiting fear and misinformation about the global pandemic to get victims to click on malicious links, open malicious attachments, or even download and install malware,” report authors write. “Coronavirus-themed threats will likely continue under the form of spear phishing emails, fraudulent URLs and event malicious applications, all exploiting fear and misinformation in order to trick victims into unwillingly giving away personal, sensitive or financial information.”

Pivoting to medical?

Other considerations exist for those manufacturers now entrenched in creating medical grade devices or personal protection equipment. After all, equipping a non-medical factory to manufacture medical devices is a serious undertaking, according to Deborah Jennings-Conner, Director of Global Life & Health Sciences, Regulatory & Testing Assurance at UL.

“The FDA governs this through the Quality System Regulation QSR CFR 21 part 820 which is a framework of basic requirements for manufacturers to follow. Having a sound quality management system (QMS) is key to ensure that the products produced which

occur from improper job performance. Design controls are one of the major causes of device recalls and the manufacturer must ensure the device design is correctly translated into production specifications and produced according to plan. Design changes pertaining to the product, components, packaging, labeling, or similar, cannot arbitrarily be changed mid-production. Procedures covering processes from purchasing to production, to dealing with non-conforming products from the production line are a few examples of areas must be documented and maintained. Under the Emergency Use Authorizations (EUAs) during the COVID-19 public health emergency, the FDA may issue guidance allowing flexibility in demonstrating full QMS compliance in order to help expand the availability of critical medical equipment and their accessories during this pandemic."

According to Conner-Jennings, production and process controls are key areas a manufacturer must not take lightly. "Establish procedures and implement processes to ensure the product produced meets the design specifications. Substitution of components not approved by the design, making software changes that have not been validated, and allowing non-conforming finished products to be shipped, are examples of a manufacturer's inability to produce a product that meets its predetermined design specifications and which may not be safe and effective in the field," she says. "These critical non-conformances should not occur within a well-designed medical device manufacturing process and could lead to adverse events that are required to be reported to the FDA."

Security Best Practices During the New Norm

- **Focus on Phishing.** User awareness training on phishing is crucial, explains Riley. "Organizations will be working with new suppliers, which opens the door to additional phishing opportunities," he says. "Employees will be receiving emails and communication from unfamiliar sources making them more susceptible to interacting with malicious links, documents, or passing along sensitive information."

realm. Protecting the business starts with updating, patching and ensuring the use of strong (not default) passwords. “New machines may be brought in that IT staff is unfamiliar with. IT staff will need to research these devices to fully understand what they are vulnerable to and what exactly they are introducing to their networks,” says Riley.

- **Vulnerability scanning:** Vulnerability scanning is crucial whenever introducing new devices to the network – whether its IT or OT. It is possible that there are no vendor patches available to fix issues and security personnel must understand the risk associated with any device, explains Riley. “Security teams can consider DMZing any equipment that are a higher risk to minimize the ability for attackers to laterally move throughout the network or to spread malware,” he says.
- **Tighten settings**. Whether remote operation requires new equipment or reimagining the use of existing equipment, remote operation often requires external facing settings. However, Riley recommends that security teams speak with product vendors to receive trusted IP address ranges and secure devices to only allow external communication from those devices.

LATEST IN COVID-19 CRISIS

Daily COVID-19 Updates: May 1
MAY 01, 2020
COVID-19 Crisis

CDC: Over 4,000 Meat Workers Have Contracted COVID-19
MAY 01, 2020
COVID-19 Crisis

Why Companies Doing the Right Thing Matters More than Ever
MAY 01, 2020
Leadership

Load More Content