Cybersecurity

Bereit für die Sicherheitsanforderungen von morgen!

Hans Michael Krause, Bosch Rexroth AG
30. September 2025

ctrlX AUTOMATION | rexroth A Bosch Company

This is Bosch Rexroth
Bosch Group: Figures 2024

Bosch Group in total:

90.5 bn
turnover

417,900
employees

280
manufacturing plants

Mobility Solutions

- One of the largest suppliers of mobility solutions worldwide

Industrial Technology

- **One of the leading suppliers of industrial automation**
- Bosch Connected Industry

rexroth
A Bosch Company

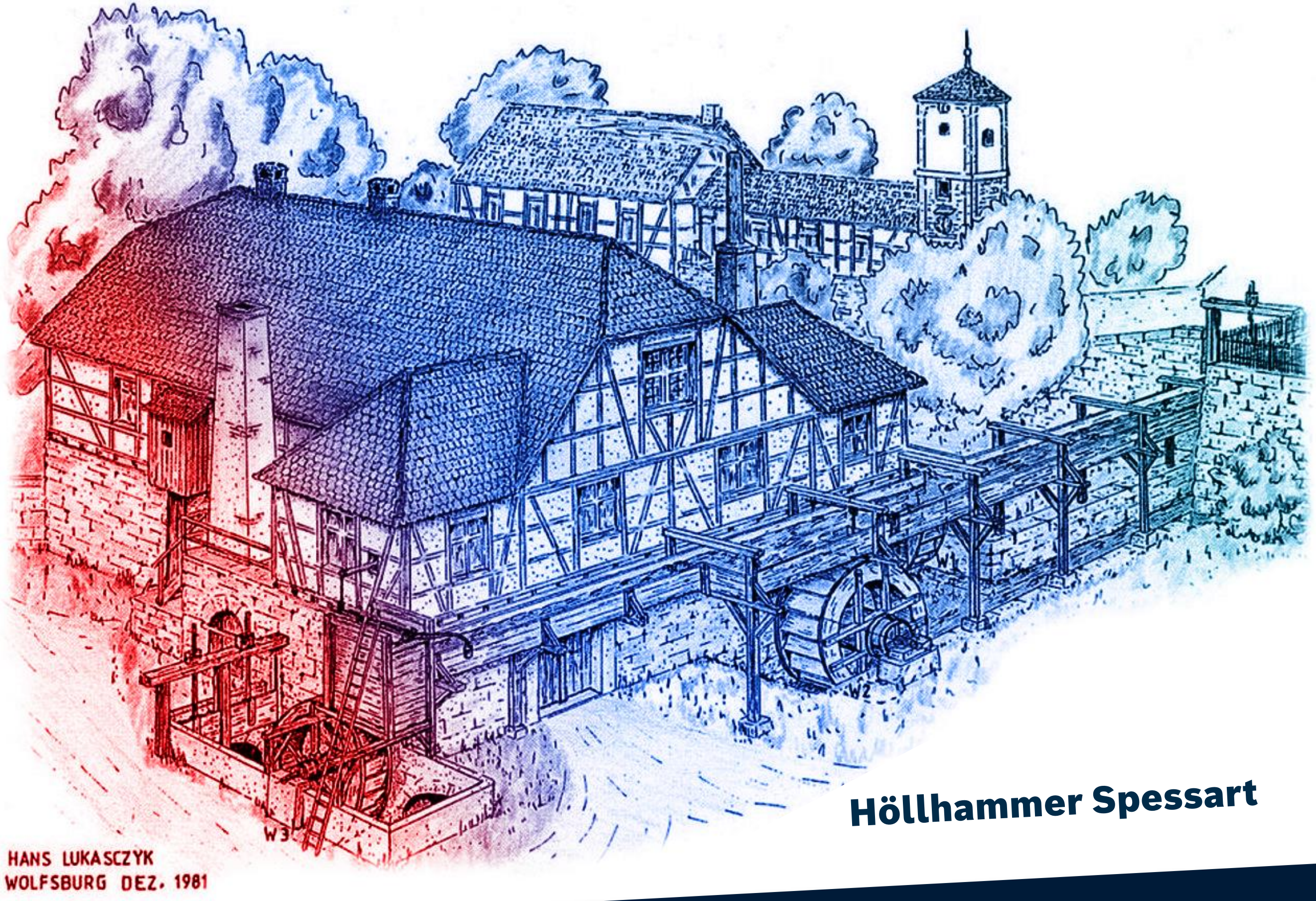
Energy & Building Technology

- One of the leading manufacturers of safety and communications
- Leading supplier of heating products and hot water solutions

