rexroth
A Bosch Company

IndraControl Security Manual

Project Planning Manual
R911342562

Edition 06

Change Record

Edition	Release Date	Note
Edition 01	2013-11	First edition
Edition 02	2015-01	Supplements
Edition 03	2017-04	Introductory chapter revised and references to external information sources supplemented. New devices supplemented.
Edition 04	2017-05	Notes on crypto trojans and ransomware supplemented.
Edition 05	2018-07	Devices (IndraControl VE*) with Windows Embedded compact 7 supplemented Notes on WebConnector supplemented with regard to the WebComposer Notes on trojans and ransom hardware edited Reference to basic BSI IT protection components System Drive (MLD) supplemented
Edition 06	2019-02	Additions: • SafeLogic compact • WinStudio software • Frequency converter EFC

Editorial Department

Development Automation Systems Control Hardware ThSc (MiNi/PiaSt)

Table of Contents

Page

1 Glossary

ACL	Access Control List Access rights to computer resources (files and programs) are administered using the ACL.
BSI	German Federal Office for Information Security The "BSI" is part of the German Federal Ministry of the Interior.
DHCP	"Dynamic Host Configuration Protocol" The DHCP service facilitates the assignment of the network configuration to clients by a server.
Firewall	A "firewall" is a network security systems in hardware or software to protect the system against unauthorized access.
(T)FTP	(Trivial) File Transfer Protocol (T)FTP is a file-oriented client-server protocol via a TCP connection. "Trivial" means that there are no functions to assign rights or functions for user authentication.
ICMP	Internet Control Message Protocol ICMP is used to exchange information and error messages via the internet protocol (e.g. ping).
ICS	Industrial Control System ICS is a superordinate term which describes the different types of controls systems in industrial systems.
IP	Internet Protocol "IP" is a network protocol on the level of the network layer of the OSI model.
IT Security	"IT Security" is the information security of the industrial automation according to VDI/VDE 2182.
MEP	Multi Ethernet Platform
OCI	Open Core Interface
OSI Model	Open Systems Interconnection Model The OSI model is a reference model for network protocols.
Ping	"Ping" is a diagnostic tool that queries a computer on a network using its IP address or the network name to determine whether there is a connection.
Port	The port is part of the network address to assign TCP and UDP connections between client and servers
RADIUS	Remote Authentication Dial-In User Service Client-server protocol to authenticate, authorize and account users in case of dial-in connections to a computer network.
Router	A "Router" is a network device to couple computer networks.
Switch	A "Switch" is a coupling element to connect network segments.

telnet	"Telnet" is a character-oriented client-server protocol via a TCP connection.
TCP	Transmission Control Protocol "TCP" is a connection-oriented network protocol on the level of the network layer of the OSI model.
UDP	User Datagram Protocol "UDP" is a minimal, connectionless network protocol on the level of the network layer of the OSI model.
Encryption	"Encryption" describes the conversion of plain text to non-readable text by using a secret key.
VPN	Virtual Private Network "VPN" is a closed network using a different network infrastructure and it is based on that structure.
Viruses	"Viruses" are malware that compromise functions and that are used to spy out data on a computer.
WLAN	Wireless Local Area Network "WLAN" is a wireless local network.
(Digital) certificate	A digital certificate confirms properties of persons or objects and their authenticity and integrity by cryptographic procedures.

2 Introduction

The topic "IT security" in production plants has previously been neglected. Controls and systems have been developed and operated according to functional aspects.

The topic "IT security" becomes increasingly more important due to the increased use of network components, their specific properties and requirements as well as the discrepancy to existing network structures and requirements in an office environment.

IT security is a precondition to ensure safe and smooth operation, in particular under the requirement scenarios of "Industry 4.0" and "Internet of Things", assuming a complete network of all objects involved.

The IT security requirements are divided into organizational and technical aspects.

As precondition for establishing and operating an IT-secure system, the network properties of the components used have to be known. The provision and the information and documentation exchange are part of the network properties that need to be known. Consequently, the manufacturer, the integrator and the operator can devise corresponding IT security concepts and solutions.

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

This approach is based on directive **VDI 2182**.

2.1 Purpose of this manual

The purpose of this manual is to provide the following information:

- Special information on the secure operation of Bosch Rexroth IT systems and devices
- General information about the "IT security" topic in manufacturing systems

By means of this information, the user can take network-technical and organizational measures and select special device settings to integrate the used products and to safely operate them.

2.1.1 Customer feedback

Customer requests, comments or suggestions for improvement are of great importance to us. Please email your feedback on the documentations to Feedback.Documentation@boschrexroth.de. Directly insert comments in the electronic PDF document and send the PDF file to Bosch Rexroth.

2.2 Manual structure

Initially, general IT security aspects are described, including a description regarding the differentiation to Safety.

The main part of this guideline contains a description of Bosch Rexroth devices and systems from an IT security point of view. The description contains a list and a description of the system properties as well as a list of the protocols and the ports used. Finally, the main part contains recommendations about the integration and the operation of these products in the network.

The last part consists of general information on the topic "IT security" and information on further reading and sources of information.

.

2.2.1 Differentiating "IT security" from "Safety"

In the following table, the differentiation IT Security vs. Safety is explained.

