As Autonomous Mobile Robots Advance in the Delivery and Logistics Industry, How Can We Ensure and Maintain Our Safety and Theirs?

Autonomous mobile robots (AMR) in the delivery and logistics industry have taken the world by storm. Still, we need to ask: How will they continue to deliver without being tampered with, and what technology is used to keep operations safe?

What is a Delivery Bot, and How Does it Work?

A compact box on wheels, delivery bots are essentially AMRs that transport retail goods to their destination via a delivery app, whereupon the consumer retrieves the goods inside by unlocking it with a unique auto-generated code.

The safety of AMRs seems foolproof. AMRs encompass computer vision, GPS, all-surrounding cameras, ultrasonic sensors, tamper detectors, and intelligent traffic avoidance. Powered by deep learning and edge devices, AMRs continuously evolve to optimize logistics and improve customer satisfaction. Rain or shine, these autonomous mobile robots promise a zero-emissions delivery, promoting a greener city and reducing time and money on physical manpower.

When AMRs and Remote Edge Systems Come Under Attack

However, vandalism and theft often become significant concerns. Without human on-site vigilance, how can a robot protect itself and the retail goods they are out to deliver?

When delivery bots are forcibly shut down and tampered with by intruders, the AMR cannot utilize its motion and vibration sensors to detect and send out tampering alerts to prevent vandalism and theft of goods. This leads retailers and AMR companies to lose business and trust in the operations. Thankfully, Allxon provides powerful edge solutions to ensure all AMR technology can continue to operate as normal even in the event of an attack.

Edge Solution Conquers Safety Challenges

Access to Allxon Portal allows for the effective monitoring of edge device operations. Managed service providers (MSPs) can check on AMR operations such as power statuses (whether the device is on or off), GPU performances, battery usage etc.

In the event of a tampering incident, when the power status of the targeted AMR appears to have been shut down (abnormal), Allxon instantly sends out alerts to the business to take immediate action. Allxon swiftDR OOB Enabler also enables superior functions such as the Allxon swiftDR for Power Cycling to instantly power the AMR motherboard back ON to normal operations, even if outside users have forcibly turned it off. This powerful rapid disaster discovery feature instantly resumes its sensor functions to set off voice warnings and sends alerts back to the server.

Allxon provides businesses with an effective turnkey solution using their most in-demand SaaS-In Chip technology, making it possible to develop and add customization for Out-Of-Band management services onto an open, integrated platform for limitless remote management. In partnership with Nuvoton, developers can use Allxon plugIN on the Nuvoton NUC 980 Chili Board to build more custom OOB tampering features specific to the AMR operation needs. e.g., surveillance, GPS tracking, electric, spring, or magnetic lock sensors to its safety protocols, thereby reinforcing AMR edge AI protection.

Allxon: Reinforcing Safety in AMRs and its Surroundings

As more AMRs are introduced worldwide, technical malfunctions and temptations of tampering are guaranteed. Allxon ensures AMRs are protected and secure to not only protect the devices and save companies exorbitant financial costs, but it can uphold societal values and the safety of its people.

Read more on customizable OOB features with Allxon

Find out more about Allxon OOB technology