Enhancing Security and Reducing Expenses With Robotics

June 2020

SIA
SECURITY INDUSTRY ASSOCIATION

Enhancing Security and Reducing Expenses With Robotics

How can robots enhance security?

While people generally think of robots as machines that are designed in a way that mimics some human actions and characteristics, a much broader definition is more technologically accurate. One way to describe a robot is "a piece of hardware powered by software that performs any task." In those terms, of course, robots are already well integrated into the physical security ecosystem, and the devices that are emerging today are simply the next stage in an evolutionary process that is steadily expanding robots' abilities.

As they become "smarter" and more capable, robots are able to take on more roles. This reduces – but does not replace – the need for human personnel, much like how access controls and video cameras provide a way to secure multiple areas without employing a massive number of people. At the same time, robots, like other technologies, can serve as force multipliers for a leaner, more cost-effective – and more operationally effective – security team.

The presence of security robots alone serves as a deterrent to bad actors, and they are especially valuable when doing dull, dirty or dangerous tasks, such as continually patrolling and monitoring a site – studies show that humans lose focus within minutes of undertaking a monotonous assignment – or venturing into an area where there is a risk of physical danger or contamination. In addition, security robots' abilities can extend beyond security, making them multi-functional, autonomous remote services platforms.

What are some of the potential use cases for robotics?

Robots can be stationary or mobile, and they can be positioned on or traverse many types of locations and surfaces. Some mobile robots can even manipulate Americans With Disabilities Act-compliant doors and elevators. In virtually every use case, they provide, at a minimum, surveillance and a physical deterrent, and other functionalities can be added, as appropriate. A few examples are:

- ***Campuses, parking lots and other large spaces*** Fence line breach detection and response; night vision; vehicle counting; people counting; two-way communication
- ***Lobbies*** Access control/facial recognition; identify and alert to "tailgating" and other improper entrance procedures; people counting; two-way communication
- ***Gates/entrances*** License plate recognition; sensing of dangerous materials; access control; vehicle counting
- ***Offices/facilities/institutions*** Two-way communication; verification that sensitive areas are secured and no unauthorized personnel are present; sounding an alarm when an emergency is detected and broadcasting safety messages and instructions

- ***Retail establishments*** People counting; queue monitoring; analysis of traffic flows/heat mapping
- ***Warehouses*** Inventory tracking; detection of anomalies

What role do robots have in the pandemic environment, in particular?

Robots can enhance both security and public health during the current pandemic, and their inclusion in security systems helps businesses and institutions to be better prepared for future contingencies. Their functionalities and benefits include:

- Reducing the need for a human presence at a site while still ensuring situational awareness from indoors to the perimeter
- Approaching individuals to deliver messages and directives that otherwise would require face-to-face interaction
- Monitoring and providing reminders of social distancing and personal protective equipment requirements
- Measuring body temperatures of employees and visitors
- Providing a way to manage costs during economically challenging times, especially through "as-a-service" subscription contracts

How can I prepare my site and my team for a robotics deployment?

Adding robots to a security solution is an exciting upgrade that will attract a lot of interest from both within and outside an organization. Communicate early and often, manage expectations about the robot's capabilities – it will not be like on TV or in the movies – and be sure to include all relevant departments in the process:

- ***Security*** What tasks can robots do instead of humans? How can robots enhance the effectiveness of a security system?
- ***IT*** Will the Wi-Fi or cellular network coverage be strong and reliable enough to enable the use of robots in the chosen areas? Will any upgrades be necessary?
- ***Finance*** How much will labor and operational costs be reduced by making robots part of a security solution?
- ***Facilities/operations*** Will any design or traffic flow changes be necessary to enable a robot's positioning/mobility/charging? How will visitors – customers, clients, vendors, etc. – be affected?
- ***Legal*** How should vendor contracts and terms and conditions read? What might be the legal implications of the use of robotics? Can putting robots in security roles *reduce* an organization's liability risk?
- ***Human resources*** How will some job roles change? How can employees be kept informed to make acceptance more likely? How can they be included in the deployment process (e.g., robot naming contest)?

- ***Marketing*** What are the branding possibilities? Consider robot "skins," voice, messaging, etc.
- ***Communications/public relations*** How can the organization best leverage likely media attention? How can the official deployment be made into a media event?

What factors should I consider when adding robotics to a security system?

Careful planning and preparation will maximize the effectiveness of security robots. Discussions with vendors, IT departments and others should start with the following:

- ***Coverage area*** Where will the robot be stationed or, if mobile, where will it go? Can network connectivity be ensured throughout the selected area, both inside and outside?
- ***Performance*** What functions will the robot perform? The more use cases there are, the greater the demand on the network will be.
- ***Security*** How will the data collected by the robot be encrypted? Where will it be stored and for how long?
- ***Scalability*** Might the robot eventually be tasked with more duties, such as an expanded coverage area or additional data collection? Will greater security be required? Consider future use cases.
- ***Resilience*** Will the robot be able to maintain functionality and communication through system malfunctions, natural disasters, cyberattacks, etc.?
- ***Multi-frequency needs*** Can network interference be tolerated? Will there be a need to send and receive data simultaneously?
- ***Durability*** How ruggedized does the connection (e.g., radio node) need to be? Consider not just climate and environmental conditions but also – given the current situation – the ability to sanitize and disinfect the unit.
- ***Size*** What are the onboard dimensions? This will drive access point and radio node choices.
- ***Weight tolerance*** How much payload can the robot carry? Consider the types and numbers of radios, sensors and other devices with which it will be equipped and how additional weight will increase power drain.
- ***Power consumption*** Will the robot have sufficient power to fully cover its designated route and perform its prescribed functions before recharging? If not, are options available to extend its range?

Much of the material in this fact sheet was taken from the SIA webinar "How Intelligent Robotics Can Contribute to Health Compliance and Safety," featuring Alice DiSanto from Rajant, Mark McCourt from Cobalt Robotics, Steve Reinharz from Robotic Assistance Devices, and Stacy Dean Stephens from Knightscope. The full webinar can be viewed on demand on the SIA website.

The SIA Drones and Robotics Working Group brings together members of the security industry, end users, technology experts and other interested parties to promote best practices regarding the use of drones and robots in security, develop research, offer guidance on legislative and regulatory matters and enhance communication and collaboration.