Comparing the terms "Safety" and "IT security"

Safety	IT security
Protection **of** humans and environment.	Protection **from** humans and environment.
Only **one** possible, calculable originator.	**Many** possible, partially incalculable originators
Threats: **Internally** to **Externally**.	Threats: **Externally** to **Internally**
Functional safety guarantees a smooth function free from threats	IT security ensures confidentiality, integrity and availability of information
Guidelines and binding laws	Guidelines incomplete, no laws

2.3 IT basic protection

The BSI (Federal Office for Information Security) regularly publishes reports about current threats and provides information on the IT basic protection. The basic IT protection components of the BSI in the IT basic protection compendium consist of ten layers and provide information on different information security topics - from applications (APP) to industrial IT (IND) and up to security management (ISMS).

VDI members can use it to obtain more information on the IT basic protection.

For notes, refer to the ICS-CERT sites under “Recommended Practices”.

chapter 6.2 "Related links" on page 29

2.4 Known vulnerabilities

Information about vulnerabilities that became known are published on Rexroth websites as well as on websites of the Bosch Product Security Incident Response Team(PSIRT). Bosch PSIRT is the central contact to replace safety-relevant information in Bosch products.

chapter 6.2 "Related links" on page 29

3 Security-relevant product description

In the following sections, the security-relevant aspects of Bosch Rexroth projects are described. Amongst others, the list of the ports, their use and particularities that have to be taken into consideration are described. This information facilitates the configuration and operation of the devices and systems by complying with the IT security aspects.

3.1 Overview Security support

Overview on security support of the devices and the software of the XLC, MLC and MTX systems

System and software	XLC, MLC and MTX				IndraDrive with and without MLD	Safe-Logic compact	Frequency converter	WebConnector	IoT Gateway	WinStudio
Device	CML10 CML20 CML40 CML25 CML45 CML65 CMP40 CMP60 CMP70 MTXmicro	CML75 CML85 XM2* VPx	VE* VP* VCP*.2 VEH**.1 VR21** MTXmicro	VP* VEP with Win7 emb. XM2* (as of 14V20)	Kxx02 KMVxx HMVxx HMS0x HMD01 HCS0x	SLC-3-CPUx SLC-3-GS3S SLC-0-GPNT	EFC	XM2*	XM2*	VE* VP* VCP*.2 VEH**.1 VR21**
Security support	No	As of FWA 14V18 and Indra Works 14V18	No	Yes	MPx20 V12 and above	No	No	Yes	Yes	No

3.2 MTX, XLC and MLC systems

MTX, XLC and MLC are VxWorks-based systems.

VxWorks is a real-time operating system used on IndraControl L, XM and VPx control systems.

For the devices IndraControl CML10, CML20, CML40, CML40.2, CML25, CML45, CML65, CMP40, CMP60, CMP70, MTXmicro with the operating system **VxWorks 6.3**, special conditions apply when commissioning and operating. Reasons for the special conditions with **VxWorks 6.3**:

- No IT security measures such as firewalls and antivirus software are implemented by the operating system.
- Due to the functions, IT security measures can sometimes neither be implemented nor installed.

- The network ports for FTP, Telnet and debugging are freely accessible in the basic settings.
- As additional network functionalities such as "Routing" und "NAT" are implemented on these devices, network security measures have to be taken to ensure safe operation of the devices.
- **VxWorks 6.3** provides only a limited user management

The real-time operating system **VxWorks 6.9** is used with the following characteristics for the devices CML75 , CML85, XM2* and VPx*:

- Due to compatibility reasons, the network port for FTP is open in the basic settings
- VxWorks 6.9 supports the implementation of further security mechanisms.
- As additional network functionalities such as "Routing" und "NAT" are implemented on these devices, network security measures have to be taken to ensure safe operation of the devices.

3.3 Device properties – Controls with VxWorks 6.3 operating system

Concerns the controls:

- CML10
- CML20
- CML25
- CML40
- CML40.2
- CML45
- CML65
- CMP40
- CMP60
- CMP70
- MTX micro

Debug access

In the basic setting, the debug port is open. The Wind River debug agent (WDB agent) is active.

Telnet server

The Telnet server is active (Telnet port is open).

The login name and the password are implemented into the runtime system. The password is encrypted (Wind River encryption "vxencrypt.exe").

FTP server

The FTP server is active. (FTP port is open).

The FTP server can be accessed with a "anonymous" user. The USER drive is read-only.

The login name and the password are integrated in the runtime system. The password is encrypted (Wind River encryption "vxencrypt.exe").

Further information

- An SNTP client application is available.
- A TFTP client application is available.
- The system does not have any local firewall.
- An ICMP functionality is implemented.
- Only a IPv4 stack is implemented.

Network infrastructure components

Functions required for the operation of the network infrastructure and the connection of different Ethernet-based bus systems, also field buses (Sercos, Profinet) and their data exchange, router and switch components are integrated into the operating system kernel. The functions are configured application-independently by means of the Engineering tools by the user.

Please note in particular the field buses that implicitly allow tunneling of standard IP protocols within a field bus protocol. Also refer to the field bus-specific documentation.

3.4 Device properties – Controls with VxWorks 6.9 operating system

Concerns the controls:

- CML75
- CML85
- XM2*
- XM4*
- VPx*

Debug access

In the basic setting, the debug port is closed. For OCI development purposes, the debugger can be enabled. After the development, disable the debugger.

