IEC 62443 using the myREX24 V2 portal

Convergence between IT and OT in everyday routine

Version 01 / 16.08.2019

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com

Content Page

1 IEC 62443 in practice

The international standard IEC 62443 is a foundational body of rules concerning security in the area of industrial communication and IT networks. Industrial companies should in this way be better protected against failures in IT and OT. A special focus is on the protection of the networks against hacker attacks, manipulation, malware, and other similar attacks.
This standard also makes reference to fault conditions and false configurations that can influence the output or productivity. Remote maintenance is only one element within the IEC 62443 perspective to which special attention is paid.

1.1 Fundamental requirements of systems and components pursuant to IEC 62443

The following points are to be observed pursuant to IEC62443:

- Identification and authentication
- Usage control
- System integrity
- Confidentiality of data
- Restricted data flow
- Timely reaction to events
- Availability

In the following chapters, the subject of how the IEC 62443 harmonizes with the myREX24 V2 will be covered in more detail. The requirement will be explained at the beginning of each point and the approach to a solution with the myREX24 V2 or a best practice approach shown.

1.2 Interface between machine mechanical engineers and operators

The myREX24 V2 portal, in combination with the REX routers, assists you with the best possible implementation of this standard. The portal is thus an important component of machine integration in your company network. From the perspective of IT security, conventional remote maintenance of a machine should always be considered a critical element in the risk evaluation. However, remote maintenance is indispensable for production routine. For machine manufacturers, it is for a number of reasons often unprofitable and/or incompatible with the appropriate own protection of the machine/development know-how to accept customer-specific remote maintenance solutions. Of course, the focus is always on the IT security aspect, both for the mechanical engineers and the machine operators. A common process or a shared interface should therefore be defined both technically and in the communication between operators and mechanical engineers.

1.3 myREX24 V2 as a technical interface at eye level

The myREX24 V2 portal is designed from the start for the interplay of IT and OT and is integrated seamlessly into the existing infrastructure. Both machine operators and machine and system builders thus have a common interface at an industrial level at their disposal. Handiness and availability are maintained on both sides.

Through the use of REX routers in combination with the myREX24 V2 portal, one also profits from the auxiliary effect of a structured network topology, micro-segmentation (smaller broadcast domains), and insight into how often remote maintenance accesses are activated. This alone provides more insights and possibilities for reevaluating or reorganizing remote maintenance.

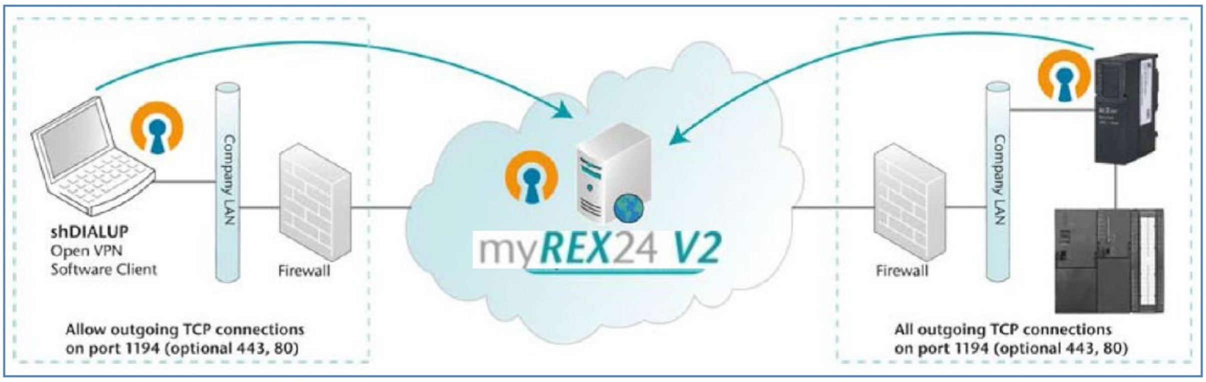
Administrators in the myREX24 portal can at any time trace which users are connected with the respective machine. The duration and quantity of data transferred is also logged.

Many Helmholz customers are deciding in favor of the use of the public portal, thus the use of the Helmholz server. Upon request, the myREX24 V2 server software can also be comfortably hosted in one's own computer center. Usability is thus retained, in comparison to classic IT remote solutions, and data sovereignty returns to one's own company. Those who don't wish to use their own IT resources for a myREX24 V2 server, but nonetheless wish to retain data sovereignty, leave administration to Helmholz. Helmholz will then establish a virtual myREX24 V2 server with a professional hoster, which belongs to the respective customer. The server and the related data are thus transferred to the buyer, while Helmholz looks after the commissioning of the server.

1.4 The myREX24 portal

The VPN portal myREX24 V2 serves as a mediation server for VPN communication between the provider of remote maintenance and the customer facility. On the one hand, it provides central VPN access for programmers and machine and service technicians, while it also serves as an access point of the machine for the REX routers. The myREX24 V2 portal can also be used for the protocoling and visualization of machine data, which can be read in from the machine via the REX router.

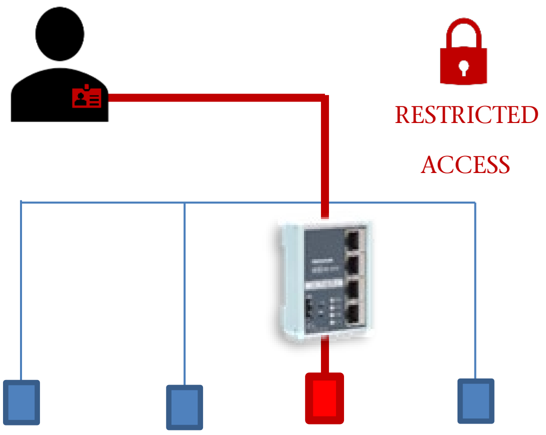
Each REX router is unambiguously assigned to a company account in the myREX24 V2 portal. Any number of users with access rights can be administered in the account. This ensures that only authorized users have access to the approved router on this platform.


shDIALUP
Open VPN
Software Client
Company LAN
Firewall
Allow outgoing TCP connections
on port 1194 (optional 443, 80)
myREX24 V2
Firewall
Company LAN
All outgoing TCP connections
on port 1194 (optional 443, 80)

Likewise, integration into local firewalls is simplified with the VPN portal. Local firewalls are connected to the WAN network of the router. Access from the Internet to the REX router is usually prohibited. Outgoing connections are often allowed or can be easily and securely realized. The router then in this way "dials" into its account on the central VPN server.

