

RE 95406 / 2023-10-06

# **BODAS Connect Device Connectivity | RE95406**

# Contents

<b>1</b>	<b>BODAS Connect</b>	<b>5</b>
1.1	Device Connectivity	6
1.2	All-in-one Connectivity	6
<b>2</b>	<b>Variants</b>	<b>8</b>
<b>3</b>	<b>Features</b>	<b>9</b>
3.1	Device Software for Rexroth Connectivity Unit	9
3.1.1	Complimentary Software Development Kit	10
3.2	Device Management	10
3.2.1	Device Portal	10
3.2.2	Device Portal Artifact Repository	10
3.2.3	Private Artifact Repository	10
3.2.4	Device Overview	10
3.2.5	Device Information View & Monitoring	11
3.2.6	Device Configuration	12
3.2.7	Software List View	12
3.2.8	Device Portal Activity overview	13
3.3	BODAS Connect OTA Services	14
3.3.1	Device Software, ECU Firmware and Parameter Over the Air	14
3.3.2	Software update Over-the-Air (SOTA) for RCU and SOTA Campaign Management	15
3.4	APIs	15
3.5	Integrated mobile radio	16
<b>4</b>	<b>Privacy, Security &amp; Safety</b>	<b>17</b>
4.1	Security & Safety instructions	17
4.1.1	CAN	17
4.1.2	Physical Interfaces	17
4.1.3	Protective Measures	17
	Strong Passwords	17
	Hacker Attacks	18
	Social Engineering	18
4.2	Cybersecurity	18
4.2.1	BOSCH Security Engineering Process	18
4.2.2	Certificate management and Certificate-based device authentication	18
4.2.3	Embedded firewalls	19
4.3	Safety instructions	19
4.3.1	General instructions	19
4.3.2	Intended use	20
4.3.3	Improper use	20
4.3.4	Use in safety-related functions	20
<b>5</b>	<b>OTA Services - OEM Responsibilities</b>	<b>21</b>

5.1	Overview Workflow	21
5.1.1	Terminology	21
5.2	OEM Responsibilities with regard to functional safety	21
5.2.1	Before using OTA services	22
5.2.2	While using OTA services	22
5.2.3	After using OTA services	22
<b>6</b>	<b>Project Planning Notes</b>	<b>23</b>
6.1	Software & Bus configuration for allowing IoT Services	23



# 1 BODAS Connect

**Bosch Rexroth Digital Application Solutions – BODAS** stands for the entire portfolio of IoT solutions, software and electronic hardware for the off-highway market.

BODAS Connect is Bosch Rexroth's integrated telematics solution that **enables** machine **OEMs**

- to **gain** internal R&D and customer support **efficiency**,
- to establish external **data driven business** models

both based on a **industry-proven infrastructure**, which OEMs can fully customize to leverage their **core competencies**.

The respective BODAS Connect packages are described in:

- Rexroth Connectivity Unit (RCU): RE95430
- Device Connectivity (Device Management for RCU): RE95406
- All-In-One Connectivity (Data Management and features for off-highway applications): RE95407

BODAS Connect is a modular end-to-end connectivity solution to transfer data from and to the mobile machine. Unbundled and freely selectable services consisting of device management, data management and ready to use apps for fleet management, vehicle health, remote R&D services and vehicle operation workflows.



It is built on the Linux-based Bosch Rexroth Connectivity Unit (RCU), which is remotely managed and administrated via the Bosch Device Management Portal. Data storage, processing and analysis are performed via the data management in Bosch IoT Insights.

Depending on customer requirements, BODAS Connect is flexibly customizable and offers both specific device management and data management functions.

The following figure shows an overview and the classification of the Bosch Rexroth IoT solution with the two products "Device Connectivity" for device management and "All-in-One Connectivity", which adds data management on top.

# BODASConnect<sup>®</sup>

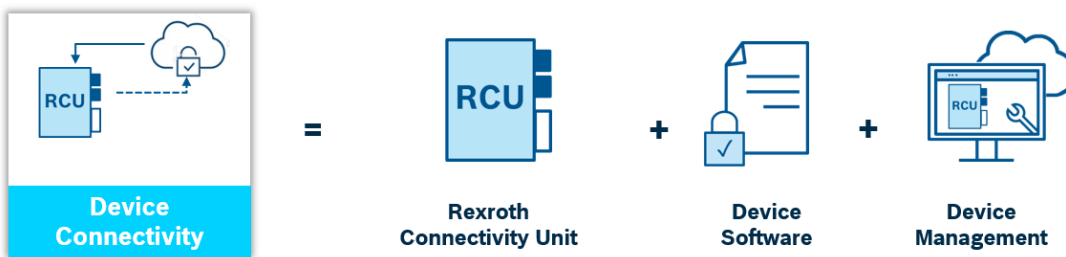
## The Comprehensive IoT Solution for Off-Highway Applications



### 1.1 Device Connectivity

The digital transformation of the off highway market is already well underway and has given rise to new challenges for mobile machines. In our continuous effort to support clients as a strong partner and solutions provider, Bosch Rexroth combines in-depth applications expertise and the BODAS software and hardware portfolio to create an integrated Internet of Things (IoT) solution BODAS Connect.

As an integral part of BODAS Connect, Device Connectivity uses the Rexroth Connectivity Unit (RCU) to enable numerous options to wirelessly access the control networks of off highway vehicles. Interactions include flashing, diagnosis and parameterization of Rexroth Controllers (RC). For customers with pre-existing data management, BODAS Connect Device Connectivity offers an ideal package for connecting their mobile machines.



### 1.2 All-in-one Connectivity

BODAS Connect All-in-one Connectivity extends the functions of BODAS Connect Device Connectivity with industry-proven data management services. Based on the BOSCH IoT Insights Platform with over 10 million connected vehicles, this fully integrated IoT solution for mobile machinery handles, processes and stores data obtained from Rexroth Connectivity Units (RCU). It provides an ever-growing variety of off-the-shelf fleet management and condition monitoring services. Our REST-API interfaces as well as our customizable front end, Bosch IoT Insights, offer even more data analysis options.