Telnet server

The Telnet server is disabled (Telnet port is closed). The user can access the control via SSH instead.

SSH server

The command line previously provided by Telnet is now provided via SSH. The protocol "Telnet" is disabled due to security reasons and is not provided anymore as of 14V18 for the mentioned controls. The SSH server is active on the devices from the firmware release 14V18.

FTP server

The FTP server is active upon the control delivery. (FTP port is open). It is noted that the unsecure service can and should be disabled when creating a control.

The FTP server can be accessed with a "anonymous" user. The USER drive is read-only.

The login name and the password are integrated into the runtime system. The password is encrypted (Wind River encryption "vxencrypt.exe").

SFTP server

Secure File Transfer Protocol (SFTP) is used for safe data transfer. SFTP is part of the SSH- service and provides the same security mechanisms. Many known clients, such as WinSCP (Windows) or Filezilla (Windows, Linux, Mac OS) supports data transfer via SFTP. The SFTP server is active upon delivery.

Network infrastructure components

Functions required for the operation of the network infrastructure and the connection of different Ethernet-based bus systems, also field buses (Sercos, Profinet) and their data exchange, router and switch components are integrated in the operation system kernel. The user configures application-specifically using engineering tools.

Please note in particular the field buses that implicitly allow tunneling of standard IP protocols within a field bus protocol. Also refer to the field bus-specific documentation.

3.5 Drive system (IndraDrive with and without MLD)

IndraDrive uses a real-time system. Special conditions apply when commissioning and operating these devices. Reasons for the special conditions: No IT security measures such as firewalls and antivirus software are implemented by the operating system.

- Due to the functions, IT security measures can sometimes neither be implemented nor installed.
- The available ports are freely accessible in the basic settings.
- As additional network functionalities such as “routing” are implemented on these devices, network security measures have to be taken to ensure safe operation of the devices.
- IndraDrive does not provide any user management.

3.5.1 IndraDrive device properties

Telnet server

- The Telnet server is active (Telnet port is open).
- The login name and the password are integrated in the runtime system. The user can overwrite the password using a customer password.

FTP server

- The FTP server is active (FTP port is open).
- The FTP server can be accessed with an "anonymous" user and a default user.
- The USER drive is read-only for both users. The default user can write on the USER drive.
- The login names and the password are integrated in the runtime system. The user can overwrite the password for a default user using a customer password

Further information

- The system does not have any local firewall.
- There is a TFTP client application for IndraDrive Advanced devices.
- The ICMP functionality is implemented.
- Only a IPv4 stack is implemented.

Network infrastructure components

Functions required for the operation of the network infrastructure and the connection of different Ethernet-based bus systems, also field buses (Sercos, Profinet) and their data exchange, router and switch components are integrated into the operating system kernel. The functions are configured application-independently by means of the Engineering tools by the user.

Please note in particular the field buses that implicitly allow tunneling of standard IP protocols within a field bus protocol. Also refer to the field bus-specific documentation.

3.6 SafeLogic compact (SLc)

A SafeLogic compact station consists of one CPU module, optionally up to 2 Gateway modules (Sercos, PROFINET) as well as up to 12 extension modules (I/O modules, drive monitor). No IT security measures such as firewalls and antivirus software are implemented.

The Slc CPU is not equipped with any network-capable interfaces. Ethernet-based communication to Engineering PC or a higher-level control is realized via the SLC-3-GS3S Sercos gateway or via the SLC-0-GPNT PROFINET gateway.

- The available ports are freely accessible.

- As additional network functionalities such as “routing” are implemented on these devices, network security measures have to be taken to ensure safe operation of the devices.

3.6.1 SLc Ethernet Gateways device properties

Telnet server

The Telnet server is active (Telnet port is open)

FTP server

The FTP server is active (FTP port is open).

The FTP server can be accessed with a "anonymous" user.

Network infrastructure components

In particular, note the field buses that implicitly allow tunneling of standard IP protocols within a field bus protocol.

3.7 Device characteristics Sercans

Sercans is a Linux-based system. Ubuntu 4.4 is the Linux version used. The preempt-rt-patch was used to extend it to a real-time system. It is used in the Sercans variants L and S.

Debug access

The debug port is closed by default.

SSH server

A command line is provided via SSH. The SSH server is active.

SFTP server

Secure File Transfer Protocol (SFTP) is used for data transfer. The SFTP server is not active upon delivery and has to be enabled before updating the firmware. This is executed automatically if the firmware is updated using IndraWorks Ds.

3.8 Frequency converter EFC device properties

Devices with Multi Ethernet expansion card

Telnet server

No Telnet server available on the MultiEthernetPlatform

FTP server

No FTP server available on the MultiEthernetPlatform

TFTP server

The TFTP server is active (TPTP port is open)

The MultiEthernetPlatform only accepts certain file names, other files are rejected.

Further information

- The system does not have any local firewall.
- ICMP functionality is implemented
- Only an IPv4 stack is implemented.

Network infrastructure components

Functions required for the operation of the network infrastructure and the connection of different Ethernet-based bus systems, also field buses (Sercos, Profinet) and their data exchange, router and switch components are integrated into the operating system kernel. The functions are configured application-independently by means of the Engineering tools by the user.

Please note in particular the field buses that implicitly allow tunneling of standard IP protocols within a field bus protocol. Also refer to the field bus-specific documentation.