Further information can be found in the white paper "The myREX24 V2 functional principle." In addition to the public portal, the myREX24 V2 portal can also be hosted as an autonomous virtual server or OEM variant.

2 Requirement: Identification and authentication

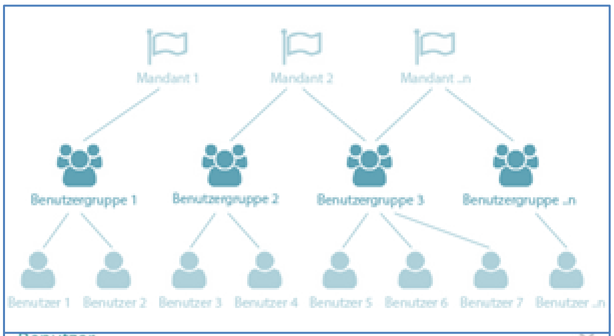


Requirement:
It must be possible to clearly identify and authenticate processes, devices, and users! Distribution of responsibilities and restriction of access should be observed accordingly.

Solution:
The myREX24 V2 portal fulfills these requirements through comprehensive user access administration and can, depending upon the user, restrict the access such that only the required components can be seen and accessed.

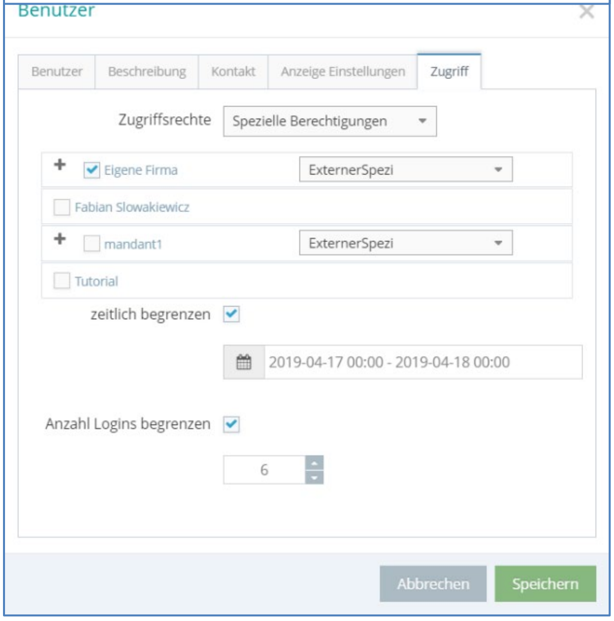
Conventional remote maintenance solutions generally have access to the entire machine network and can often not implement these restrictions. With the myREX24 V2, you have access control during maintenance work in your hands at all times. You require an optional license for this function: *"Access restriction to component level 800-874-USR01"*
You can find details under the chapter "Limited data flow control"

2.1 User and client administration



A differentiation is generally made in the myREX24 V2 portal between user groups, users, clients, and projects.

Each user receives his own user name and password.
Every user is thus clearly identifiable at the portal.


Benutzer

Zugriffsrechte: Spezielle Berechtigungen

+ ☑ Eigene Firma — ExternerSpezi
☐ Fabian Slowakiewicz
+ ☐ mandant1 — ExternerSpezi
☐ Tutorial

zeitlich begrenzen ☑
2019-04-17 00:00 - 2019-04-18 00:00

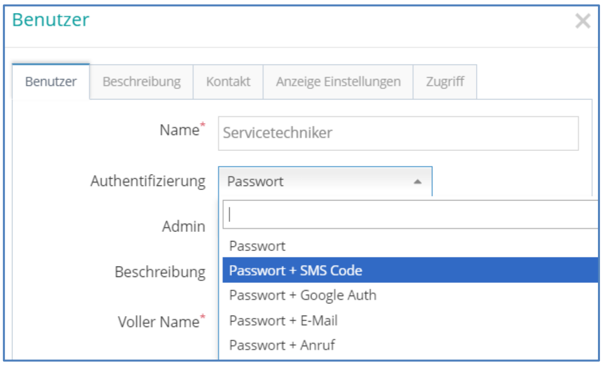
Anzahl Logins begrenzen ☑
6

In addition to normal users, it is possible to set up temporary access for external programmers (for example, a drive specialist).
Temporary access can be delimited both in terms of the number of logins at the portal and of the respective period of time.

Temporary users also receive their own access data and are limited accordingly in terms of their rights through control of the user groups. As with the standard users, all activities of the temporary user are protocoled by the myREX24 V2.

Users only have access to the projects and machines to which they have been assigned.
You can also find details here:
http://www.cc-onlinehelp.com/de/#index/verwaltung/benutzerverw_1.html

2.2 2-factor authentication



Name* Servicetechniker

Authentifizierung Passwort

For security reasons, 2-factor authentication is recommended for portal users.

Various methods are available to this purpose. Similar to with online banking, authentication can take place via an additional SMS code, a separate e-mail with activation link, a call, or Google authentication.

You can find more details on 2-factor authentication here:
http://www.cc-onlinehelp.com/de/#index/verwaltung/benutzer/authentifizi/authentifizi.html

3 Requirement: Usage control

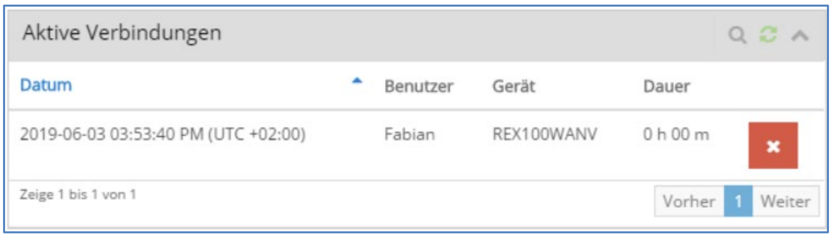
Requirement:
Relevant records must be kept and provided.