Consumer Goods

- Leading supplier of power tools and corresponding accessories
- Premier vendor of household appliances

This is Bosch Rexroth Founded in 1795



Höllhammer Spessart

Georg Ludwig Rexroth

SEIT 1795

We already shaped Industry 1.0

rexroth
A Bosch Company

This is Bosch Rexroth Today

Status 2024

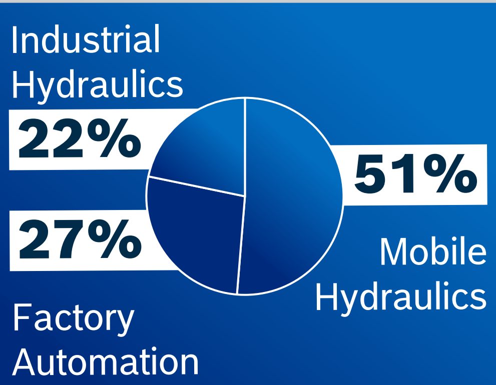
32,600
People associates

33,000
Active **customers**

€ 6.5 @2024
billion

€ 456
million in R&D
7% of sales

1.3 Mio
saleable **products**



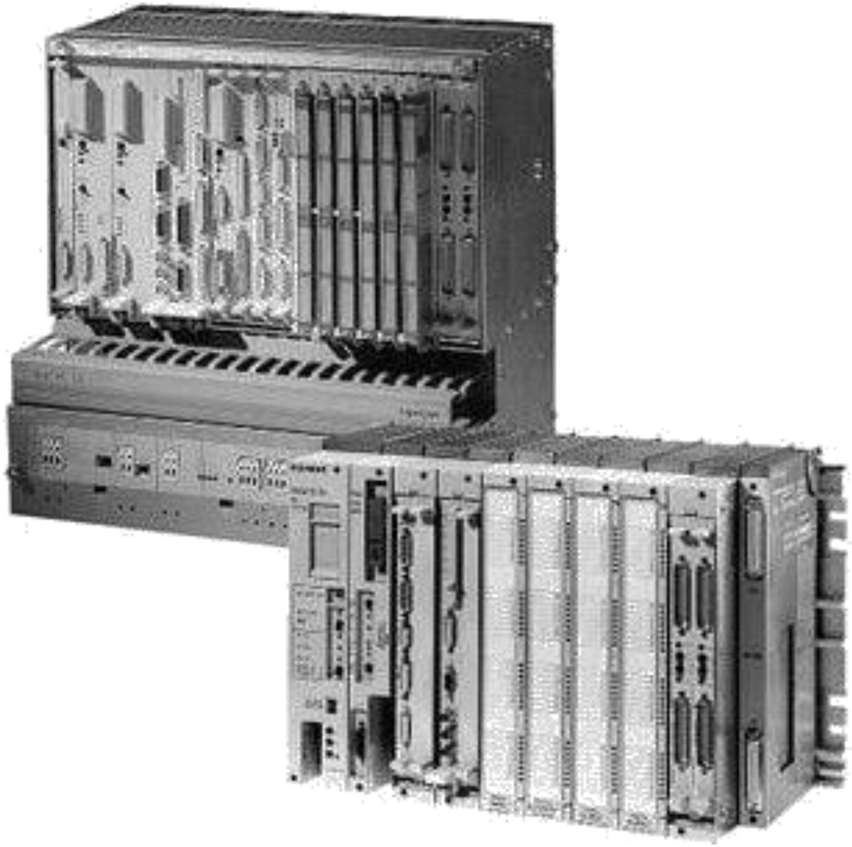
49

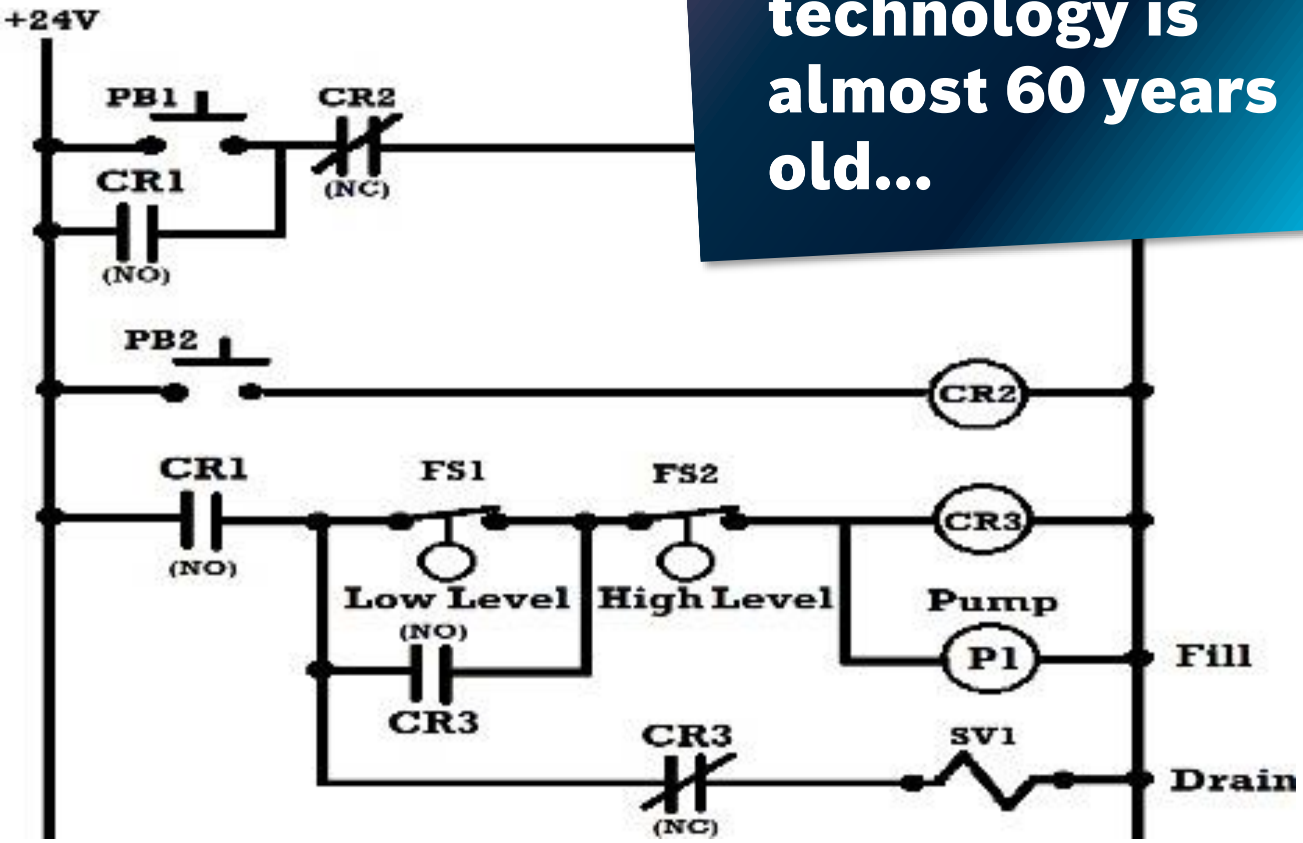
Manufacturing locations and customization sites in 22 countries

80

Countries
Sales and service network throughout

Today’s automation technology





Current PLC technology is almost 60 years old…

Today’s automation technology

Todays Industrial Automation Technology is mostly **CLOSED**, **COMPLEX** and not **SECURE**.

🔒 Closed Systems

Everybody talks about openness, but no-one is really open regarding tools, standards, interfaces and ecosystems. There is no user journey without a **LOCK-IN**.

🚫 Complexity & Effort

Systems are complex, inflexible and rely on tightly **coupled hardware and software**, making scaling or changes time-consuming and costly. Engineering requires major effort – and developers often struggle with **proprietary tools** and environments.

⚠ IT-Security Risks

Today’s control systems often rely on **outdated operating systems, lack update capabilities,** and **cannot be accessed remotely secure** – making it almost impossible to meet future standards and legal requirements.