3.9 Port lists

All ports on which server services are provided, are shown in the following port lists. For the specific design upon delivery on the different devices and systems, refer to the following tables.

In the columns "Required for...", "Operation", "Commissioning" and "Service", it is specified in which phase the ports for the respective functions are required.

In the column "Can be disabled", it is specified if the port can be disabled by the end user within the framework of the application configuration.

Port list CML25, CML45, CML65

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
21	TCP	ftp	open	-	Y	Y	Y	N
23	TCP	telnet	open	-	N	N	Y	N
80	TCP	http	open	-	Y	Y	Y	N
1740	UDP	Gateway	open| filtered	-	Y	Y	Y	N

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
1741	UDP	Gateway	open|filtered	-	Y	Y	Y	N
4840	TCP	OPC-UA	open	-	Y	Y	Y	N
5003	TCP	SIS	open	-	Y	Y	Y	N
5300	TCP	MLPI	open	-	Y	Y	Y	N
6040	UDP	Com server (HMI)	open|filtered	-	Y	Y	Y	N
6042	TCP	Com server (HMI)	open	-	Y	Y	Y	N
11001	UDP	ILNG.Online	open|filtered	-				
11740	TCP	IndraLogic Gateway	open	-	Y	Y	Y	N
17185	UDP	Wind River Debug port	open|filtered	-	N	N	N	N

Port list CML75, XM2*, VPx*

incl. the firmware 14V16

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
21	TCP	ftp	open	-	Y	Y	Y	N
23	TCP	telnet	open	-	N	N	Y	N
80	TCP	http	open	-	Y	Y	Y	N
111	TCP, UDP	Port mapper	open	-	Y	Y	Y	N
443	TCP	https	open	Not CML75	-	-	-	-
972	UDP	-	open|filtered	Only VPx*	-	-	-	-
974	UDP	-	open|filtered	Only VPx*	-	-	-	-
980	UDP	-	open|filtered	Only VPx*	-	-	-	-

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Opera-tion	Commis-sioning	Service	
982	UDP	-	open|filtered	Only VPx*	-	-	-	-
984	UDP	-	open|filtered	Only VPx*	-	-	-	-
985	UDP	-	open|filtered	Only VPx*	-	-	-	-
988	UDP	-	open|filtered	Only VPx*	-	-	-	-
990	UDP	-	open|filtered	Only VPx*	-	-	-	-
994	UDP	-	open|filtered	Only VPx*	-	-	-	-
996	UDP	-	open|filtered	Only VPx*	-	-	-	-
1000	UDP	-	open|filtered	Only VPx*	-	-	-	-
1004	UDP	-	open|filtered	Only VPx*	-	-	-	-
1740	UDP	Gateway	open|filtered	-	Y	Y	Y	N
1741	UDP	Gateway	open|filtered	-	Y	Y	Y	N
1742	UDP	Gateway	open|filtered	Only VPx*	Y	Y	Y	N
4840	TCP	OPC-UA	open	-	Y	Y	Y	N
5003	TCP	SIS	open	-	Y	Y	Y	N
5300	TCP	mlpi	open	-	Y	Y	Y	N
6040	UDP	Com server (HMI)	open|filtered	Not XM2*	Y	Y	Y	N
6042	TCP	Com server (HMI)	open	-	Y	Y	Y	N
8080	TCP	Redirection to https	open	Not CML75	-	-	-	-
11001	UDP	ILNG.Online	open|filtered	-	-	-	-	-

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
11740	TCP	IndraLogic Gateway	open	-	Y	Y	Y	N
17185	UDP	Wind River Debug port	open| filtered	-	N	N	N	N

Port list CML75, XM2*, VPx*

from firmware 14V18

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
21	TCP	ftp	open	-	N	N	N	Y
22	TCP	ssh, sftp	open	-	Y	Y	Y	Y
80	TCP	http	open	-	-	-	-	-
111	TCP, UDP	Port mapper	open	-	Y	Y	Y	N
443	TCP	https	open	Not CML75	-	-	-	-
974	UDP	-	open| filtered	Only VPx*	-	-	-	-
976	UDP	-	open| filtered	Only VPx*	-	-	-	-
978	UDP	-	open| filtered	Only VPx*	-	-	-	-
982	UDP	-	open| filtered	Only VPx*	-	-	-	-
984	UDP	-	open| filtered	Only VPx*	-	-	-	-
986	UDP	-	open| filtered	Only VPx*	-	-	-	-
990	UDP	-	open| filtered	Only VPx*	-	-	-	-
994	UDP	-	open| filtered	Only VPx*	-	-	-	-

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
996	UDP	-	open|filtered	Only VPx*	-	-	-	-
998	UDP	-	open|filtered	Only VPx*	-	-	-	-
1000	UDP	-	open|filtered	Only VPx*	-	-	-	-
1004	UDP	-	open|filtered	Only VPx*	-	-	-	-
1740	UDP	Gateway	open|filtered	-	Y	Y	Y	N
1741	UDP	Gateway	open|filtered	-	Y	Y	Y	N
1742	UDP	Gateway	open|filtered	Only VPx*	Y	Y	Y	N
4840	TCP	OPC-UA	open	-	Y	Y	Y	N
5003	TCP	SIS	open	-	Y	Y	Y	N
5300	TCP	MLPI	open	-	Y	Y	Y	N
5335	TCP	MLPIS	open	-				
6040	UDP	Com server (HMI)	open|filtered	-	Y	Y	Y	N
6042	TCP	Com server (HMI)	open	-	Y	Y	Y	N
8080	TCP	Redirection to https	open	Not CML75	-	-	-	-
11001	UDP	ILNG.Online	open|filtered	-	-	-	-	-
11740	TCP	IndraLogic Gateway	open	-	Y	Y	Y	N
17185	UDP	Wind River Debug port	open|filtered	-	N	N	N	Y