- Usage control:
    - Which router/machine was online?
    - When?
    - How long?
    - Which user?
    - What was done?
- Activity monitoring:
    - Configuration changes
        - If yes, which and why?
    - Attempts to log in/ login activity

Solution:
The myREX24 V2 portal fulfills these requirements through automatic protocoling of various activities or offers documentation possibilities at the places that can’t be automatically registered.

Usage control for an active VPN connection:

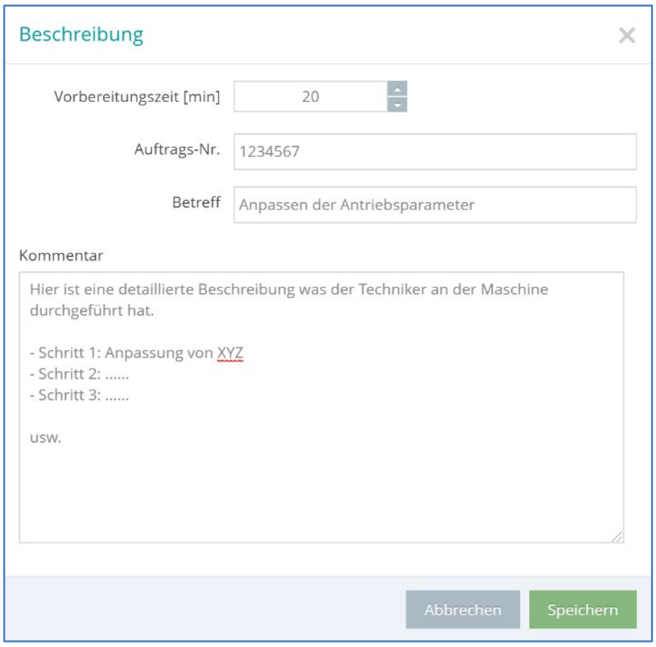
If an active connection exists, this is visible at several points of the portal. For example, on the welcome page, in the main navigation, or for the respective device.



Aktive Verbindungen

Datum	Benutzer	Gerät	Dauer
2019-06-03 03:53:40 PM (UTC +02:00)	Fabian	REX100WANV	0 h 00 m

Zeige 1 bis 1 von 1



Beschreibung

Vorbereitungszeit [min]	20
Auftrags-Nr.	1234567
Betreff	Anpassen der Antriebsparameter

Kommentar

Hier ist eine detaillierte Beschreibung was der Techniker an der Maschine durchgeführt hat.

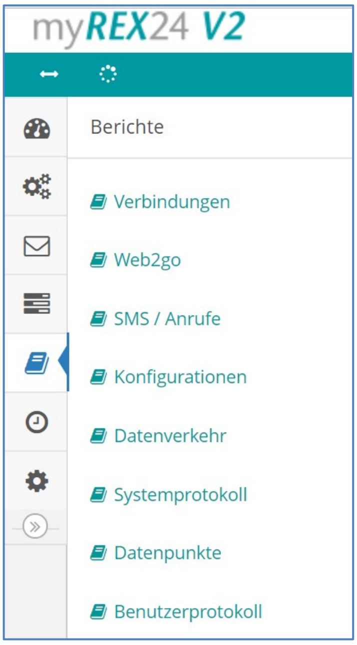
- Schritt 1: Anpassung von XYZ
- Schritt 2: ......
- Schritt 3: ......

usw.

The user can document the work carried out following each VPN connection.

Additional fields for, for example, an order number and set-up/preparation time are offered. This also makes the detailed invoicing of the service with the end customer easier.

3.1 Automatic protocoling

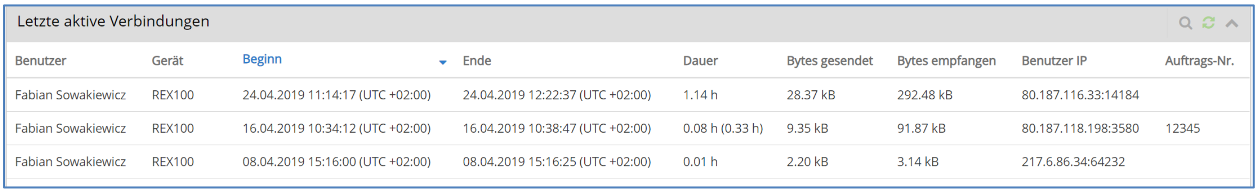


Insight into all portal activities is possible via the "Reports" tab.

The task planner also makes it possible to automatically send the reports once a month, for example, to an e-mail address.

Extensive information for usage control can be viewed in the individual reports. Here are only a few examples:

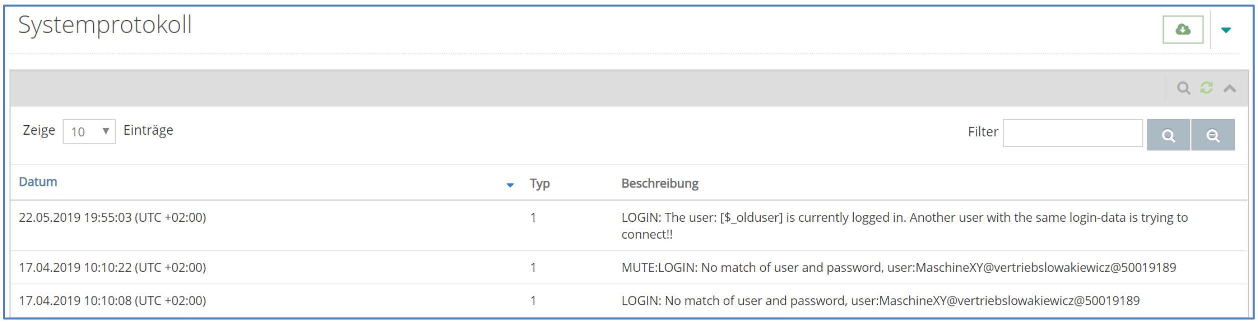
History of the active connections:



Letzte aktive Verbindungen

Benutzer	Gerät	Beginn	Ende	Dauer	Bytes gesendet	Bytes empfangen	Benutzer IP	Auftrags-Nr.
Fabian Sowakiewicz	REX100	24.04.2019 11:14:17 (UTC +02:00)	24.04.2019 12:22:37 (UTC +02:00)	1.14 h	28.37 kB	292.48 kB	80.187.116.33:14184	
Fabian Sowakiewicz	REX100	16.04.2019 10:34:12 (UTC +02:00)	16.04.2019 10:38:47 (UTC +02:00)	0.08 h (0.33 h)	9.35 kB	91.87 kB	80.187.118.198:3580	12345
Fabian Sowakiewicz	REX100	08.04.2019 15:16:00 (UTC +02:00)	08.04.2019 15:16:25 (UTC +02:00)	0.01 h	2.20 kB	3.14 kB	217.6.86.34:64232	

System protocol:

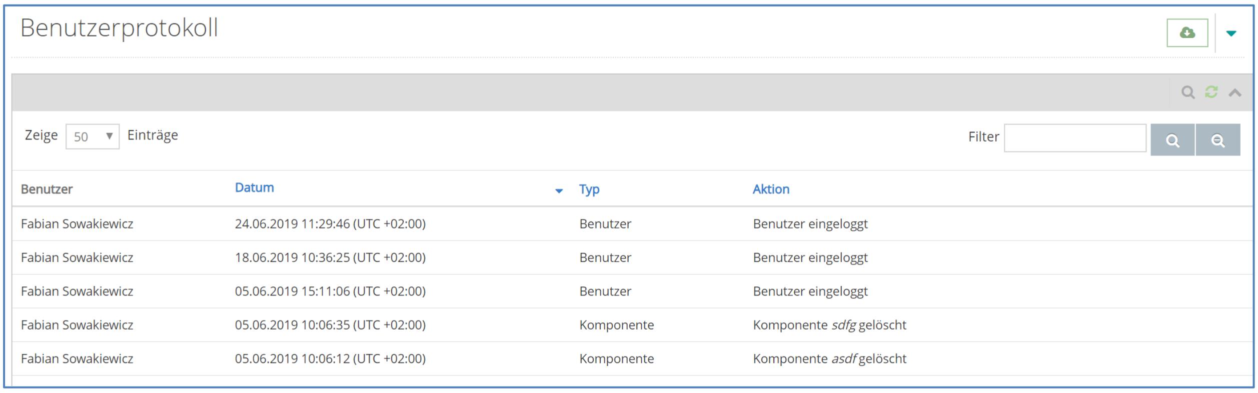


Systemprotokoll

Zeige 10 Einträge Filter

Datum	Typ	Beschreibung
22.05.2019 19:55:03 (UTC +02:00)	1	LOGIN: The user: [$_olduser] is currently logged in. Another user with the same login-data is trying to connect!!
17.04.2019 10:10:22 (UTC +02:00)	1	MUTE:LOGIN: No match of user and password, user:MaschineXY@vertriebslowakiewicz@50019189
17.04.2019 10:10:08 (UTC +02:00)	1	LOGIN: No match of user and password, user:MaschineXY@vertriebslowakiewicz@50019189

User protocol:



Benutzerprotokoll

Zeige 50 Einträge Filter

Benutzer	Datum	Typ	Aktion
Fabian Sowakiewicz	24.06.2019 11:29:46 (UTC +02:00)	Benutzer	Benutzer eingeloggt
Fabian Sowakiewicz	18.06.2019 10:36:25 (UTC +02:00)	Benutzer	Benutzer eingeloggt
Fabian Sowakiewicz	05.06.2019 15:11:06 (UTC +02:00)	Benutzer	Benutzer eingeloggt
Fabian Sowakiewicz	05.06.2019 10:06:35 (UTC +02:00)	Komponente	Komponente *sdfg* gelöscht
Fabian Sowakiewicz	05.06.2019 10:06:12 (UTC +02:00)	Komponente	Komponente *asdf* gelöscht

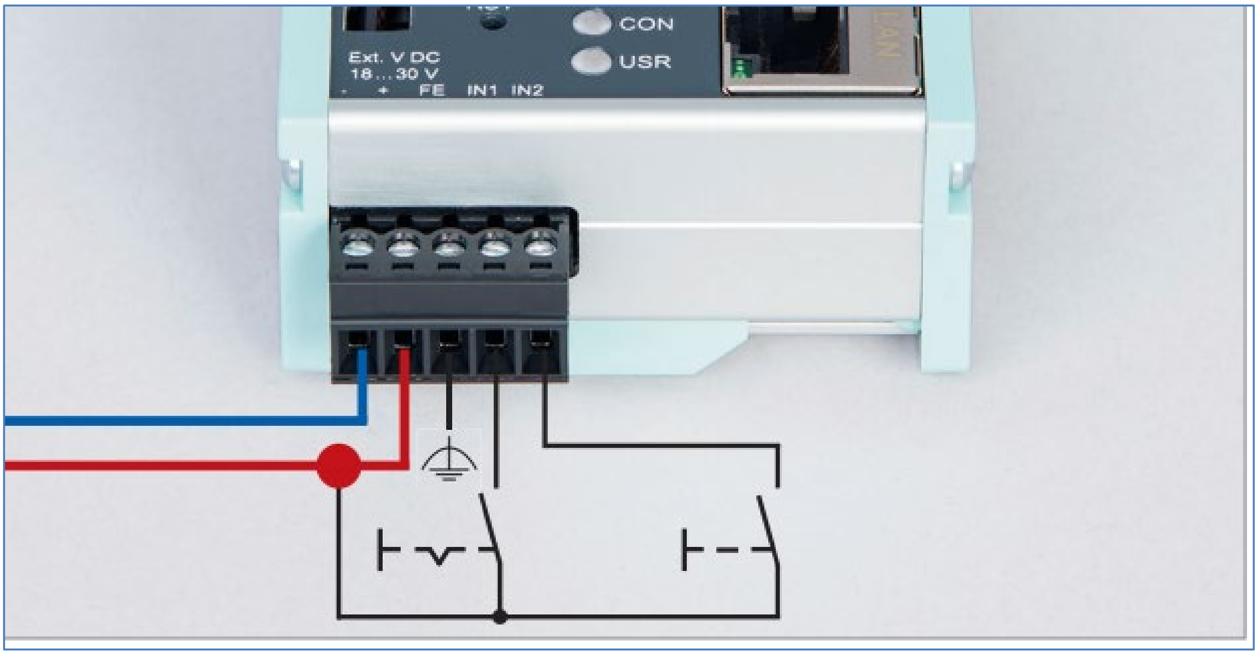
You can also find details about the reports here:
http://www.cc-onlinehelp.com/de/#index/berichte/berichte.html