Cybersecurity Threat Situation

76% of organizations had 1+ intrusions in the past year

31% had 6+

↑ **73%** of intrusions impacted OT systems[1]

[1] 61% in 2022

55% experienced operational outages reducing productivity

2024, FORTINET – State of Operational Technology and Cybersecurity Report

Average amount of damage

↑ **$ 4.88 million**[2]

[2] 2.8 million in 2022

Average recovery time after a cyberattack

7.34 months

2024, IBM – Cost of a Data Breach Report   2024, Fastly – Cybersecurity at the Crossroads

Cybersecurity
Laws & Regulations

EU Machinery Regulation 2023/1230

Cybersecurity and safety requirements for machinery and connected equipment

Adopted in 2023
Mandatory from 2027

EU Cyber Resilience Act (CRA)

Protection against vulnerabilities in connected devices

Adopted in 2024
Mandatory from 12/2027

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, USA)

Mandatory cyber incident reporting for critical infrastructure operators

Adopted in 2022
Mandatory from: expected 2026

Radio Equipment Directive (RED)

Cybersecurity requirements for wireless devices

Adopted in 2014
Additional requirements adopted in 2022
Mandatory from 1 August 2025

EU NIS-2 Directive (2022/2555)

Enhanced cybersecurity requirements for essential & important entities

Adopted in 2023
Mandatory from 2024

Cybersecurity Law of the People´s Republic of China

Comprehensive framework for network operations and data protection

Adopted in 2016
Mandatory from 2017

Cyber Resilience Act

Cyber Resilience Act
Preamble

The Cyber Resilience Act (CRA) has been published in 12/2024. Although the regulation provides a comprehensive set of requirements on a product and process level, many details of those requirements are yet unclear. Currently, no standards have been defined and no notified bodies have been named.

Therefore, all statements on the following slides represent our interpretation based on a thorough analysis of the requirements.

PLEASE TAKE THOSE STATEMENTS WITH A GRAIN OF SALT!

Everything that

COMMUNICATES DIGITALLY

will be covered by the

CYBER RESILIENCE ACT (CRA)

Cyber Resilience Act Requirements & Obligations

Design & Engineering

PRODUCT CYBERSECURITY REQUIREMENTS

Products must be developed, designed and produced in a way so that an appropriate level of cybersecurity based on the risks that are assessed for the products is ensured.

Product Lifecycle

VULNERABILITY HANDLING REQUIREMENTS

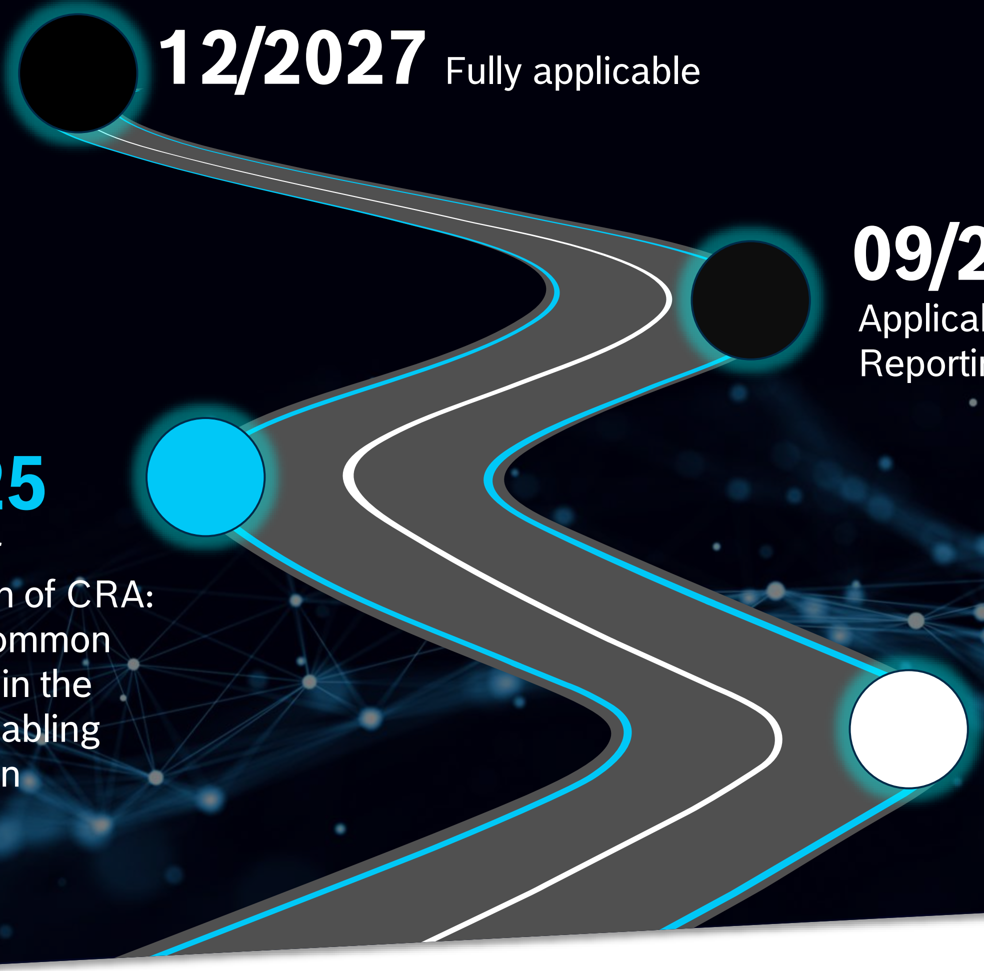
Manufacturers of the products with digital elements shall identify and document vulnerabilities and components contained in the product, address and remediate vulnerabilities without delay