IndraDrive port list

(with/without MLD)

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
20 / 21	TCP	ftp	open	Access opt. SD	Y	Y	Y	Y*
23	TCP	telnet	open		N	N	Y	Y*
69	UDP	TFTP	open	FW update	Y	Y	Y	Y*
80	TCP	WebServer(http)	open	IDST	Y	Y	Y	Y*
1200	TCP	CoDeSys Kommunikation	open		-	-	-	-
1202	UDP	Network variables	open	Available in the firmware versions from MPx02 to MPx17	-	-	-	-
1740 - 1743	UDP	MLD Broadcast	open		Y	Y	Y	N
5002	TCP	SIS server	open		Y	Y	Y	Y*
6040	UDP	ComServer (HMI)	open		Y	Y	Y	Y*
6042	TCP	ComServer (HMI)	open		Y	Y	Y	Y*
11740 - 11743	TCP	MLD connections	open		Y	Y	Y	N
35021	TCP	S/IP	open		Y	Y	Y	N
35021	UDP	S/IP	open		Y	Y	Y	N
51000	TCP	Trace (MEP)	open		N	N	Y	N
51001	TCP	TCP console (MEP)	open		N	N	Y	N

Tab. 3-1: * The ports can only be disabled in MPx-20V12 or above using the parameter P-0-1535 (settings IP communication).

Sercos port list

Gateway SLC-3-GS3S

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
23	TCP	telnet	open	-	-	-	-	-
69	UDP	tftp	open|filtered	-	-	-	-	-
3908	UDP	-	open|filtered		-	-	-	-
5002	TCP	SIS	open	-	-	-	-	-
9000	TCP	SafeLogic Designer communication	open	-	-	-	-	-
30718	UDP	Safe Logic Designer scan service	open|filtered	-	-	-	-	-
35021	TCP	S/IP	open	-	-	-	-	-
35021	UDP	S/IP	open|filtered	-	-	-	-	-
48232	UDP	-	open|filtered	-	-	-	-	-

PROFINET port list

Gateway SLC-0-GPNT

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
23	TCP	telnet	open	-	-	-	-	-
80	TCP	http	open	-	-	-	-	-
161	UDP	SNMP	open|filtered		-	-	-	-
1024	UDP		open|filtered	-	-	-	-	-
4606	TCP		open	-	-	-	-	-

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
4607	TCP		open	-	-	-	-	-
8160	UDP		open|filtered	-	-	-	-	-
8161	UDP		open|filtered	-	-	-	-	-
9000	TCP	SafeLogic Designer communication	open	-	-	-	-	-
9011	UDP		open|filtered	-	-	-	-	-
9100	TCP		open	-	-	-	-	-
30718	UDP	SafeLogic Designer scan service	open|filtered	-	-	-	-	-
34962	UDP		open|filtered	-	-	-	-	-
34964	UDP		open|filtered	-	-	-	-	-

Sercans port list

Port	Protocol	Service	Status	Note	Required for... [Y/N]			Can be disabled [Y/N]
					Operation	Commissioning	Service	
22	TCP	SSH	open	-	-	-	-	-
22	TCP	SFTP	open	If server active	-	-	-	Y
35021	TCP, UDP	S/IP	open		Y	Y	Y	Y

Frequency converter port list

EFC with Multi Ethernet Platform(MEP)

Port	Protocol	Service	Status	Note	Required for... [Y/N]	Commissioning	Service	Can be disabled [Y/N]
69	UDP	tftp	open	MEP firmware update	Y	Y	Y	N
502	TCP	Modbus/TCP	open*		Y*	Y*	N	N
x	TCP	Modbus/TCP	closed	User definable port number (H3.51)	Y*	Y*	N	Y
2222	UDP	EtherNet/IP	open*	EtherNet/IP Implicit Mes-saging	Y*	Y*	N	N
34964	UDP	PROFINET	open*	PROFINET Connect Manager and RPC handler	Y*	Y*	N	N
35021	TCP	Sercos/IP	open	Engineering	Y	Y	Y	N
35021	UDP	Sercos/IP	open	Engineering	Y	Y	Y	N
44818	TCP	EtherNet/IP	open*	EtherNet/IP Explicit Mes-saging	Y*	Y*	Y	N
51000	TCP	Trace (MEP)	open		N	N	Y	N
50001	TCP	TCP console (MEP)	open		N	N	Y	N

Tab. 3-2: * = only if the respective field bus type of the MultiEthernetPlatform has been enabled

3.10 IndraControl VP*, VE*, VEP*, VCH*, VR21* devices

- The Windows-based systems (XP, XPembedded, Windows 7, Windows 10, CE) are configured and delivered with a preset firewall, services and applications.
- An antivirus software is not installed.

  Rexroth does not test the compatibility and does not recommend any antivirus software!