3.2 Physical authorization via digital inputs

There is also a possibility to activate/deactivate the outgoing VPN connections of the router to the portal via the digital inputs of the routers. In practice, this takes place via key switches directly at the control cabinet. Only authorized persons receive the keys. There is generally prior contact by telephone between mechanical engineers and operators in order to define the authorized key persons and clarify technical benchmark data.

Example on the basis of a REX 100:
IN1 can be used for the VPN establishing of connection with the myREX24 portal. An alarm can be triggered with the IN2. The use of both inputs for the alarm is also possible. The configuration of the alarms takes place via alarm management in the myREX24 V2 portal.

Example illustration:



4 Requirement: System integrity

Requirement:

The integrity of the data sent to the control system should be ensured.

This includes:

- Malware or unauthorized software should be recognized, reported, and its execution prevented or limited. This also applies to unauthorized access.
- Planned behavior of the devices, for example, planned upkeep, should also be verified. Should devices demonstrate anomalous behavior here, this must be displayed for the user.
- Software changes and unauthorized manipulation of information should be recognized and recorded. It is of course of primary importance to provide protection against such changes.

Solution:

Within the machine, additional tools, such as the use of an Intrusion Detection and Intrusion Prevention System (abbreviated: "IPS&IDS"), as well as the use of engineering tools with corresponding security features is presumed. The PLC used must also harmonize with the engineering tool and support the security standards.

4.1 General:

Because the testing of system integrity contains several important points, the consideration of holistic communication is always to be kept in mind. The myREX24 V2 may be the transmission path, but it is primarily the communication between PLC and the engineering tool that is decisive for the integrity of the data. The security level can be additionally improved by, for example, additional passwords (PLC write protect) and other security measures, such as monitoring for PLC program changes, etc. Depending upon the desired security level, the use of "security boxes" that also check the PLC for variables or program changes is also conceivable.

You can also find more information on the theme of system integrity with the manufacturer of your PLC and the engineering tool.

4.2 Fail2ban:

The myREX24 V2 system uses the software Fail2ban on the remote maintenance side. The configuration of this function is only accessible via the back end of the myREX24 V2 server. Fail2Ban serves the purpose of determining and blocking certain IP addresses that might belong to attackers. If, for example, repeated attempts are made to log in with false passwords or other unplanned actions are carried out, these IP addresses are blocked.

In practice, the block will be lifted by the system after a few minutes in order to continue to allow serious connection attempts (user name or password entered incorrectly). Blocking for a few minutes effectively counters, for example, brute force attacks.

5 Requirement: Confidentiality of data

Requirement:

The confidentiality of communication is to be protected. Cryptographic methods and internationally recognized and proven security practices are to be used.

Solution:

The myREX24 Server Portal was implemented on the basis of OpenVPN. The encryption of OpenVPN is based on OpenSSL.

Access to the website of the myREX24 V2 portal is only possible via the HTTPS-encoded connection. The “v2.myrex24.net” website is secured with a certificate that is also tested by the shDIALUP software.

The following security features are used on the public servers:

- Based on open source standard “OpenVPN”
- Authentication of the server by X.509 certificate (RSA 1024-bit)
- Client authentication by user name/password
- Password rules for user authentication can be set
- 2-factor authentication methods (SMS, e-mail, telephone call, Google authentication)
- Random 15-digit OpenVPN password for each REX router (can be changed)
- Diffie-Hellman key exchange with 1024-bit
- OpenVPN transmission encryption with OpenSSL (TLS 1.x), Blowfish CBC (128-bit), SHA1
- Only HTTPS access to the web front end of the portal is possible
- A separate OpenVPN server is assigned to each account (allocation via account name)
- REX routers are hard-connected with one account in the initial configuration
- Hosted in a high security computer center of a European hoster: o PCI-DSS certification
- Certification according to ISO/IEC 27001
- Certification according to SOC 1 TYPE II and SOC 2 TYPE II
- Redundant hosting (up to 99.5 % availability)
- Separation of business and machine network in the REX router with internal firewall
- User and rights management system in the portal
- Extensive reporting (connection history, configuration changes, activity protocol)
- “myREX24 virtual server” for independent, autonomous, and stand-alone operation
- Constant security updates of the portal software
- Rapid response when security vulnerabilities are reported

Additional information

http://openvpn.net/index.php/open-source/documentation.html

http://www.openssl.org/related/ssl.html

https://www.bsi.bund.de → “ICS Security Compendium” & “Remote maintenance in the industrial environment”

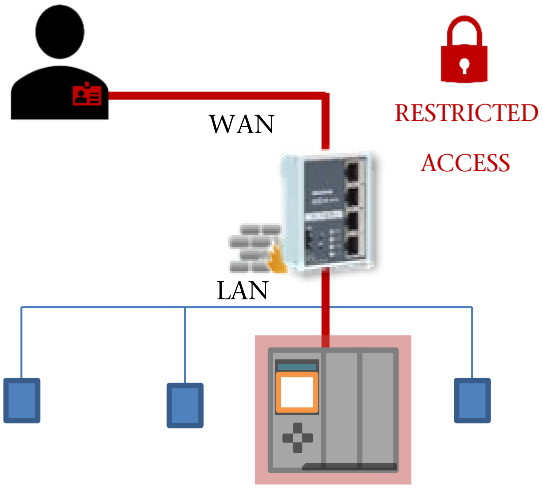
https://www.allianz-fuer-cybersicherheit.de

6 Requirement: Restricted data flow

Requirement:

- Segmentation of networks
- Restriction of general communication in the network from person to person (e-mails, social media, etc.)

