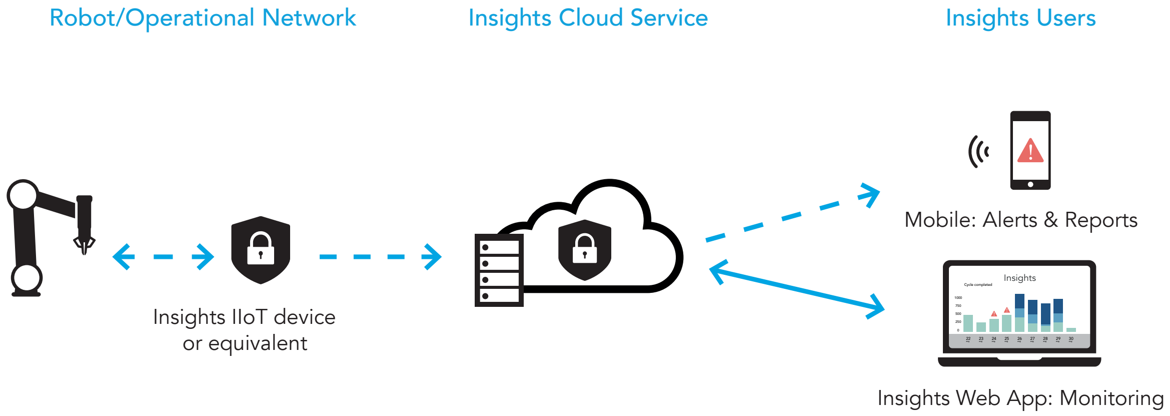
ROBOTIQ

Insights Security Sheet

Insights provides your manufacturing engineer & production managers the following features:

- KPIs to monitor production
- Data to improve product quality and process efficiency
- SMS alerts & performance reports
- Remote Access to the robot
- Complete robot backup for easy recovery

Industrial Internet of Things (IIoT) brings tremendous benefits to your company. But as every IIoT component, connecting a robot to internet without securing it might represent a risk for your data, equipment and workers.



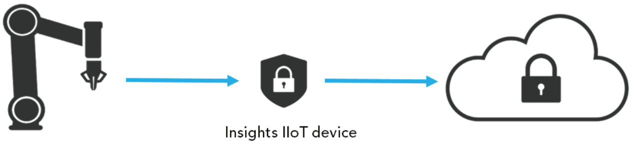
IIoT Device

As part of the Starter Kit, Robotiq provides a pre-configured device that includes a firewall. It is designed to block all ports except the ones required to ensure connection to the Insights cloud services:

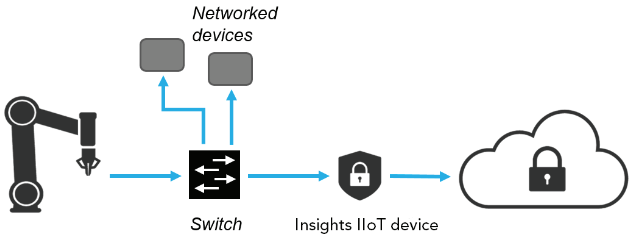
Protocol	Port	Host address	Use
MQTT	443	aws-iot-prod.robotiq.com	Publish robot data to the cloud service
HTTPS	443	www.amazon.com	Test Internet connectivity
HTTPS	443	insights-api.robotiq.com	Communicate with the Insights API
NTP	123	us.pool.ntp.org	Synchronize the robot with a time server
DNS	53	DNS server	Resolve the IP addresses
STUN & TURN	443	remote-access-turn.robotiq.com	Remote Access functionalities
HTTPS	443	box-drive-api.robotiq.com	Backup functionalities

For ease of connection, you can use our IIoT device with a SIM card. **It is strongly recommended to change the password of the IIoT Device.** In order for Insights to work with your robots when connected to your own network, you might need to open the described ports on your corporate firewall.

The IIoT device only allows outbound connection from the robot. This means only the robot can initiate a connection with the cloud service. All inbound connections to the IIoT device are blocked. A limited, temporary, encrypted and secure communication is established for the Remote Access feature. The IIoT device position in the network affects the communication between devices:



You can connect the IIoT device directly between the robot and Internet. Doing so will block any other device to communicate with the robot.



You can connect the IIoT device next to a network switch. You can also decide to secure a subnetwork that contains other devices (a PLC, CNC machine, etc.).This will allow those devices to communicate with each other while blocking all other connections with another network level that are not allowed by the IIoT device.

You may have to modify the default IIoT device configuration in order to place it on the same subnetwork. Every robot cell network topology is different. Therefore, make sure your network setup meets your security requirements. Robotiq recommends you perform a risk assessment to ensure proper security.

Data Security

All data sent from the robot to the Insights cloud service and from the cloud service to the user dashboard are encrypted. The database can only be accessed via the Insights cloud server, hosted by Amazon.

When pairing a robot to an account, a temporary pairing code is generated for a specific robot serial number. A handshake is performed between the pairing code and robot serial number in order to authenticate the robot and coodinate it with the right user account.

You can further increase the security of Insights by enabling the 2-factor authentification for your personal account. When an account has not been used for 30 days, the application will prompt you to re-enter your password.

Fore more details about Insights, consult:

- Support documentation
- Privacy policy & Licence agreement

Questions ? Contact support@robotiq.com !