## 2 Variants

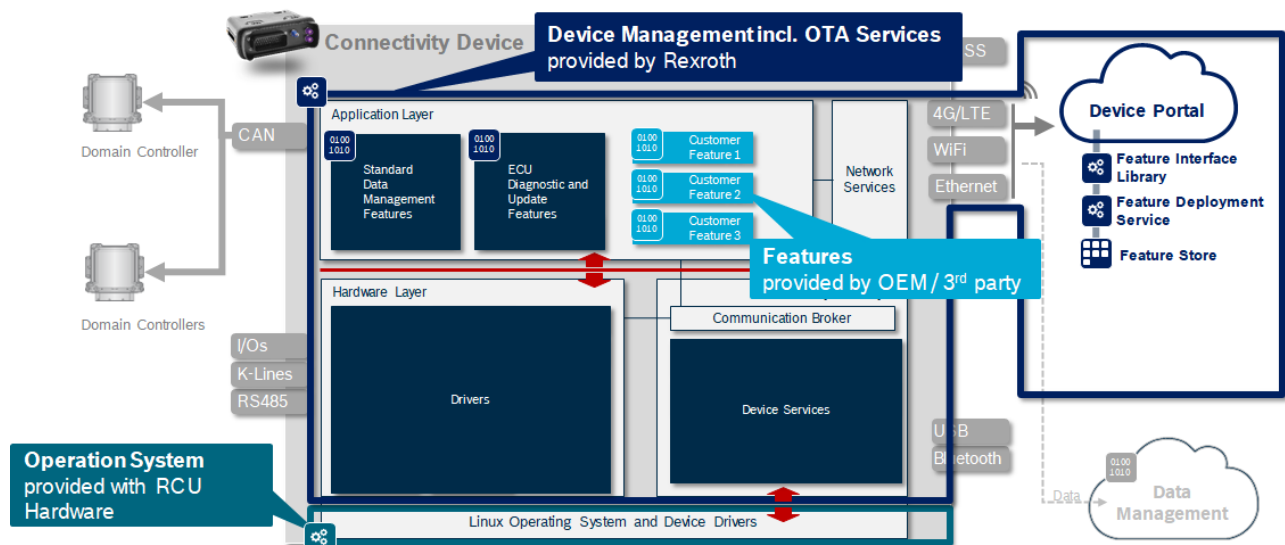
Category	Service	Material Number	Description
Device Management	Essential	R917014562	Default for not yet activated RCUs (Claimed RCUs; valid until RCU goes online for the first time)
	Compact	R917014006	Default for active RCUs (incl. Software update Over-the-Air (SOTA) for RCU and SOTA Campaign Management)
	Extended	R917014007	Choose this, if you need Over-the-Air (OTA) services for connected devices (incl. RCU Software update Over-the-Air (SOTA) for RCU and SOTA Campaign Management)
Mobile Radio provided by Vodafone (optional)	5 MB	R917014014	Monthly data transfer for soldered eSIM in RCU
	10 MB	R917014015	
	50 MB	R917014016	
	100 MB	R917014017	
	150 MB	R917014018	
	1 GB	R917014019	



## 3 Features

The Bosch Rexroth Device Connectivity combines the Bosch Rexroth Device Software with the BODAS Connect Device Management. It is a Software as a Service (SaaS) solution on a monthly subscription basis for managing electronic devices (ECUs, CCUs, Gateways, Sensors, ...). Moreover the Bosch Rexroth Device Connectivity is used for managing the connection of off-highway machines to cloud services such as the data management service also offered by Bosch Rexroth (RE95407). This facilitates various use cases around operations monitoring for both end user and OEMs or fleet owners.

In order to use the Bosch Rexroth Device Connectivity for managing devices in an off-highway machine, a Linux-based Rexroth Connectivity Unit (RCU), with an application processor, e.g. the Bosch Rexroth Connectivity Unit (RE95430), shall be available in the off-highway machine. The main RCU will be directly connected to the BODAS Connect Device Portal and other devices will be connected to the BODAS Connect Device Portal through it.



### 3.1 Device Software for Rexroth Connectivity Unit

The Bosch Rexroth Device Software is a software running on the RCU of an off-highway machine. Its main functionalities are:

- **Device Administration:** It provides easy to use configuration and monitoring functionalities for the RCU.
- **Error Management:** It centrally monitors and reports all applications, system and hardware errors.
- **Hardware Abstraction:** It encapsulates complex hardware drivers and provides easy to use interfaces for reading data from or writing data to hardware interfaces, as well as configuring those hardware interfaces.
- **Communication Management:** It provides and manages a secure (certificate-based authentication), central, asynchronous and reliable communication broker, based on the MQTT protocol. This communication broker can be used by all applications for communicating with each other without the need of using heterogeneous, fault-prone and complex programming libraries.
- **Security Management:** It manages a secure communication with the Device Portal. The communication is based on TLS and the authentication is certificate-based. It regularly checks the validity of certificates and alerts the user in case a certificate needs to be updated.

- **Application Management:** It provides an easy to use interface for managing all applications (installation, configuration, update and removal). All applications are executed in a confined environment (SNAP container) with restricted rights. It also provides an easy to use interface for managing the rights assigned to each individual application.

### 3.1.1 Complimentary Software Development Kit

Developers can develop their application in any supported programming language with their preferred IDE (Integrated Development Environment). For packaging the developed application in a SNAP, developers can use the free SNAP tool-chain provided by Canonical.

The Bosch Rexroth Device Connectivity features an OpenAPI compliant description of APIs that the developer can use for communicating with other applications, reporting error or receiving configuration parameters.

Example code and examples on how to set-up the packaging tool-chain are available in the Bosch Rexroth Github (<https://github.com/BoschRexroth>).

## 3.2 Device Management

The BODAS Connect Device Management is an integrated part of the BODAS Connect Device Connectivity. It is the digital manager for IoT Devices. These may be routers/gateways, connectivity control units (e.g. Rexroth Connectivity Unit), machine controllers or even sensors, for instance. But even if the advantages of the Internet of Things, such as increased efficiency and streamlined processes, are obvious, managing a large number of IoT devices can quickly become confusing, complex and thus time-consuming and expensive. Each software change requires that associates spend time gathering information from each device in question. In addition, there is increased vulnerability to malware, such as viruses and trojans, and risk of software becoming outdated. The Device Management is the solution to these problems.

### 3.2.1 Device Portal

The Device Portal is the graphical user interface to manage the Bosch Rexroth Connectivity Units (RCU) and the connected Rexroth Controllers (RC).

### 3.2.2 Device Portal Artifact Repository

The Device Portal Artifact Repository provides APIs which let you manage your software (for example to upload new versions) as well as define which devices can access the repository (by allowing or blocking manufacturer certificates).