Influences on the runtime behavior and the operation of the software components can thus only be determined through test in individual cases. Any resulting measures are the responsibility of the end user.

- A patch management of the operation system is not provided. The current operation system version contains the patch version of the manufacturer (Microsoft) at the time of the release. This status is checked for correct functionality and is released using the respective system software.
- No BIOS passwords are set on the devices.
- For the users created upon delivery and the device passwords, refer to the respective product documentation.

Immediately change the default passwords after commissioning.

- For users and passwords created by Telnet and FTP irrespective of the operating system, refer to chapter "Communication settings" in the device documentation.

Refer to the relevant system documentation for any changes to be implemented.

3.10.1 Devices (IndraControl VP*) with Windows XP, Windows 7, Windows 10

The aim of the configuration of these operating systems for their use in an industrial environment should be to only use the relevant applications, services and communication accesses. This configuration increases the overall system stability and minimizes the number of potential targets. In the following, the Windows tools used for the configuration are described.

The following security-relevant settings can be selected by configuring the "Local Policies": **Control Panel ▶ Administrative Tools ▶ Local Policies**.

- Managing the access rights to directories, files and functions
- Configuring the password properties
- Configuring the software restrictions (white listing)

Further measures:

- Preventing the automatic execution of applications on removable data carriers (USB flash drive, CD, DVD), see:

  http://support.microsoft.com/kb/967715
- Using the "Enhanced-Write-Filter" (XP and 7), see

  http://technet.microsoft.com/en-us/library/bb932158.aspx

  For more filter and setting options, refer to

  http://msdn.microsoft.com/en-us/library/ff794908%28v=winembedded.60%29.aspx.
- Configuring the Windows firewall

  Windows 7, see

http://windows.microsoft.com/en-us/windows7/understanding-windows-firewall-settings

Windows XP, see

http://technet.microsoft.com/en-us/library/cc875811.aspx

- Windows Security, general

  https://technet.microsoft.com/en-us/security

Always install the current Windows security updates on your devices.

Crypto trojans and ransomware use different loopholes in the operating system and in the software. The internet sites of the BSI and the ICS-CERT regularly provide information on leaks as well as possible actions to ensure that no one takes advantages of these leaks. chapter 6.2 "Related links" on page 29

Disconnect the devices from the network until the updates closing the security leaks are installed.

3.10.2 Standard Windows ports

For information on the current Microsoft Windows standard port, refer to the following link:

https://support.microsoft.com/en-us/kb/832017

In the subsequent sections, the active ports of the respective devices are listed in the different operating system variants upon delivery.

Unless otherwise specified in the system software documentation, no changes of the default firewall settings are implemented.

During the operation, the active ports and applications can be identified with administrator rights and the following commands:

`netstat -an -p tcp -b` or `netstat -an -p udp -b`

3.10.3 Devices (IndraControl VE*) with Windows 7 Embedded Standard 32 and 64 bit

Port	Protocol	Application
81	TCP	portico (if installed)
515	TCP	LPDSVC [svchost.exe]
1234	TCP	Studio Manager, if activated
2103	TCP	[mqsvc.exe]
2105	TCP	[mqsvc.exe]
2107	TCP	[mqsvc.exe]
5900	TCP	portico or UltraVNC (if installed)
6002	TCP	portico (if installed)

Port	Protocol	Application
8085	HTTP	WebConnector console (if installed)
8086	HTTP, TLS	WebConnector console (if installed)
15000	HTTP	WebConnector service (if installed)
15001	HTTPS, TLS	WebConnector service (if installed)
49155	TCP	[lsass.exe]

3.10.4 Devices (IndraControl VP*) with Windows 7 Ultimate 32 and 64 bit

Port	Protocol	Application
9876	TCP, UDP	Acronis

3.10.5 Devices (IndraControl VP*) with Windows 10 IoT Enterprise LTSB 64 bit

Port	Protocol	Application
9876	TCP, UDP	Acronis

3.10.6 Devices (IndraControl VP*) with Windows 7 Embedded Standard 32 and 64 bit

Port	Protocol	Application
81	TCP	portico (if installed)
515	TCP	LPDSVC [svchost.exe]
2103	TCP	[mqsvc.exe]
2105	TCP	[mqsvc.exe]
2107	TCP	[mqsvc.exe]
5900	TCP	portico or UltraVNC (if installed)
6002	TCP	portico (if installed)
8085	HTTP	WebConnector console (if installed)
8086	HTTPS, TLS	WebConnector console (if installed)
9876	TCP, UDP	Acronis [agent.exe] (if installed)
15000	HTTP	WebConnector service (if installed)
15001	HTTPS, TLS	WebConnector service (if installed)
49155	TCP	[lsass.exe]

3.10.7 Devices (IndraControl VP*) with Windows XP 32 bit

Port	Protocol	Application
123	UDP	[svchost.exe]
135	TCP	[svchost.exe]
137	UDP	[System]
138	UDP	[System]
139	TCP	[System]
445	TCP, UDP	[System]
500	UDP	[lsass.exe]
1028	TCP	[alg.exe]
1900	UDP	[svchost.exe]
4500	UDP	[lsass.exe]
9876	TCP, UDP	Acronis[agent.exe]

3.10.8 Devices (IndraControl VR21*) with Windows Embedded compact 7

Port	Protocol	Application
123	UDP	ntp
137	UDP	netbios-ns
138	UDP	netbios-dgm
4322	TCP	
4500	UDP	nat-t-ike