Solution:



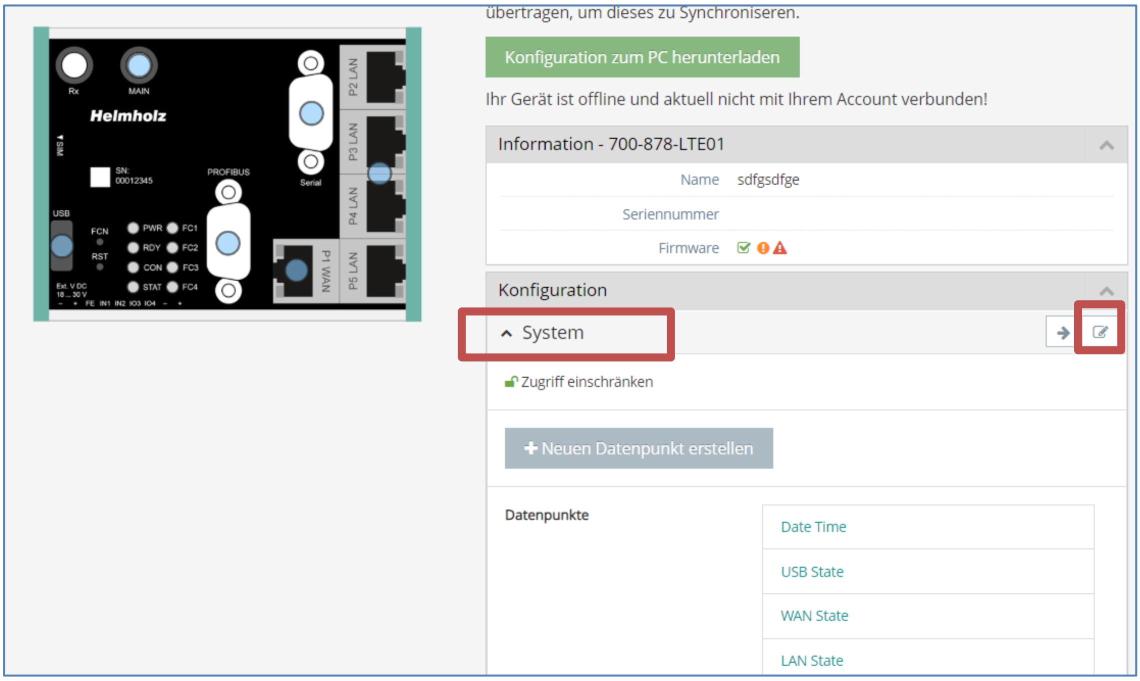
For purposes of segmentation, the REX routers are equipped with a WAN interface for the factory network and a LAN interface for the machine network.

In the factory setting, the firewall integrated into the routers prevents all access of the factory network to the machine network (WAN >LAN). Appropriate exceptions can be added through the firewall setting of the router.

In order to further restrict the data flow of the provider of remote maintenance, access to individual components, for example, exclusively to the PLC of the machine, can be restricted.

> Conventional remote maintenance solutions generally have access to the entire machine network and can often not implement these restrictions. With the myREX24 V2, you have access control during maintenance work in your hands at all times. You require an optional license for this function: *"Access restriction at component level 800-874-USR01"*

Access can be restricted as follows in one series of steps:



übertragen, um dieses zu Synchroniseren.

Konfiguration zum PC herunterladen

Ihr Gerät ist offline und aktuell nicht mit Ihrem Account verbunden!