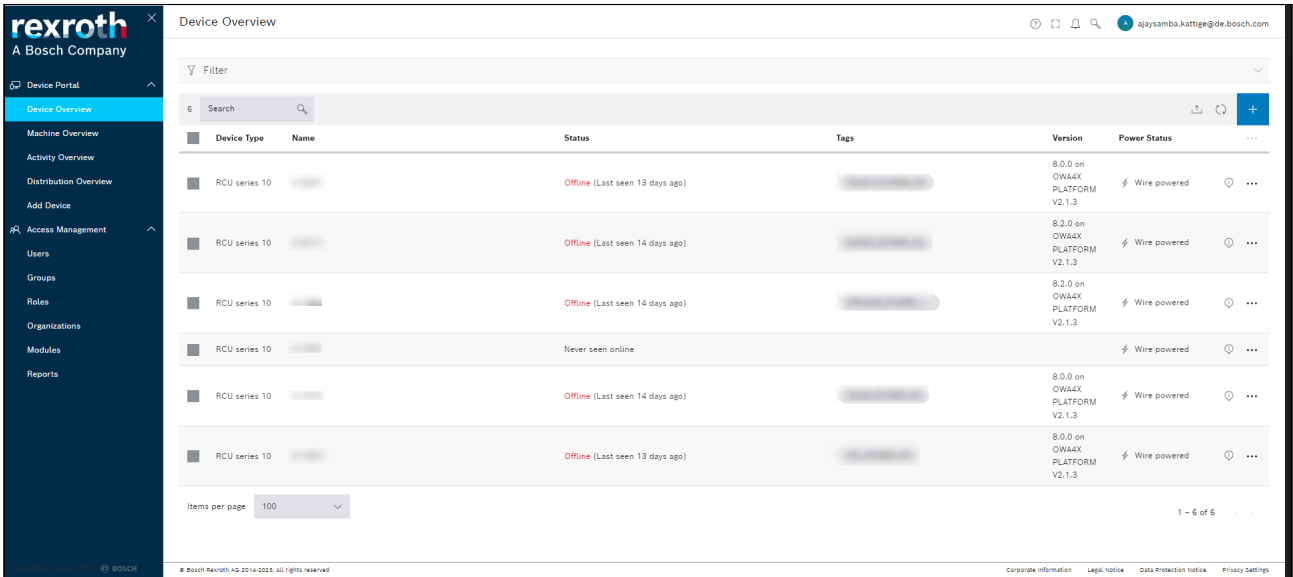
The backbone of the Device Portal Artifact Repository is based on the MS Azure infrastructure. MS Azure is not available in all countries today. Therefore, it may not be possible for all customers to host their own Artifact Repository. For this reason, the availability of MS Azure should be checked on a case-by-case basis.

### 3.2.3 Private Artifact Repository

A user-specific repository can be connected to the Device Portal. The connection enables the rollout and management of external software components. In addition, device manufacturers can make their repositories available to customers in this way.

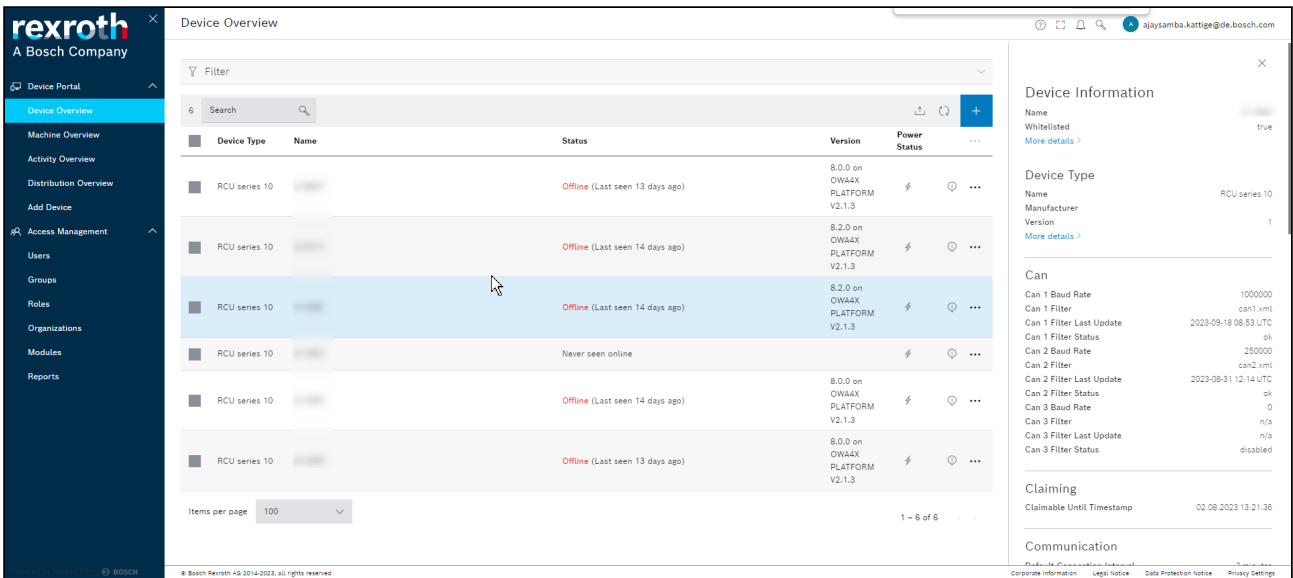
### 3.2.4 Device Overview

The Device Overview displays all devices with some information. The user can also use the search/filter function to display only a small set of devices that he wants to monitor.



### 3.2.5 Device Information View & Monitoring

A click on the icon ⓘ of a device will open a side panel with all the information available for the device.



In order to provide meaningful insights to the user, the Bosch Rexroth Device Software collects status information from the devices. This information is grouped in following categories:

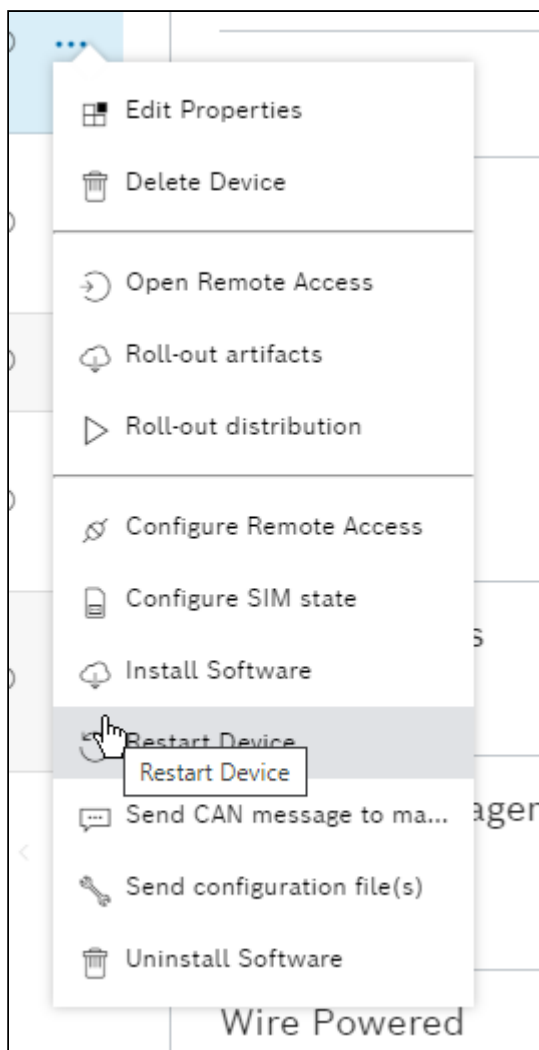
- **Communication:** Connection status of the device.
- **Device:** Additional information about the device itself.
- **Device Administration:** Data which is intended to be used for administrative purposes (e.g. operating hours, uptime, etc.).
- **CAN configuration status:** status of connected CAN busses & their configured baudrate
- **Diagnosis:** Data which is intended to be used for error analysis.
- **Geo location:** Geo location of the device.
- **Cellular:** Information about the SIM-card used on the device.
- **Network:** Data of the devices TCP/IP network interface.

The device does not need to provide information to all categories. Customer specific categories can be added on demand.

### 3.2.6 Device Configuration

All devices that are managed with the Bosch Rexroth Device Connectivity can be configured and/or administrated through the user friendly interface of the BODAS Connect Device Portal. Following commands are available for configuration purposes (commands are subject to continuous modifications):

- Edit Properties of one or more devices; e.g. Tags, Name, Description
- Delete Device from the Device Management tenant
- Open Remote Access to start OTA services for connected devices (e.g. ECUs)
- Roll-out artifacts for updating and/ or installing RCU software
- Rollout Distribution
- Configure Remote Access to request or de-activate a Remote Access
- Configure SIM state for deactivating or re-activating RCU eSIM
- Install Software triggers the installation of a new RCU software (expert form)
- Restart Device triggers a RCU restart
- Send CAN message to machine will be released later
- Send configuration file(s) to the RCU
- Uninstall Software from the RCU



### 3.2.7 Software List View

A software list view is provided by the BODAS Connect Device Portal. This view lists all software packages available for a RCU.

Following information are displayed for each software package:

- name of the software package
- description, including the latest stable version available
- installed version












As shown in the following picture, the user can:

- install an available, but not yet installed software package
- update an already installed software package to the newest version
- remove an already installed software package

Device Overview

Device: RCU Sample 1 - Online

Software

Name ↑	Description	Update Channel	Installed Version	
BODAS Service	BODAS Service Application for remote diagnosis, Version 3.6.8	latest/local	3.6.8	
Bosch Uploader	Application for uploading data to Bosch IoT Insight, Version 0.1.7	latest/local	0.1.7	
Customer App 1	Customer Application, version 0.7.4	latest/local		
DBC Decoder	Application for decoding CAN frames based on a DBC File, Version 1.2.4.	latest/local	1.2.0	 
Error Service	Errors management service, Version 1.0.1	latest/local	1.0.1	
Geolocation Service	Application providing Geolocation Services, Version 3.0.0	latest/local	2.3.0	 
ISOBUS	ISOBUS Stack, Version 2.3.5	latest/local	2.3.5	
Operating System	Basic Operating System and drivers, Version 4.14.67	latest/local	4.14.67	
UDS	UDS Stack, Version 0.3.7	latest/local	0.3.7	

### 3.2.8 Device Portal Activity overview

In order to check all device activities that have been performed during the past month, the user can consult the activity overview.

Activity Overview

Command Batches Commands

Status	Roll-out ID	ID	Command Name	Description	Progress	Created	Last Change	
Successful		75039	UPDATE_TUNNEL		0 / 1 / 0	22.09. 13:36	22.09. 13:38	...
Successful		74936	UPDATE_TUNNEL		0 / 1 / 0	21.09. 13:45	21.09. 13:46	...
Successful		74770	UPDATE_TUNNEL		0 / 1 / 0	20.09. 11:49	20.09. 11:50	...
Successful		74649	UPDATE_TUNNEL		0 / 1 / 0	19.09. 14:53	19.09. 14:54	...
Successful		74490	UPDATE_TUNNEL		0 / 1 / 0	18.09. 11:54	18.09. 11:56	...
Successful		74476	RESTART		0 / 1 / 0	18.09. 10:54	18.09. 10:59	...
Successful		74471	UPDATE_CONFIGURATION		0 / 1 / 0	18.09. 10:34	18.09. 10:53	...
Failed		74434	INSTALL_SOFTWARE	Roll-out 'update-service 4.1.3' from channel 'latest/stable'.	0 / 0 / 1	15.09. 18:01	18.09. 08:26	...
Successful		74433	INSTALL_SOFTWARE	Roll-out 'pollux-gps-gsm 2.0.0' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	18.09. 08:26	...
Successful		74432	INSTALL_SOFTWARE	Roll-out 'remotereagent 0.5.0' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:30	...
Successful		74431	INSTALL_SOFTWARE	Roll-out 'power-control 0.5.0' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:29	...
Successful		74430	INSTALL_SOFTWARE	Roll-out 'can 1.8.2' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:28	...
Failed		74429	INSTALL_SOFTWARE	Roll-out 'network 0.15.0' from channel 'latest/stable'.	0 / 0 / 1	15.09. 18:01	15.09. 18:26	...
Successful		74428	INSTALL_SOFTWARE	Roll-out 'gps 1.5.3' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:20	...
Successful		74427	INSTALL_SOFTWARE	Roll-out 'itk-uploader 0.9.3' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:17	...
Successful		74426	INSTALL_SOFTWARE	Roll-out 'uds-br30 1.0.0' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:14	...
Successful		74425	INSTALL_SOFTWARE	Roll-out 'rcu-base 9.0.2' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:13	...
Successful		74424	INSTALL_SOFTWARE	Roll-out 'config-service 1.2.1' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:12	...
Successful		74423	INSTALL_SOFTWARE	Roll-out 'status-service 2.1.0' from channel 'latest/stable'.	0 / 1 / 0	15.09. 18:01	15.09. 18:10	...