MANUFACTURER OBLIGATIONS

Manufacturers must ***notify about actively exploited vulnerabilities*** *& any severe incident within a very short time interval (****24h for early warning****)*

Source: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130-FNL-COR01_DE.pdf

Cybersecurity
Cyber Resilience Act



12/2027 Fully applicable

09/2026
Applicability of Article 14:
Reporting obligations

Q4/2025
Description for implementation of CRA: Definition of common standards within the community, enabling self-certification

12/2024
Publication CRA

Shift from **VOLUNTARY BEST PRACTICES** to legally binding **OBLIGATIONS**

Cyber Resilience Act
Demands from end users

- End customers increasingly demand connected and intelligent machines with corresponding digital products and platforms
- At the same time, awareness of cybersecurity risks is growing, along with the desire for transparency and control over all system components
- “New” regulatory frameworks (CRA, NIS, ...) also pose a challenge for end customers
- Digital products and services require secure and reliable solutions

Cyber Resilience Act
IT requirements for machine builders

Typical IT requirements that machine builders face today from machine operators

- Network structuring/segmentation
- Firewall + Secure VPN solutions
- Network transparency down to the bus level
- Update management
- Security certifications + threat analyses
- Prohibition of USB hardware or personal engineering PCs
- Integration into threat detection systems

+ all OT requirements that are normal for machine builders ;-)

Cyber Resilience Act
What do you need to do?

The **Cyber Resilience Act** introduces **far-reaching challenges** for component suppliers and machine manufacturers.

Making existing platforms ready for the CRA often requires **massive effort** and **might not be feasible** at all in some cases.

Checklist

- ✓ What are the functions of your product?
- ✓ What is the expected service life of your product?
- ✓ What is the expected installation environment at the customer's site?
- ✓ What is the expected usage at the customer's site?
- ✓ Does the machine have security-relevant features?
- ✓ Are predictable applications possible?
- ✓ How do you deal with security vulnerabilities?