Information - 700-878-LTE01

Name sdfgsdfge

Seriennummer

Firmware

Konfiguration

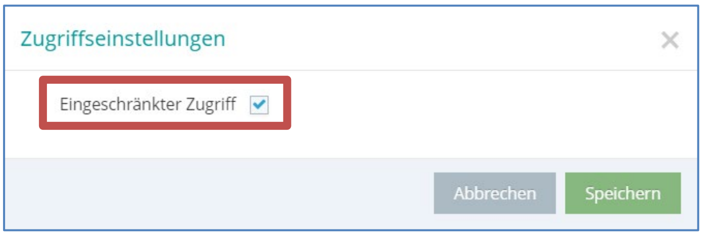
System

Zugriff einschränken

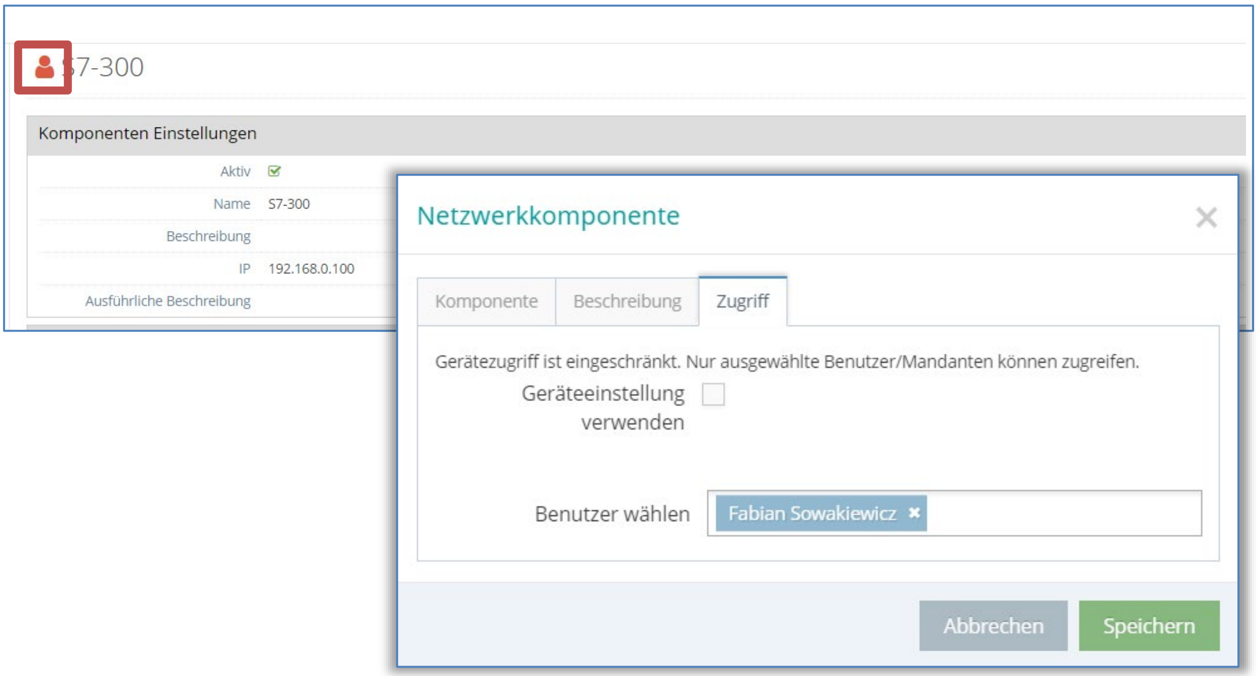
+ Neuen Datenpunkt erstellen

Datenpunkte

- Date Time
- USB State
- WAN State
- LAN State



Eingeschränkter Zugriff ☑



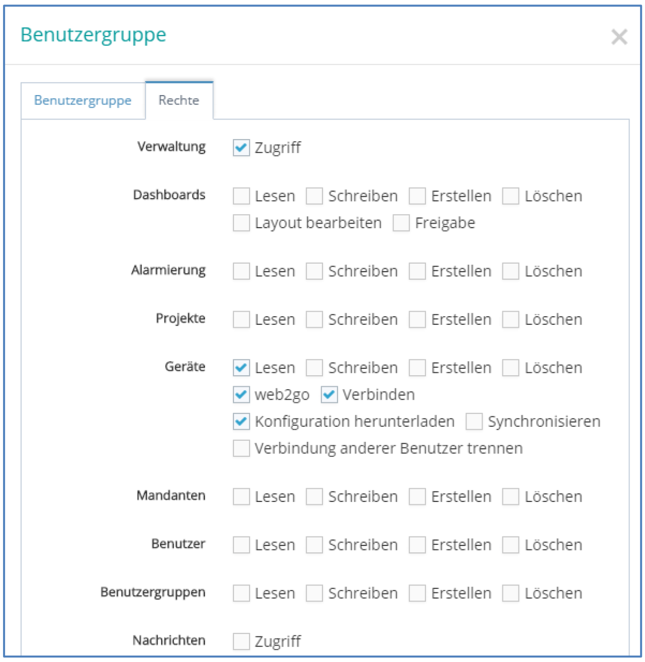
Aktiv ✓
Name S7-300
Beschreibung
IP 192.168.0.100
Ausführliche Beschreibung

Gerätezugriff ist eingeschränkt. Nur ausgewählte Benutzer/Mandanten können zugreifen.
Geräteeinstellung verwenden □
Benutzer wählen: Fabian Sowakiewicz ×

Only the selected user now has access to these network components.

6.1 Rights administration within a user group

Specific rights can already be defined in advance at the user group level.
Changes in the respective user group take effect for all affiliated users.
The settings can be made fine-grained. Here an excerpt:



Verwaltung	☑ Zugriff
Dashboards	□ Lesen □ Schreiben □ Erstellen □ Löschen □ Layout bearbeiten □ Freigabe
Alarmierung	□ Lesen □ Schreiben □ Erstellen □ Löschen
Projekte	□ Lesen □ Schreiben □ Erstellen □ Löschen
Geräte	☑ Lesen □ Schreiben □ Erstellen □ Löschen ☑ web2go ☑ Verbinden ☑ Konfiguration herunterladen □ Synchronisieren □ Verbindung anderer Benutzer trennen
Mandanten	□ Lesen □ Schreiben □ Erstellen □ Löschen
Benutzer	□ Lesen □ Schreiben □ Erstellen □ Löschen
Benutzergruppen	□ Lesen □ Schreiben □ Erstellen □ Löschen
Nachrichten	□ Zugriff

7 Requirement: Timely reaction to events

Requirement:

The performance of the system must be continuously monitored through security mechanisms. Security breaches or anomalies must be reported and evaluated immediately.

