SHARP INTELLOS™ A-UGV

WHITE PAPER

Rajant Network & Sharp INTELLOS A-UGV

Network design is a key consideration when selecting a robotic system. After all, the robot is traversing around a property and transmitting your proprietary information to and from the robot. Transmitted from the robot to the command center is high quality HD video and other sensor data about your property. This includes everything that the robot “sees” and “hears” through its cameras and microphone. This data should not be allowed to be accessed by an outside party due to the confidential nature of this data.

Positional data of the robot is also broadcast back to the command center, so that the operator knows where the robot is located along its path. This information is also confidential as the outside world should not know the patrol routines of the robot.

Finally, routing instructions and controls are transmitted to the robot from the command center. This information should not be disrupted or intercepted in any way.

Therefore, the following elements are paramount considerations in the network apparatus used:

1. Must be secure to prevent interception of data and hacking into the network.
2. Must have high bandwidth and speed to deliver the high-quality video necessary for the operator viewing and for the detail to use with software analytics programs.
3. Must have seamless handoffs between access points (APs) as the robot travels along the patrol path. This allows for uninterrupted video streaming.

Network Security Features

The Sharp INTELLOS A-UGV uses the Rajant Kinetic Mesh® Network, which includes a robust security platform that supports several strong cryptography options used for separately configured data and MAC address encryption via AES-256 with the above considerations in mind. With ruggedized hardware designed for Ingress Protection (IP67), it can withstand a wide range of challenging environmental conditions to which it will be exposed which improves the reliability and uptime of the system. The following important security features are employed:

1. Rajant is a proprietary system that can be configured to only allow other Rajant APs to connect. This means that a would-be hacker, using a standard 802.11 Wi-Fi device, cannot connect to the Rajant network for malicious purposes.

2. Rajant APs can only be added to the network by the system administrator, thereby only permitting known Rajant APs to connect to the robot's kinetic mesh network.
3. Multi-factor authentication is used to allow access to the administrative functions.
4. Mac address filtering is available. Each network device (e.g. PCs, smartphones) that connects to a network has a physical address (i.e. Mac address) that is unique to that device. The network administrator can configure the kinetic mesh to only permit known Rajant APs to connect based on their known Mac address. This prevents any other unauthorized device from connecting to the network. This locks out would-be hackers from accessing the network.
5. Up to 256-bit encryption is used for the data transmission across the kinetic mesh. Data encryption makes it virtually impossible to view or decipher the data that's transmitted over the network, and this 256-bit encryption is one of the highest levels of encryption that is commercially available.
6. Network packets, that are transmitted across the kinetic mesh, can be individually secured and authenticated to prevent malicious packet injection, which is the equivalent of having virus protection within the network.
7. The Sharp Command and Control System and the Sharp INTELLOS A-UGV operate on a "premise-based" network. That is, the control program and the robot all sit within the confines of the site on which it is operating, so no data is transmitted over any public internet to an offsite shared cloud server. A premised-based system provides the peace of mind that the customer's confidential data is not travelling offsite where controls are not optimal and hacking incidents could be more likely.
8. The Rajant Kinetic Mesh can be set up so it can be completely isolated from the company's network, thereby insuring there is no physical connection that can be accessed.

Kinetic Mesh Benefits

1. Operates at higher frequencies (5.8 GHz) than traditional 802.11 networks, which means that it doesn't have the "clutter" of all the other 802.11 devices to contend with.
2. APs can be moved around as the patrol routes potentially are changed. Rajant InstaMesh® technology allow the APs to automatically connect to each other and handle network packet routing using the optimal path without having to manually program the routing path.