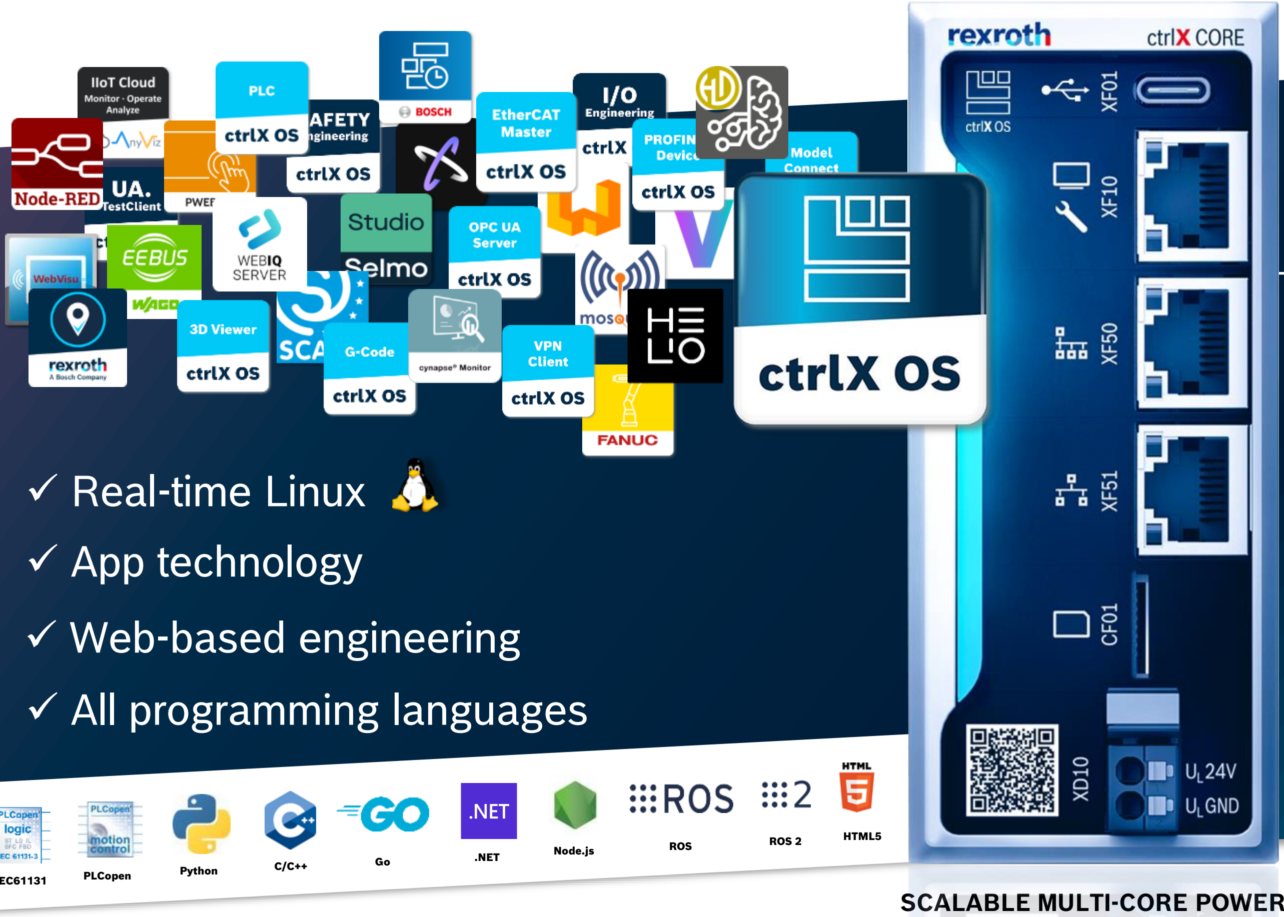
Reference: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

Innovative **Cybersecurity Solutions**

Our mission is to make automation **truly open**, programmable for **everybody** and to enable **co-creation** like never before.

and secure

ctrlX AUTOMATION
The Smartphone of Automation



- ✓ Real-time Linux
- ✓ App technology
- ✓ Web-based engineering
- ✓ All programming languages

SCALABLE MULTI-CORE POWER

- ✓ Complete Automation System

- ✓ ctrlX OS Store
- ✓ ctrlX Device Portal

CENTRAL IT PORTALS

- ✓ IoT integration with security by design
  compliant to IEC62443 SL2 (SL3 in preparation)

Cyber
Resilience
Act ready

ctrlX AUTOMATION | rexroth A Bosch Company

ctrlX AUTOMATION
Our Journey so far...

MARKET LAUNCH
THE MOST OPEN AUTOMATION SYSTEM

2020 | ctrlX AUTOMATION

FROM AN OPEN AUTOMATION SYSTEM TO AN **INDUSTRIAL ECOSYSTEM**

ctrlX World

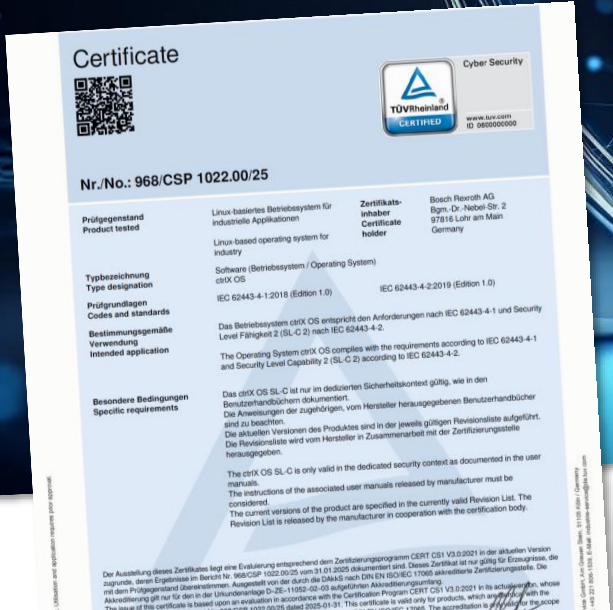
2021 | ctrlX World

THE **OPERATING SYSTEM** FOR INDUSTRIAL AUTOMATION

ctrlX OS

2022 | ctrlX OS

Why are we **CRA** ready?