3.10.9 Devices (IndraControl VH21) with Windows Embedded compact 7

Port	Protocol	Application
137	UDP	netbios-ns
138	UDP	netbios-dgm
139	TCP	NetBIOS Session Service
445	TCP	SMB release (Windows share)
4322	TCP	-
4500	UDP	nat-t-ike
6089	UDP	-
49152	UDP	ComServer, EIS

3.10.10 Devices (IndraControl VE*) with Windows XP embedded 32 bit

Port	Protocol	Application
123	UDP	[svchost.exe]
135	TCP	[svchost.exe]
137	UDP	[System]
138	UDP	[System]
139	TCP	[System]
161	UDP	[snmp.exe]
445	TCP, UDP	[System]
500	UDP	[lsass.exe]
1025	TCP	[inetinfo.exe]
1026	UDP	[svchost.exe]
1027	UDP	[mqsvc.exe]
1028	TCP	[mqsvc.exe]
1029	TCP	[alg.exe]
1801	TCP	[mqsvc.exe]
2103	TCP	[mqsvc.exe]
2105	TCP	[mqsvc.exe]
2107	TCP	[mqsvc.exe]
3389	TCP	[svchost.exe]
3456	UDP	[inetinfo.exe]
3527	UDP	[mqsvc.exe]
4500	UDP	[lsass.exe]

3.10.11 Devices (IndraControl VE*) with Windows Embedded compact 7

Port	Protocol	Service
80	TCP	HTTP
443	TCP	HTTPS
5120	TCP	UPnP

3.10.12 Devices (IndraControl VE*) with Windows CE

Port	Protocol	Application
20, 21	TCP	ftp
23	TCP	telnet
80	TCP	Web server
137	UDP	NTP

Port	Protocol	Application
138	UDP	NetBIOS
443	TCP	HTTP SSL
5120	TCP	UPnP

3.10.13 Devices (IndraControl VCP*.2) with Windows CE 5.0

Port	Protocol	Application
20, 21	TCP	ftp
80	TCP	Web server
137	UDP	NTP
138	UDP	NetBIOS
443	TCP	HTTP SSL
1025	TCP	ESTAB (ComServer)

3.10.14 Devices (IndraControl Control VCH 08.1) with Windows CE 5.0

Port	Protocol	Application
20, 21	TCP	ftp
80	TCP	Web server
135	TCP	DCOM
137	UDP	NTP
138	UDP	NetBIOS
139	TCP	NetBIOS
161	UDP	-
443	TCP	HTTP SSL
445	TCP	SMB
1025	TCP	ComServer
1026	UDP	ComServer key transmission
1050-1053	TCP	ComServer

3.10.15 Devices (IndraControl Control VCH 05.1) with Windows CE 6.0

Port	Protocol	Application
80	TCP	Web server
137	UDP	NTP
138	UDP	NetBIOS
443	TCP	HTTP SSL
49152	UDP	ComServer key transmission

3.11 Software

3.11.1 WebConnector, WebComposer

Visualizations on all devices with an executable Yava VM can be connected to controls using the WebConnector. The protocols OPC UA and OCI (MLPI) are supported. The user has to configure the secure communication via OPC UA. The secure communication via MLPIS is only supported as of 14V20 and has to be configured by the user at Connect .

To provide customized HTML5 sites with a direct access on the automation level, the WebConnector has an integrated web server. Secure data communication is optionally via HTTPS and TLS encryption.

The WebConnector is available on the devices P*. and VE* with Windows 7 embedded. In the default setting, the unencrypted communication (HTTP/WS) is active as console via the port 8085 and the Windows service via the port 15000 and the encrypted communication (HTTPS/TLS) is active as console via the port 8086 and the Windows service via the port 15001. The user has to disable the unencrypted communication.

In IndraWorks, the Engineering tool is available for commissioning visualizations of the WebComposer. If WebComposer objects are created in the project, the WebConnector service is started and the ports 15000(HTTP/WS) and 15001(HTTPS/TLS) are active. The WebConnector service is not exited by closing IndraWorks. The service stops only running after the computer has been restarted (starting method: manual). If the WebConnector service is not required anymore after closing the IndraWorks project or exiting IndraWorks or the WebComposer application, start "services.msc" and stop the boschrexroth.webconnector service. Use a firewall to ensure that accessing the WebConnector ports from outside is not possible if allowed by the application.

Port list

Port	Protocol	Application	Device
8085	HTTP	WebConnector console (if installed)	VP* with Win7emb., VE* with Win7emb.
8086	HTTPS, TLS	WebConnector console (if installed)	VP* with Win7emb., VE* with Win7emb.
15000	HTTP	WebConnector service (if installed)	VP* with Win7emb., VE* with Win7emb.
15001	HTTPS, TLS	WebConnector service (if installed)	VP* with Win7emb., VE* with Win7emb.

Tab. 3-3: WebConnector port list

3.11.2 WinStudio

WinStudio is a visualization software for all PC-based and embedded systems. The product consists of two parts.

WinStudio Engineering

Configuration tool to create individual HMI screens up to complete user interfaces.

WinStudio Engineering package characteristics

- Integral part in IndraWorks Engineering to create visualization applications.
- Stand-alone editor to create individual visualizations (WinStudio Engineering stand-alone).

