Bosch Rexroth IoT Gateway Security Guidelines

Document Version 3.1.0 (June 2019)

Table of content

1 Introduction

1.1 Purpose of this guidline

The Rexroth IoT Gateway Software is a Java based software product, which can be executed on different hardware and operation system environment.
This document focusses on the Rexroth IoT Gateway software itself.

1.2 Rexroth Security Manual Electric Drives and Controls

The content of this document is based on and extends the information of the Rexroth Security Manual Electric Drives and Controls (R911342562).
Please refer to this Security Manual Electric Drive and Control for further informations about
• Special information on the secure operation of Bosch Rexroth IT systems and devices
• General information about the “IT security” topic in manufacturing systems

Note
System and machine operation requires the implementation of an integral, state-of-the-art IT security concept.
Bosch Rexroth products are part of this integral concept. The products have to be taken into consideration in an integral IT security

concept with regard to their properties.

1.3 Intended and approved use cases

The IoT Gateway software supports the following use cases:

a) Installation of IoT Gateway on devices within a shopfloor network

Connect machines and devices in an isolated shopfloor automation network to other IT system within the same network

- IoT Gateway can be used without addtional security restrictions
- Existing shopfloor network infrastructure has to provide appropppritate isolation towards other networks like Enterprise or cloud networks

Connect machines and devices within an isolated shopfloor automation network to other IT system on Enterprise IT or Cloud

- IoT Gateway may not be used without additional security measures
- Separate VPN and/or Firewall devices have to be installed between IoT Gateway and Enterprise IT / Cloud network

b) Installation of IoT Gateway on devices in an Enterprise IT (server)

Connect machines and devices in a shopfloor automation network to other IT system on Enterprise IT or Cloud

- IoT Gateway may not be used without additional security measures
- A surrounding security concept has to be installed e.g by using external VPN and/or Firewall Functionality

c) Installation of IoT Gateway on devices in a Cloud infrastructure

This deployment scenario is not supported

2 Security relevant product description

The following sections describe the security-relevant aspects of the Rexroth IoT Gateway Software.

Important Note: Security properties of Bosch Rexroth products

Bosch Rexroth products are - unless otherwise documented - designed for usage in local, physical and logical protected networks with limited access to authorized persons. Bosch Rexroth products are not classified according to IEC 62443.4.2.

2.1 Java Virtual Machine

To reduce the risk of security impacts, it is important to keep Java updated to the latest version available.
Oracle provides Security Alerts with the option to subscribe to be notified by email for critical updates to Java: Instructions for subscribing to email notifications of Critical Patch Update Advisories and Security Alerts

For information about update Java on Windows operation systems, please refer to the Java update recommendations

General information about Java and security can be found in documents from BSI:
• Overview about Java and Security: Sicherheit von Java
• Recommendations for a secure Java configuration: Konfiguration der Sicherheitseinstellungen von Java, Sicherheit von Java - Empfehlungen zur sicheren Nutzung

2.2 OSGi Framework

The IoT Gateway is built upon the OSGi (https://www.osgi.org/) architecture.
According to the OSGi basic mechanisms, users can extend the IoT Gateway functions during runtime by installing additional features.
These features have to be provided as Java bundles.
Only authorized users should have access to the IoT Gateway Software for loading additional bundles to avoid that malicious bundles are loaded.

2.3 Communication Interfaces

HTTPS Web Interface
IoT Gateway Software uses HTTPS to access the web based user interface. HTTP is not supported.

REST API
Software features of the IoT Gateway are available via a REST API.
This REST API is designed for script based configuration of the IoT Gateway and supports basic autentication and authorisation mechanisms.

Device and Processing protocols
Depending on the actual use cases and scenarios, the IoT Gateway uses TCP/IP and HTTP / HTTPS to exchange information with data sources (Devices) and cloud services (Processings).
Usage of these protocols depends on customer specific IoT Gateway configuration. Please refer to the IoT Gateway Online Help for further information.

2.4 Network Ports

The Rexroth IoT Gateway uses the following ports:

Port	Description
8888	Web Server (landing page): https://{device_address}:8888/home/index.html
9999	OPC UA Server
(dynamic)	Depending on device and processing configuration, ports are allocated dynamically. Ths dynamic port allocation is standard behaviour on Windows and Linux operating systems. Please refer to the Windows or Linux documentation for an overview about the typical ranges for dynamic port assignment.

2.5 Web Console

Self signed Certificate

The certificate of the IoT Gateway is currently self-signed and therefore your web browser displays a security warning upon the initial connection and navigation to a website in the web root. Please verify and add the untrusted certificate to your exceptions.
Login Authentication

On first access of the built-in Web Console, please login with the Default user:
user: admin
password: admin

After first login, you must change the password. It is stronlgy recommended to provide a strong password.

