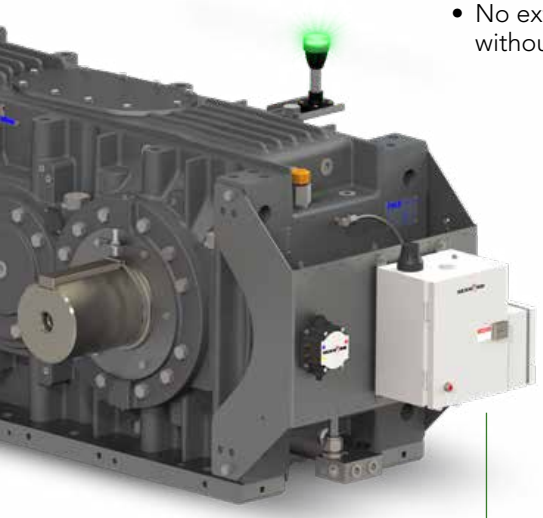
Rexnord Smart Condition Monitoring System

Security Guidelines

Keeping your network & data protected



Your data is protected in the cloud

- OAuth authentication
- No external parties allowed access without user permission

Cloud & Rexnord Connect Portal

LTE or Ethernet

Connection to Cloud (optional)

Standard Firewall configurations

- No inbound ports need to be opened
- Only industry standard MQTT ports opened

Encrypted communications

- TLS encryption
- Based on x509v3 certificates with 2 way authentication

Connection to PLC

Automation Networks

EtherNet/IP · MODBUS TCP · PROFINET

Your operations network is protected

- Data only published when requested
- No control performed by Edge Device

PLCs

SIEMENS · Allen-Bradley · Other

Questions	Answers
How much work is required from my IT team to make this work?	Typically, very little. We require only the following items to make this work: • Wired Ethernet connection with DHCP enabled • Outbound SSL (TCP 443) to be opened through your firewall to the internet - If your IT group restricts access to specific URL's, we can provide a list of the 9 URL's that need to be permitted • Outbound MQTT (TLS over TCP8883) to be opened through your firewall to the internet • Outbound FTP/S (TLS over TCP990) to be opened through your firewall to the internet • No incoming connections from the internet are required
Can a hacker remotely connect into my connected product and speed it up/slow it down or otherwise cause problems?	No, these devices are read-only, there is no capability to remotely change the speed/etc. Remote firmware updates are served from Rexnord's secured repository over TLS and are verified before execution.
What is done to prevent these devices from becoming infected and propagating a worm/ malware/etc.?	Rexnord Connected product uses a proprietary firmware that is not susceptible to common worms, viruses, etc.
How much bandwidth does this use?	Minimal bandwidth is required, as the connected product typically needs only 50bps — this is 6 times less bandwidth than the original modem that was developed in 1962
Do I need to worry about my data in the cloud being remotely accessed by my competitors or somebody else with malicious intent?	We use OAuth to secure access to your data — the same authentication used by Amazon, Google, Facebook, Microsoft and Twitter. No external parties are allowed access to your data without your explicit permission.

Physical Security Considerations

Enclosures
The Rexnord Edge Device enclosure is designed to protect the equipment from damage and unauthorized physical access. There are no user serviceable parts within the enclosure and it should remain sealed throughout the life of the equipment.

Locations
The Rexnord Edge Device should be treated like other networking equipment with regards to physical access control. It is expected that only authorized personnel have physical access to the Rexnord Edge Device.

Cabling
Physical network cables used to connect the Rexnord Edge Device to your organization's operational Technology network should be protected to prevent tapping, deliberate damage and related attacks and accidents. Protective methods include conduit, raceways, ducting and the like.

Rexnord Edge Device Operating System and Applications

Operating System and Rexnord Edge Software
Do not attempt to access, modify or manipulate the Rexnord Edge Device operating system or any software running on the Rexnord Edge Device besides the PLC networking configuration as specified by those instructions. Such actions may cause the Devices to fail or operate improperly. Deliberate attempts to modify or manipulate the Rexnord Edge Device may result in voiding service agreements between your organization and Rexnord. There is no provision to connect a keyboard or monitor directly to the Rexnord Edge Device.

PLC Interface
The Rexnord Edge Device will output current sensor readings and any warnings through a data packet accessible via EtherNet/IP, Modbus TCP or ProfiNet. This data is only provided when requested by the PLC. This port does not allow access to the Rexnord Edge Device applications or operating system and will not send any data to the PLC unless requested. The architecture prevents a path or capability for the cloud or Rexnord Edge to disrupt or change the PLC control.

Networking/Cloud Considerations

Cloud Network Access (optional)
The Rexnord Connect web portal utilizes OAuth industry standard authentication and authorization technologies. The only data stored in the cloud is time-based sensor data, alerts and warnings. The data center is SOC2 Compliant and FedRAMP Certified.

Portal Access
Any new users wishing access to the connected asset will register on Rexnord.com, verify their E-mail address and be verified by the site administrator before access to any asset monitoring data is allowed.

Operational Technology and Information Technology Networks
Your organization should configure its routers and firewalls to allow the Rexnord Edge Device traffic to be routed to the internet so it can communicate with the cloud service. No inbound ports need to be opened. The Rexnord Edge Device uses port 443 and standard MQTT ports. The Rexnord Edge Device uses TLS encryption based on x509v3 certificates and 2-way asymmetric authentication. It is best practice to isolate any 3rd party device from your corporate network.

The following ports, protocols and destination URLs must be allowed:

HTTPS Port 443:

h2s://nodev2.iotium.io
https://checkip.amazonaws.com
https://update.iotium.io
https://download.iotium.io
https://journal.iotium.io
https://upload.iotium.io
https://index.docker.io/v1/
https://rexnorddockerregistry.azuercr.io

FTP/S over TLS Port 990

ftp:// ftp.box.com

MQTT over TLS Port 8883

ssl://*.messaging.internetofthings.ibmcloud.com

Risk Assessment

Rexnord follows the industry standard Center for Internet Security Risk Assessment Method (CIS RAM) for assessing cyber security risks across all components of the Rexnord IIoT ecosystem. CIS RAM is aligned with ISO 27005 and NIST SP 800-30 to insure reasonable and appropriate implementation of security controls to satisfy a Duty of Care Risk Analysis for compliance with regulatory (NIST 800-171 standard and the Cyber Security Framework) as well as legal requirements. ***The scope includes the Smart Condition Monitoring System platform, cloud systems, network server, workstations/desktop support and security teams. Risk assessments are not shared externally.***

A third party is used to scan internal assets and identified vulnerabilities are reviewed and remediated based on priority. External penetration tests are conducted at least annually and identified vulnerabilities are reviewed and remediated based on priority.