WinStudio Runtime:

Software on visualization devices is pre-installed or prepared for installation (software download).

WinStudio runtime environment characteristics

- WinStudio in IndraWorks HMI interface (IndraWorks OPD). (Ready user interface of the systems MLC, MTX and IL under Windows CE/Windows 7 embedded compact, Win XP/ Win XPe, Win 7/ Win 7e)
- WinStudio Runtime (IndraWorks independent of User Interface).

Port list

Port	Protocol	Application
1234	TCP	Studio manager
3997	TCP	Studio Database Gateway (StADOSvr.exe)
4322	TCP	Remote agent (CEServer.exe)
4448	TCP	Mobile Access Runtime (MobileAccessTask.exe)
51234	TCP	InduSoft Web Studio project runtime server . Encrypted with TLS 1.2

Tab. 3-4: Port list WinStudio

4 Possible measures

4.1 System decoupling concept

According to state-of-the-art, control and system networks decoupled from other systems within an industrial network infrastructure are recommended. Different protection requirements can be taken into consideration by a decoupled system. In case of larger units, decoupling within the control and system networks is recommended. By decoupling larger units, malware can only spread within smaller areas. Consequently, all invisible devices are located in the control and system network. Devices and systems without patch management and access control mechanisms are considered "unsafe".

Control and system networks only have limited or no communication possibilities in other networks and can thus not access or respond beyond the limited network. Communication with the internet should not be possible. Assign fixed IP addresses to the devices and avoid using DHCP services.

Our devices and systems are not intended for use in control and system networks, unless not specified otherwise. Use additional safety measures in case of deviating conditions of use.

These rules apply when establishing subnetworks with WLAN technology. When using WLAN technology, provide and document WLAN-specific security properties and resulting measures. Keywords in this context:

- Device visibility
- Encryption of the transmission path according to state-of-the-art with appropriate key length
- Key management
- User and administrator management

4.2 External or third-party service measures

If external service measures are required, it has to be ensured that mechanisms such as VPN are realized to facilitate access. The same applies to the assignment of user rights and the access of the service providers to controls and system parts.

4.3 Using firewalls

The use of firewalls is recommended at all network transitions to limit the used protocols to the essential information.

4.4 Using ACLs

Control of access rights to systems and system parts should always be regulated by ACLs. Unintentional access to systems or system parts decoupled into smaller network units can thus be avoided by using ACLs.

4.5 Using innominate mGuard VPN components

For the scenarios previously described, Bosch Rexroth provides devices and templates for a secure access and firewall functions.

- RS4000
- mGuard Delta²
- •mGuard Smart²

5 Concluding remark

Security is an ongoing process.

The process requires continuous monitoring by all parties involved, also by seemingly less affected parties.

All persons involved required a profound knowledge of IT security.

This awareness is a basic principle to detect and prevent potential IT security vulnerabilities and deficiencies.

5.1 Recommendations

- Minimize the visibility of the devices and the systems in the network
- Devices and systems should never have direct internet access
- Install a firewall to protect devices, systems and networks and disconnect the devices, systems and networks from the office network
- If remote maintenance is required, use approved, secure methods such as VPN. Take into account that the level of security depends on the level of security of the device as well as on the user settings.
- Remove or disable all known default accesses and user accounts or rename them
- If possible, use available account lockout policies to minimize the risk of brute force attacks
- Implement rules to force the user to enter strong passwords
- Monitor and protocol the access creation on an administrative level by third parties
- If possible, disable all hardware interfaces that are not required
- Provide adequate measures and rules to guarantee quick recommissioning after an incident

6 Sources

6.1 Bibliography

- STANDARD VDI/VDE 2182
- STANDARD ISO/IEC 27000
- STANDARD BS/IEC 62443
- VDI guideline: "10 FAQs about IT security in the industrial automation"
- Industrial Network Security; Eric D. Knapp; ISBN-10: 1597496456

6.2 Related links

- Bosch Product Security Incident Response Team(PSIRT)

  https://psirt.bosch.com/
- Rexroth security information

  https://www.boschrexroth.com/en/xc/products/product-support/security-information/security-information
- German Federal Office for Information Security:

  https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

- The Association of German Engineers, department 5:"Industrial Information Technology", department "Security":

  http://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/fachbereiche/industrielle-informationstechnik/gma-fa-522-security/ (German)

  http://www.vdi.eu/

- The Bürger-CERT (CERT = Computer Emergency Response Team) is a project of the German Federal Office for Information Security (BSI) which issues warnings about viruses, worms and other security vulnerabilities for citizens and smaller enterprises:

  https://www.buerger-cert.de (German)

- ICS-CERT warns about security vulnerabilities in IT systems:

  http://ics-cert.us-cert.gov

  https://ics-cert.us-cert.gov/Introduction-Recommended-Practices

Index

F

G

I

L

M

P

R

S

T

V

W

Notes

rexroth
A Bosch Company

Bosch Rexroth AG
Electric Drives and Controls
P.O. Box 13 57
97803 Lohr, Germany
Bgm.-Dr.-Nebel-Str. 2
97816 Lohr, Germany
Phone +49 9352 18 0
Fax +49 9352 18 8400
www.boschrexroth.com/electrics

R911342562

DOK-IWORKS-SECURITY***-PR06-EN-P