Certificate

Cyber Security

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

Nr./No.: 968/CSP 1022.00/25

Prüfgegenstand Product tested	Linux-basiertes Betriebssystem für industrielle Applikationen Linux-based operating system for industry	**Zertifikats-inhaber Certificate holder**	Bosch Rexroth AG Bgm.-Dr.-Nebel-Str. 2 97816 Lohr am Main Germany
Typbezeichnung Type designation	Software (Betriebssystem / Operating System) ctrlX OS		
Prüfgrundlagen Codes and standards	IEC 62443-4-1:2018 (Edition 1.0)		IEC 62443-4-2:2019 (Edition 1.0)
Bestimmungsgemäße Verwendung Intended application	Das Betriebssystem ctrlX OS entspricht den Anforderungen nach IEC 62443-4-1 und Security Level Fähigkeit 2 (SL-C 2) nach IEC 62443-4-2. The Operating System ctrlX OS complies with the requirements according to IEC 62443-4-1 and Security Level Capability 2 (SL-C 2) according to IEC 62443-4-2.		
Besondere Bedingungen Specific requirements	Das ctrlX OS SL-C ist nur im dedizierten Sicherheitskontext gültig, wie in den Benutzerhandbüchern dokumentiert. Die Anweisungen der zugehörigen, vom Hersteller herausgegebenen Benutzerhandbücher sind zu beachten. Die aktuellen Versionen des Produktes sind in der jeweils gültigen Revisionsliste aufgeführt. Die Revisionsliste wird vom Hersteller in Zusammenarbeit mit der Zertifizierungsstelle herausgegeben. The ctrlX OS SL-C is only valid in the dedicated security context as documented in the user manuals. The instructions of the associated user manuals released by manufacturer must be considered. The current versions of the product are specified in the currently valid Revision List. The Revision List is released by the manufacturer in cooperation with the certification body.		

Der Ausstellung dieses Zertifikates liegt eine Evaluierung entsprechend dem Zertifizierungsprogramm CERT CS1 V3.0:2021 in der aktuellen Version zugrunde, deren Ergebnisse im Bericht Nr. 968/CSP 1022.00/25 vom 31.01.2025 dokumentiert sind. Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Ausgestellt von der durch die DAkkS nach DIN EN ISO/IEC 17065 akkreditierte Zertifizierungsstelle. Die Akkreditierung gilt nur für den in der Urkundenanlage D-ZE-11052-02-03 aufgeführten Akkreditierungsumfang.

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT CS1 V3.0:2021 in its actual version, whose
1022.00/25 dated 2025-01-31. This certificate is valid only for products, which are identical with the
The accreditation is only valid for the scope

Utilisation and application requires prior approval.

GmbH, Am Grauen Stein, 51105 Köln / Germany
+49 221 806-1539, E-Mail: industrie-service@de.tuv.com

Cybersecurity
ctrlX OS main features

Available on all ctrlX OS enabled devices

ctrlX OS

Cyber
Resilience
Act ready

ctrlX OS is secure by design & secure by default

Security is a key requirement during development and for the entire product lifecycle

The device is shipped with a minimal network footprint

Only secure protocols (e. g. https) are enabled by default to protect the data which is stored, transmitted or otherwise processed

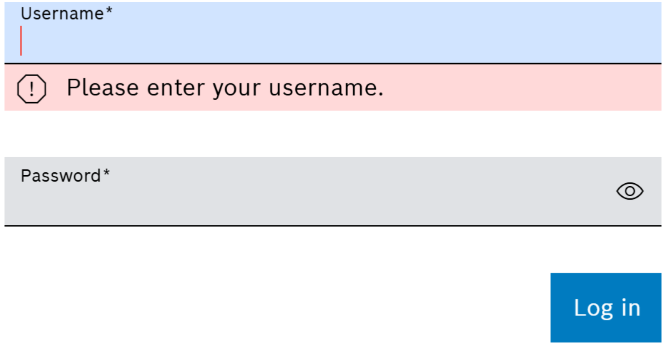
Authentication and authorization are crucial existing functions

Multiple integration points for 3rd party apps to adapt to the security ecosystem using the SDK