Important note:
Your provided credentials (username, password) must differ from credentials of the default user.
If you forgot your credentials, please contact any IoT Gateway service personal to reset.

WebServer (Jetty) security recommendation

The IoT Gateway contains the built-in WebServer component Jetty. Please perform a regular check of the shipped version against known vulnerabilities:
http://www.eclipse.org/jetty/documentation/9.4.x/security-reports.html

2.6 OPC UA Server communication

The IoT Gateway comes with an built-in OPC UA Server to be connected by any external OPC UA Client. The OPC UA Server does only expose secure server endpoints by default. Despite of that, it’ s possible to enable unsecure endpoints for testing- or commissioning purposes.

Disable this feature on production mode and use only secure OPC UA Communication.
The Iot Gateway online help for OPC UA Server application provides further information

2.7 Devices and Processings

The connections to Devices (sensors and connected data servers) and Processings (cloud services) are unsecure by default to enable easy and fault tolerant initial comissioning.
For Devices and Processing which support secure communucations, it is strongly recommended to use a secure configuration

Secure Communication

Secure communication is supported from the following Devices and Processings

- Devices: OPC-UA, MQTT
- Processings: Amazon Cloud (AWS IoT Cloud), Microsoft Azure, MQTT, Oracle IoT Cloud Service, REST, TCP/IP

Connection to OPC UA Servers using the OPC UA Device

Message security
Specify one of the available SecurityModes as connection parameter of the connect method other than None

If specified, IoT Gateway manages the created certificate for you.

User authentication
If the connected OPC UA Server supports user authentication, specify the credentials (username, password) in the device configuration

3 Further security recommendations

3.1 Overall security concept

All system topologies with IT technologies should be operated with a general security concept which outlines the general security rules and their adaption to specific devices, with respect to their properties.
Focus of the overall security concept is information security: Protection of confidentiality, integrity and availability of digital information. Regarding product security this means the protection of digital information against potential malicious attacks.
Please refer to IEC62443-3-3 for holistic system requirements.

Note: Without further security measures like additional VPN and/or firewall mechanisms, the IoT Gateway may only be used in local, isolated networks without external routing mechanisms. An appropriate network topology and its borders has to be provided and documented when an IoT Gateway is integrated into a network infrastructure.

3.2 General operating system related recommendations

Operating system updates and hardening
It is stronlgy recommended to keep operation systems up to date with the latest security patches. Moreover, whenever possible, hardened versions of operating systems should be used.

User identification and authorization
All users who have access to devices with an IoT Gateway software installed, should be identified and authorized. Modern operating systems typically support a mature user management which provide appropriate authentication and authorization mechanisms.
Those mechanisms should be implemented both for local and remote device access.
Existing default login credentials should be changed.
For additional risk reduction, users should be assigned to the lowest access level that they need for their role.

Device interfaces
Hardware and software interfaces which are note explicitly required for regular operation, should be dsabled or blocked. This should be considered for hardware interfaces (e.g. like WiFi and Blutooth interfaces) and also for software interfaces (e.g. like ports).

3.3 IoT Gateway on Linux devices

On Linux devices, typically SSH is used for remote access. To avoid security issues, the default SSH user’ s password must be changed after the first log in.
This recommendation should be applied both for Bosch Rexroth devices and third party devices

IoT Gateway Software on Bosch Rexroth PR21 hardware

It is strongly recommended to change the initial password on a PR21 hardware to ensure proper access control:

- Connect via SSH, e.g. using Putty: https://putty.org/, or directly via the HDMI port of the device
- Log in (user: boschrexroth, initial password: boschrexroth)
- Note: No visual output is available when entering the password
- After succesful login, you are now in the home directory of user “boschrexroth”

Please change the default password after first login (Caution: after a change the initial password can not longer be used)

- Enter the following command:

```
passwd
```

- You are now prompted to enter the initial password (“boschrexroth”)

- Note: The Linux console does not show any output while entering the password
- After entering the initial password you are prompted for a new password
- After entering and repeating the new password the setting is changed permanently.

3.4 IoT Gateway on Windows devices

For Windows devices, it is strongly recommended to harden the operating system as much as possible. Especially all security relevant updates from Microsoft should be installed.

Additionally, Windows services which are are not required explicitly, should be turned off.

3.5 Third Party Components (Open Source Software)

Even though Bosch Rexroth strives to provide the most secure versions of used Open Source Software available, we recommend to check the shipped versions against known vulnerabilities when using the IoT Gateway

A list of used third party components can be found in document Open Source Software in the IoT Gateway help.