## 3.3 BODAS Connect OTA Services

The Bosch Rexroth Device Connectivity features various over the air functionalities. Those functionalities allow the distribution of software updates, firmware updates and parameter updates over the mobile or wireless network without the need of a physical access to a machine. Moreover the Bosch Rexroth Device Connectivity includes a full feature remote service tool (Remote BODAS Service) that allows to perform remote diagnostic functionalities to the control connectivity unit or connected electronic control units (ECU). Those diagnostic functionalities include reading fault messages, visualizing process values, updating individual parameters or parameter sets and updating software and firmware.

### In a nutshell

#### Over-the-Air (OTA) services for connected devices

BODAS Connect Device Connectivity offers the following Over-the-Air (OTA) services for connected devices:

- FOTA (Firmware Over-The-Air), i.e. software update of connected Rexroth BODAS controllers RC
  - incl. FOTA Campaign Management: for admins to perform OTA updates & send commands to multiple devices simultaneously, available in the Device Portal under **Rollout Distributions**
- POTA (Parameter Over-The-Air), i.e. changing parameters within the software of connected Rexroth BODAS controllers RC
- BODAS-Service Remote Diagnostic or DOTA (Diagnosis Over-The-Air)

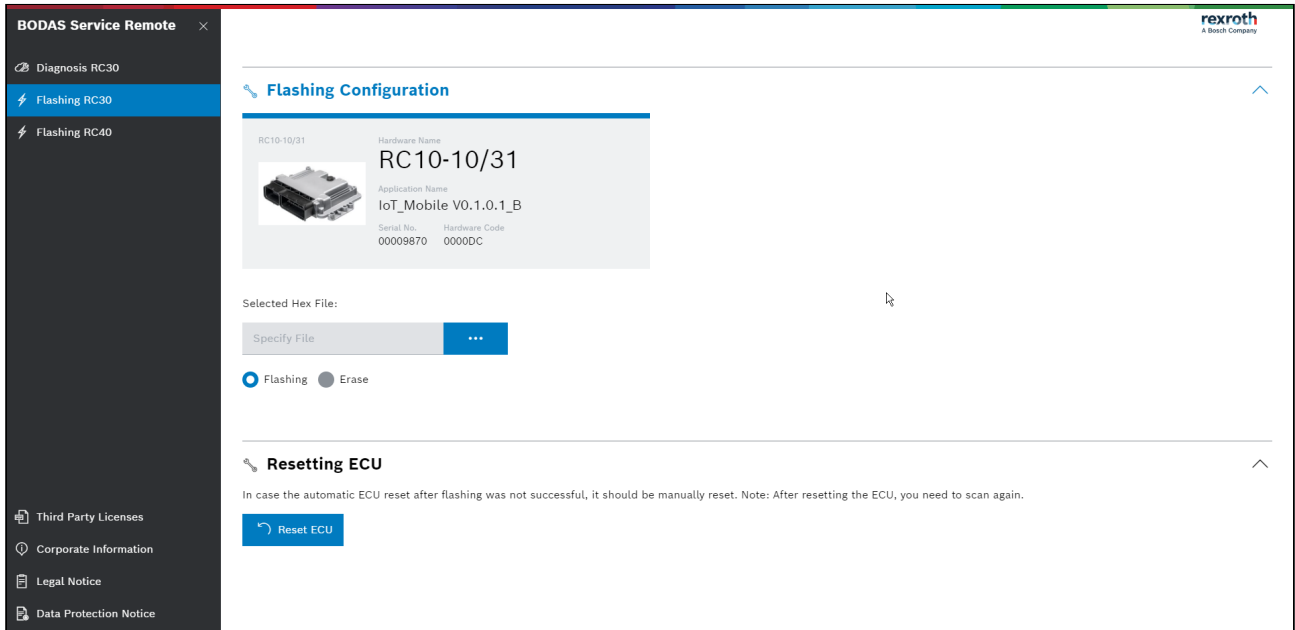
For RC series 30 FOTA, POTA and DOTA are available. For RC series 40 FOTA and POTA (file-transfer version) are also available.

BODAS Connect Universal Flasher: allows flashing software to any device (Rexroth or 3rd party ECU) in the vehicle CAN network compliant to the UDS standard.

### 3.3.1 Device Software, ECU Firmware and Parameter Over the Air

Following over the air commands are directly available from the BODAS Connect Device Portal:

- **Install Software:** This command triggers the installation of a new software in the connectivity unit.
- **Update Firmware:** This command triggers the update of the firmware on the selected ECU connected to the main connectivity unit.
- **Update Parameter Set:** This command triggers the update of the parameter set on the selected device.
- **Update Software:** This command triggers the update of the software on the selected device.
- **Uninstall Software:** This command triggers the removal of the software on the selected connectivity unit.



### 3.3.2 Software update Over-the-Air (SOTA) for RCU and SOTA Campaign Management

The solution offers Software update Over-the-Air (SOTA) for RCUs. The respective commands (e.g. Roll-out artifacts) are described in the section Device Configuration. With SOTA new RCU application software or RCU configuration can be installed or updated on a Rexroth Connectivity Unit. The update will be rolled-out by the Device Management as soon as the RCU is online.

SOTA Campaign Management means software deployment for entire fleets. New software versions are allocated to the respective machines and software is downloaded Over-the-Air onto the RCU as soon as it is online.

Device-specific over the air commands for a single device can be executed via the menu which appears when you click on the actions button of a device in the Device Overview. In order to trigger an over the air service for multiple devices (**Campaign**) you need to first select the devices by using the checkboxes and afterwards click on the actions button located in the header row. Triggering over the air services for multiple devices at once is only supported for devices of the same device type.

Device Type	Name	Connection	Firmware Version	Power Status	
<input checked="" type="checkbox"/>	Rexroth Connectivity Unit	RCU Sample 1	Online since a few seconds	Linux 4.14.67-1.0.8+	ⓘ ? No power st... ⓘ
<input checked="" type="checkbox"/>	Rexroth Connectivity Unit	RCU Sample 2	Offline since 3 months	1.0.0	ⓘ ? No power st... ⓘ
<input type="checkbox"/>	Rexroth Controller	RCU Sample 1 - RC 1	Online since a few seconds	EDA 2.0	ⓘ ? No power st... ⓘ
<input type="checkbox"/>	Rexroth Controller	RCU Sample 1 - RC 2	Online since a few seconds	DRCA 4.2	ⓘ ? No power st... ⓘ

OTA Commands for single device and for campaign

## 3.4 APIs

### Solution BFF

The Solution API allows solutions or applications to integrate with the Device Portal.

Solution API endpoint: <https://idm-solution.s-apps.de1.bosch-iot-cloud.com>

## Device BFF

The Device API allows devices to interact with the Device Portal.