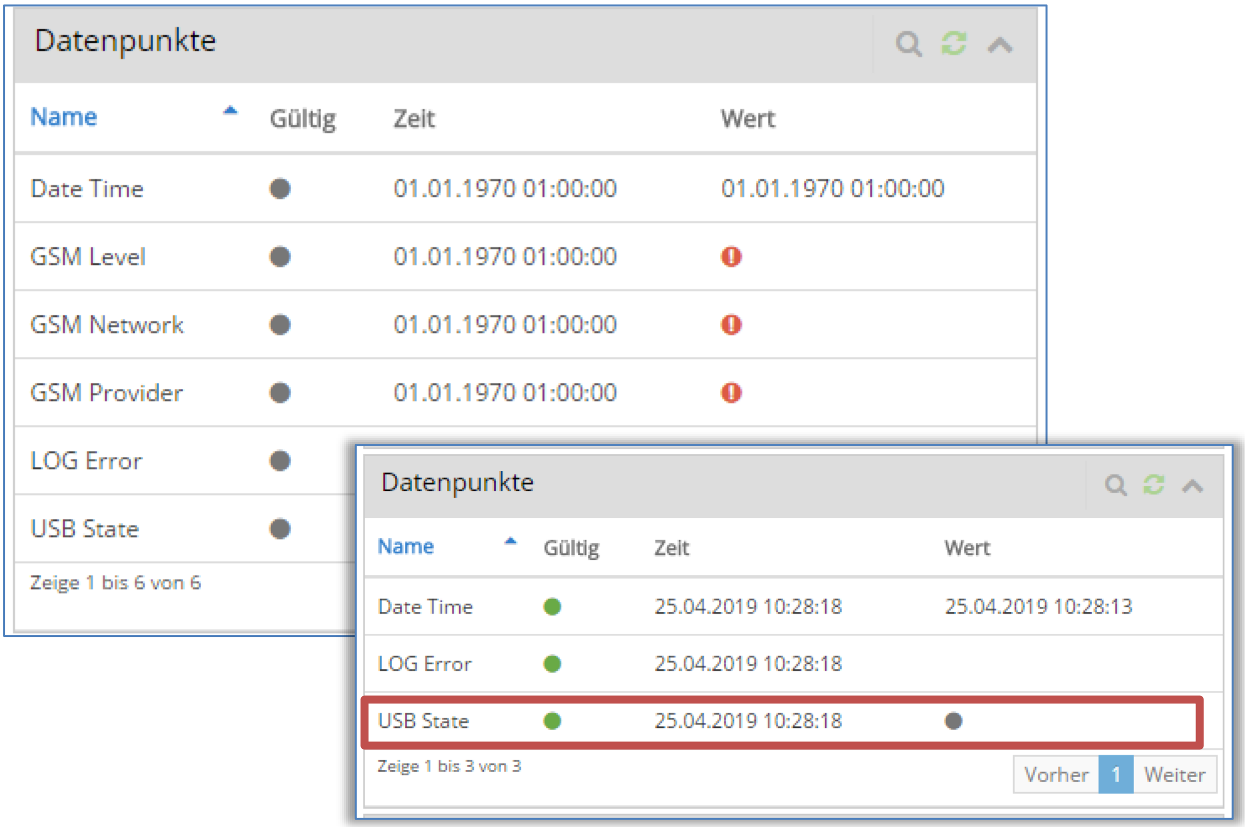
Solution:

The REX routers are equipped with data points internal to the system that can be linked with alarm and protocol functions.

7.1 Internal data points of the router

The USB socket of the device serves us in this scenario as the endpoint to be monitored. When a USB stick is plugged in or removed, an alarm message will be sent to the responsible personnel, depending upon the trigger set.

Here a brief excerpt of the system data points of a REX 250 LTE and a REX 100 WAN router. Once with active and once with inactive data values:



Datenpunkte

Name	Gültig	Zeit	Wert
Date Time	●	01.01.1970 01:00:00	01.01.1970 01:00:00
GSM Level	●	01.01.1970 01:00:00	❗
GSM Network	●	01.01.1970 01:00:00	❗
GSM Provider	●	01.01.1970 01:00:00	❗
LOG Error	●		
USB State	●		

Zeige 1 bis 6 von 6

Datenpunkte

Name	Gültig	Zeit	Wert
Date Time	●	25.04.2019 10:28:18	25.04.2019 10:28:13
LOG Error	●	25.04.2019 10:28:18	
USB State	●	25.04.2019 10:28:18	●

Zeige 1 bis 3 von 3

Various data points are available depending upon the version of the device. When the USB socket is not required for the application, it is recommended that this be deactivated. Depending upon the configuration of the router, the USB interface can be addressable in a network via the LAN.

7.2 Access control at the control cabinet

In this context, the protocoling and alarming of the digital inputs at the router is also a possible monitoring point. Through the data points internal to the router, it is registered when the key switch for activation of the VPN setup was activated.

The monitoring concept can be expanded as desired.
The following consideration as food for thought:

- Is the control cabinet door monitored with a sensor?
  Remote maintenance could then only be declared as "normal" when the control cabinet door is closed.
- The end sensor and the key switch are already monitored via the PLC.
  Can other ambient sensors also be incorporated? For example, chip cards of the machine operators?

All of these points should also be considered in the risk assessment or in the implementation of the security concept in keeping with common sense and benefit.

8 Requirement: Availability

Requirement:

Measures are to be taken in order to ensure the availability of the system.

Solution:

The myREX24 V2 is hosted in a high security computer center of a European hoster:

- PCI-DSS certification
- Certification according to ISO/IEC 27001
- Certification according to SOC 1 TYPE II and SOC 2 TYPE II
- Redundant hosting (up to 99.5 % availability)

You can also find further information on the availability of the public server in our General Terms and Conditions https://www.helmholz.de/fileadmin/documents/AGBs/AGB_myREX24_Helmholz_GmbH_u_Co._KG.pdf

8.1 Server in your own hands

The myREX24 V2 portal can also host itself as a virtual machine.

- For “self-hosters”: legal security through the purchase of software, protection of own data
- For in-house or host operation
- Up to 20,000 devices, VPN clients, dashboards, and alarms possible
- Up to 250 active connections and 500 Web2Go connections can be realized simultaneously
- Log and visualize machine data and access
- Problem-free connection of a SQL database
- M2M networks can be realized

System prerequisites:

- VMWare ESXi server (as of V5.0.0) or vSphere
- min. 2 vCPUs, 2 GB RAM
- min. 20 GB storage
- “root” access to the ESXi server
- Internet connection
- A fixed, public IP address
- Public DNS name
- Own e-mail account for the portal (“vpn-portal@firma.com”)
- SSL web certificate for the DNS name (certificate and key)

Please let us know if you are interested in your own myREX24 V2 server. You can also find more information here: https://www.helmholz.de/fileadmin/documents/Flyer/My_REX_24_V2_REX-Router/Flyer_myREX24_virtual_Server_DE_07-2019.pdf

9 Summary

The requirements pursuant to IEC 62443 with regard to persons, hardware, software, processes, documentation, and planned necessary actions are both varied and complex.

As already mentioned at the start, remote maintenance is only one of the building blocks within a cybersecurity concept to be considered. In a risk analysis, these points must be considered in detail depending upon the application.

With the myREX24 V2 portal and the affiliated REX routers, you secure yourself a remote maintenance system with an extensive documentation and alarm scope. In comparison with standard VPN solutions, access and evaluation are quickly and transparently accessible. The myREX24 V2 portal convinces in everyday routine with usability that is practical for both the automation technician and the IT admin.

myREX24 V2 virtual

Machine access and data sovereignty in your hands