Device API endpoint, Basic Auth: <https://idm-device.s-apps.de1.bosch-iot-cloud.com>

## 3.5 Integrated mobile radio

Rexroth offers mobile radio as a managed service, fully integrated in BODAS Connect Device Management. Together with the RCU, Rexroth Device Software and Device Management this integrated solution has the following advantages:

- Managed Service means Rexroth is also handling the mobile communications provided by Vodafone (= one-stop-shopping)
- Integrated SIM handling in Rexroth's Device Portal as single sign-on (SSO)
- Plug'n'play: Fully tested connectivity and communication
- Soldered and therefore more robust eSIM instead of plug-in SIM from third-party providers
- Can be deactivated and reactivated at any time to save costs outside the vehicles' operating season
- National roaming in all available countries provided by Vodafone: a current overview is given at [BODAS Connect Countries List](#)
- Pooling of data volumes across multiple RCUs with the same tariff, i.e. additional data volume of one machine can be compensated by reduced volume from another machine with the same tariff
- Pay per use if the booked data volume is exceeded
- Increased cyber security through whitelisting of Access Point Name (APN) via integrated mobile radio provided by Vodafone



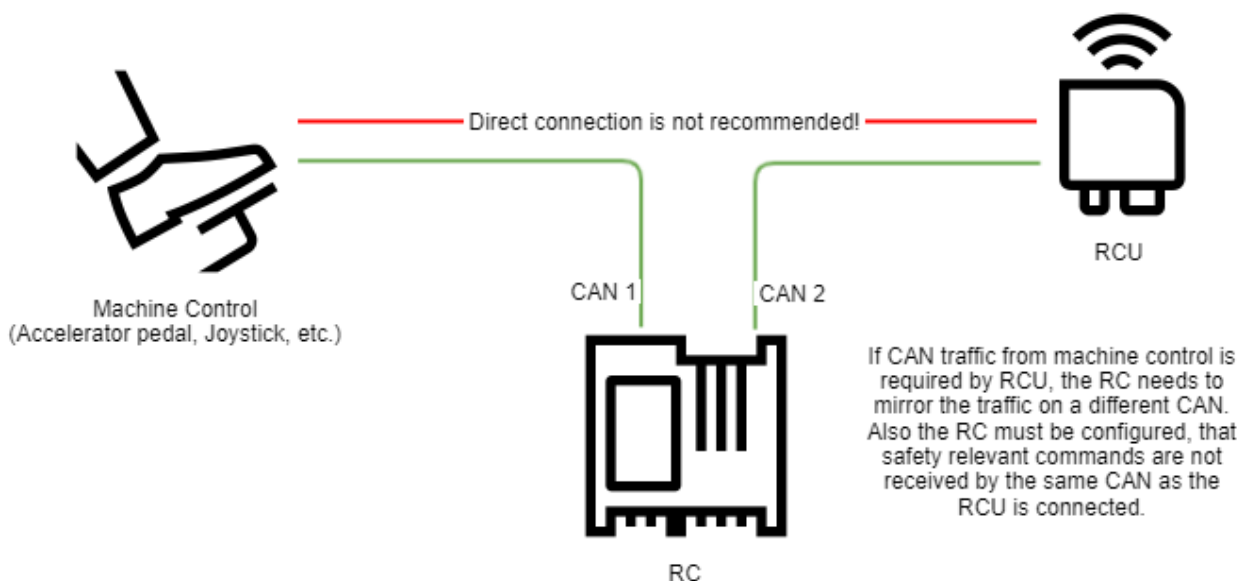
## 4 Privacy, Security & Safety

### 4.1 Security & Safety instructions

#### 4.1.1 CAN

When installing the RCU, it is important to consider the E/E architecture of machine or vehicle. The RCU shall not be connected to the same CAN network as control units like joysticks, pedals, and so on. Otherwise, the RCU would have the opportunity to send CAN frames, which may interfere with the machine control commands. Also, an attacker gaining access to the RCU would be able to control the machine.

Since the RCU is not a safety-certified device, no safety-relevant functions may be implemented and used on the RCU. The connected devices must be designed in such a way that safe operation of the machine is always ensured.



#### 4.1.2 Physical Interfaces

All interfaces are secured by the BODAS Connect software. However, precautions need to be taken to ensure that only authorized personnel has access to the RCU. Only trained users should access and work on the RCU's physical interfaces (e.g. Ethernet, USB, SD Card, SIM card, cable harness).

#### 4.1.3 Protective Measures

To reduce residual risks, all users of either the RCU or the BODAS Connect software need to be trained about protective measures with regards to IT security.

##### Strong Passwords

Weak passwords are a common source for cyber attacks (e.g. brute-force attacks). Therefore, user shall always choose a strong password complying to below suggestions.

- Use of lower- and uppercase letters
- Use of numbers
- Use of special characters (e.g. / , \$ , & , % , ...)
- Use a long password of more than 15 characters

- Avoid character sequences (e.g. 12345 , abcde , qwerty , ...)
- Avoid personal related words (e.g. pet names, spouse names, birthdays)

## Hacker Attacks

Cyber crime is common today. The following measures can help to avoid hacker attacks.

- Never use open, free, unprotected, or unknown wifi networks (wifi networks should be secured by WPA2 (AES) or WPA3)
- Never visit websites without valid SSL certificate or via HTTP protocol (websites should always use HTTPS)
- Always actively log off from websites, computers, and other devices
- Install the latest software updates from Rexroth
- Unauthorized personnel should not get access (physical and remote) to neither the RCU nor any Rexroth software
- Every user should sign in to the Rexroth software solutions with his/her individual account
- Contact Rexroth upon discovery of any suspicious or obscure activity

## Social Engineering

A social engineering attack represents the attempt of manipulating a person on a social interaction basis, in order to gain access to the user credentials or any other means of access to the software product.

A user should never pass his/her access credentials to a third party. Rexroth will **never** ask anyone for user credentials.

## 4.2 Cybersecurity

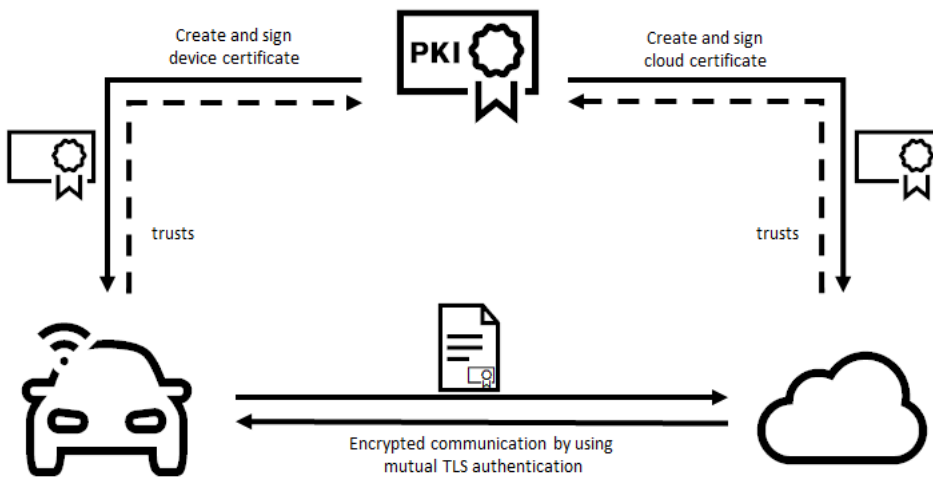
### 4.2.1 BOSCH Security Engineering Process

The development of the Bosch Rexroth Device Connectivity adheres to the BOSCH Security Engineering Process (SEP). The SEP supplements the engineering / development processes during the development of products in terms of information security and data protection, for the design and development of secure and data-protection-compliant Bosch products. In addition, the SEP covers the whole life-cycle of a product until the decommissioning.

### 4.2.2 Certificate management and Certificate-based device authentication

The Bosch Rexroth Device Connectivity uses certificates for authentication between the device and the Device Portal. If a device wants to update the status (e.g. after boot up), the device sends the status and a device certificate to the Device Portal. The device certificate is unique and created for the device during the production process by a public key infrastructure (PKI). The Device Portal will validate if the device certificate is valid or not, by having a store of trusted certificates that contains a certificate that is signed by the PKI.

The device can do the same, since the Device Portal will also send its certificate to the device with each message. This procedure is called mutual TLS authentication, since both parties can authenticate the other party without exchanging passwords. If a device is stolen, the corresponding device certificate will be blacklisted by the PKI. To increase security, the certificates are only valid for a certain period of time and will be refreshed automatically in the field.



### 4.2.3 Embedded firewalls

Vehicle interfaces as well as wireless interfaces are protected with embedded firewalls. The firewalls are used for filtering senders, receivers and incoming and outgoing packets, from cloud servers and to the vehicle (CAN).

Example:

- Only CAN messages with CAN IDs configured in the CAN Firewall will be forwarded to or read from the vehicle CAN network
- Applications will only be able to contact cloud servers with IP addresses whitelisted in the TCP firewall

## 4.3 Safety instructions

The usage of the Rexroth Device Connectivity for:

- installing new software, updating software, removing software or re-configuring hardware or software on Rexroth Controllers
- installing new software, updating software, removing software or re-configuring hardware or software on Rexroth Connectivity Units, that send or read data through or may have an impact on vehicle interfaces (CAN, Input/Output, Ethernet, Kline, RS232, RS485, KLine)

is referred to in the following as **safety-related usage**.

### 4.3.1 General instructions

- Safety-related usage in the standard working mode of the machine is not permissible.
- Safety-related usage in combination with a controller or electrified valves in a machine or vehicle is only permissible during commissioning of the machine or during service operations. Appropriate safety measures must be provided against hazards caused by unexpected operating conditions.
- Safety-related usage may only be performed by trained and experienced specialists who are sufficiently familiar with both the components used and the complete system.
- During safety-related usage, the user is responsible for ensuring that changes are compatible with the device hardware and the machine/vehicle in question.
- Incorrect safety-related usage may create potential hazards while the machine is in operation.
- It is the responsibility of the machine manufacturer to identify hazards of this type in a hazard analysis and to bring them to the attention of the end user. Rexroth assumes no liability for dangers of this type.

- System developments, installations and commissioning of electronic systems for controlling hydraulic drives must only be carried out by trained and experienced specialists who are sufficiently familiar with both the components used and the complete system.
- During safety-related usage, the machine may pose unforeseen hazards. Therefore the vehicle and the hydraulic system have to be in a safe condition during such operations.
- Make sure that nobody is in the machine's danger zone.
- No defective or incorrectly functioning components may be used. If the components should fail or demonstrate faulty operation, repairs must be performed immediately.
- During safety-related usage, the energy source (e.g. diesel engine) must be switched off during data transfer to the electronic controller.

### 4.3.2 Intended use

- Operation of the electronic hardware during safety-related usage must generally take place within the operating ranges specified and released in its data sheet, particularly with regard to voltage, temperature, vibration, shock and other described environmental influences.
- Use outside of the specified and released boundary conditions may result in danger to life and/or cause damage to the components, which could result in sub-sequential damage to the mobile working machine.

### 4.3.3 Improper use

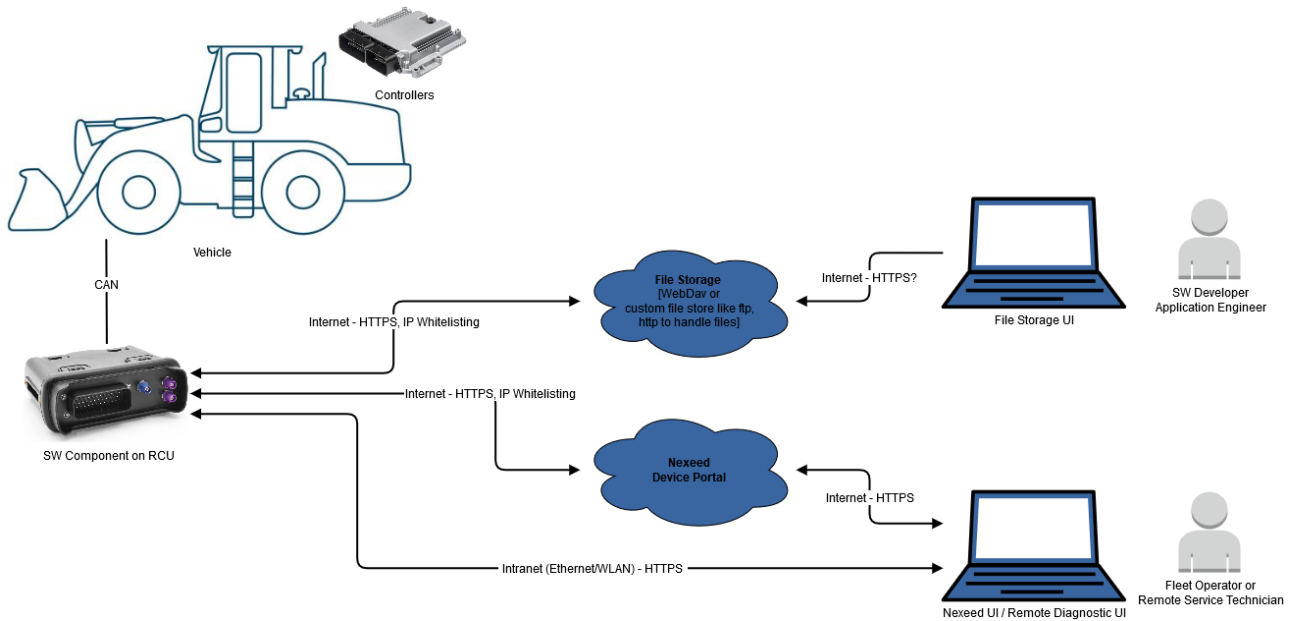
- Any safety-related usage other than described in the chapter "Intended use" is deemed to be improper use.
- Use in explosive areas is not permissible.
- Damage resulting from improper use and/or from unauthorized intervention not described in this data sheet renders all warranty and liability claims void against the manufacturer.

### 4.3.4 Use in safety-related functions

- The customer is responsible for performing a risk analysis of the mobile working machine and determining the possible safety-related functions.
- In order to ensure the functional safety according to EN ISO 13849 and/or ISO 25119, the customer (machine manufacturer) must make sure that following requirements are strictly followed.
  - The machine must go into the safe state before a safety-related usage is allowed and stays in the safe state during safety-related usage.
  - The disconnection from the diagnostic session for flashing must not lead to automatic initiation of machine movements and must not automatically lead the machine to an unsafe state.
  - Before safety-related usage, the changes shall be validated with sufficient testing and approved for the machine configuration.
  - After safety-related usage, it must be sufficiently verified that the correct changes have been performed.

# 5 OTA Services - OEM Responsibilities

## 5.1 Overview Workflow



### 5.1.1 Terminology

- **OTA Services:** Software and parameter update, read and erase errors, read process values on Rexroth Controllers using BODAS Connect Solutions.
- **RC information:** Minimum information for identifying a controller on the web-frontend:
  - Hardware type and serial number
  - Base software name and version
  - Application software name and version
  - Last flashing date

## 5.2 OEM Responsibilities with regard to functional safety

A distinction is made between two different use cases, "**Service Case**" and "**End User Case**", where the "**End User Case**" has higher requirements regarding OTA Services than the "**Service Case**".

1. Use Case "**Service Case**". Here, in the event of a troubleshooting or maintenance activity, an update of the software or change of parameters is performed in a 1:1 relationship. This activity takes place time-synchronously and with direct access to the machine or vehicle. Therefore, an explicit handshake between the machine and the telemetry unit is not required.
2. Use Case "**End User Case**". Here, in the case of a 1:n relationship, an update of the software is performed. This activity takes place time-asynchronously and without direct access to the machine or the vehicle. The update is assigned to specific vehicles and installed at a later time. The machine must be in a safe state for this and the respective control unit decides whether or not the update is carried out based on the integrated detection of the ambient conditions.
  - a. The BODAS Connect Device Connectivity Software will forward CAN messages on the CAN vehicle with information about the progress, success/failure and impacted safety function of/by OTA Services. The OEM is responsible to display those information, with the right representation (e.g. warning icon for a warning), to the machine driver/operator.

Please pay attention

- Incorrect OTA Services may create potential hazards while the machine is in operation.
- No defective or incorrectly functioning components may be used. If the components should fail or demonstrate faulty operation, repairs must be performed immediately.

### 5.2.1 Before using OTA services

- OTA Services may only be performed by trained and experienced specialists who are sufficiently familiar with both the components used and the complete system.
- Machine operators/drivers shall be trained with regard to the impact of OTA Services.
- There are necessary security measures to ensure that communication over CAN is secured.
- In order to ensure the functional safety according to EN ISO 13849 and/or ISO 25119, the customer (machine manufacturer) must make sure that following requirements are strictly followed.
  - The machine must go into the safe state before OTA Services are allowed and stays in the safe state during OTA Services.
  - The disconnection from the diagnostic session for flashing or parametrization must not lead to automatic initiation of uncontrolled machine movements and must not automatically lead the machine to an unsafe state.
- It is the responsibility of the machine manufacturer to identify hazards of this type in a risk analysis, to document safety-related functions that might be impacted by OTA Services in the machine manual and to bring them to the attention of the end user. Rexroth assumes no liability for dangers of this type.

### 5.2.2 While using OTA services

- Ensure that nobody is in the machine's danger zone.
- The remote maintenance technician/fleet operator/software developer is responsible for ensuring that any changes (e.g. software changes, parameter adjustments, etc. ) are compatible with the device hardware and the respective machine/vehicle.
- Provide a possibility for displaying approval or disapproval request of OTA Services to the machine operator/driver performed through the Device Management (Bodas Service Remote Diagnostic not used).
- The energy source (e.g. diesel engine) must be switched off during data transfer to the connected electronic devices

### 5.2.3 After using OTA services

- The machine driver/operator shall be informed on the success and failure of update.
- After OTA Services that are performed through the Device Management (Bodas Service Remote Diagnostic not used), the OEM machine software shall inform the machine driver/operator about the safety functions that have been re-configured, updated, deleted or added, the machine driver/operator shall only start the vehicle after reading and understanding the information that is provided.

## 6 Project Planning Notes

### 6.1 Software & Bus configuration for allowing IoT Services

Rexroth will provide a customized software for reading out CAN values from CAN bus. For this, following prerequisites are among others to be fulfilled from the customer side:

- Machine with fully functional E/E architecture including CAN-bus interface
- Cabling to connect the Rexroth Connectivity Unit (RCU)
- Customer provides CAN Configuration (e.g. DBC) with parameters which should be read out from the vehicle/ machine and visualized on the dashboard

For the entire catalogue of prerequisites please get in touch with your sales interface or contact [connect.bodas@boschrexroth.de](mailto:connect.bodas@boschrexroth.de)

Bosch Rexroth AG  
Robert-Bosch-Straße 2  
71701 Schwieberdingen  
Germany  
[www.boschrexroth.com](http://www.boschrexroth.com)

© Bosch Rexroth AG 2023. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

The data specified within only serves to describe the product. No statements concerning a certain condition or suitability for a certain application can be derived from our information. The information given does not release the user from the obligation of own judgment and verification. It must be remembered that our products are subject to a natural process of wear and aging.