Reduced development effort

Cybersecurity
ctrlX OS main features

User Management



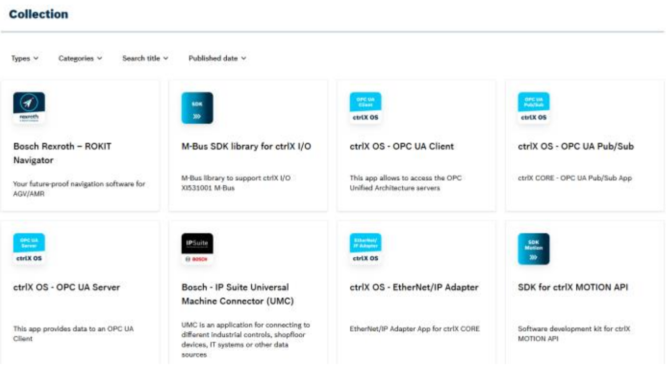
Username*

Please enter your username.

Password*

Enforces mandatory login, **configurable** password policies, and granular permission management for **secure access**.

App Management



Collection

Bosch Rexroth – ROKIT Navigator
Your future-proof navigation software for AGV/AMR

M-Bus SDK library for ctrlX I/O
M-Bus library to support ctrlX I/O XI531001 M-Bus

ctrlX OS - OPC UA Client
This app allows to access the OPC Unified Architecture servers

ctrlX OS - OPC UA Pub/Sub
ctrlX CORE - OPC UA Pub/Sub App

ctrlX OS - OPC UA Server
This app provides data to an OPC UA Client

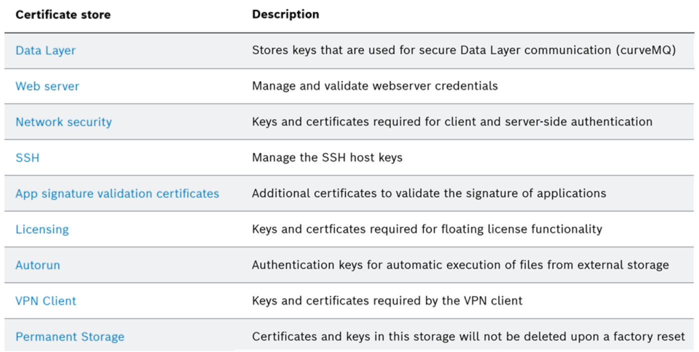
Bosch - IP Suite Universal Machine Connector (UMC)
UMC is an application for connecting to different industrial controls, shopfloor devices, IT systems or other data sources

ctrlX OS - EtherNet/IP Adapter
EtherNet/IP Adapter App for ctrlX CORE

SDK for ctrlX MOTION API
Software development kit for ctrlX MOTION API

Provides sandboxed app execution, managed updates, and **signature verification** for **application integrity**.

Certificate Management



Certificate store	Description
Data Layer	Stores keys that are used for secure Data Layer communication (curveMQ)
Web server	Manage and validate webserver credentials
Network security	Keys and certificates required for client and server-side authentication
SSH	Manage the SSH host keys
App signature validation certificates	Additional certificates to validate the signature of applications
Licensing	Keys and certficates required for floating license functionality
Autorun	Authentication keys for automatic execution of files from external storage
VPN Client	Keys and certificates required by the VPN client
Permanent Storage	Certificates and keys in this storage will not be deleted upon a factory reset

Ensures data confidentiality and **secure** communication through app-specific key stores and **automated certificate lifecycle**.

ctrlX OS – Cybersecurity Vulnerability Handling

Security along the entire life cycle

ctrlX OS

Cyber Resilience Act ready

ctrlX OS is actively and continuously monitored for vulnerabilities in all (sub-)components

The developers are notified about potential vulnerabilities immediately when detected

ctrlX OS is subject to regular internal vulnerability assessments and external penetration tests

Dynamic and static application security testing using self-developed and established tools

Penetration tests upon each LTS release

Cybersecurity – Apps and Services
ctrlX CORE? A Security Gateway!

W 580 02
ctrlX OS
rexroth
ctrlX CORE
XF01
XF10
XF50
XF51
CF01
XD10
U₁ 24V
U₁ GND

Security Scanner
ctrlX OS

Machine assessment / network testing

- List the components and determine the overall security state of your machinery
- Identify potential attack surfaces

Firewall
ctrlX OS

Protection against unauthorized access

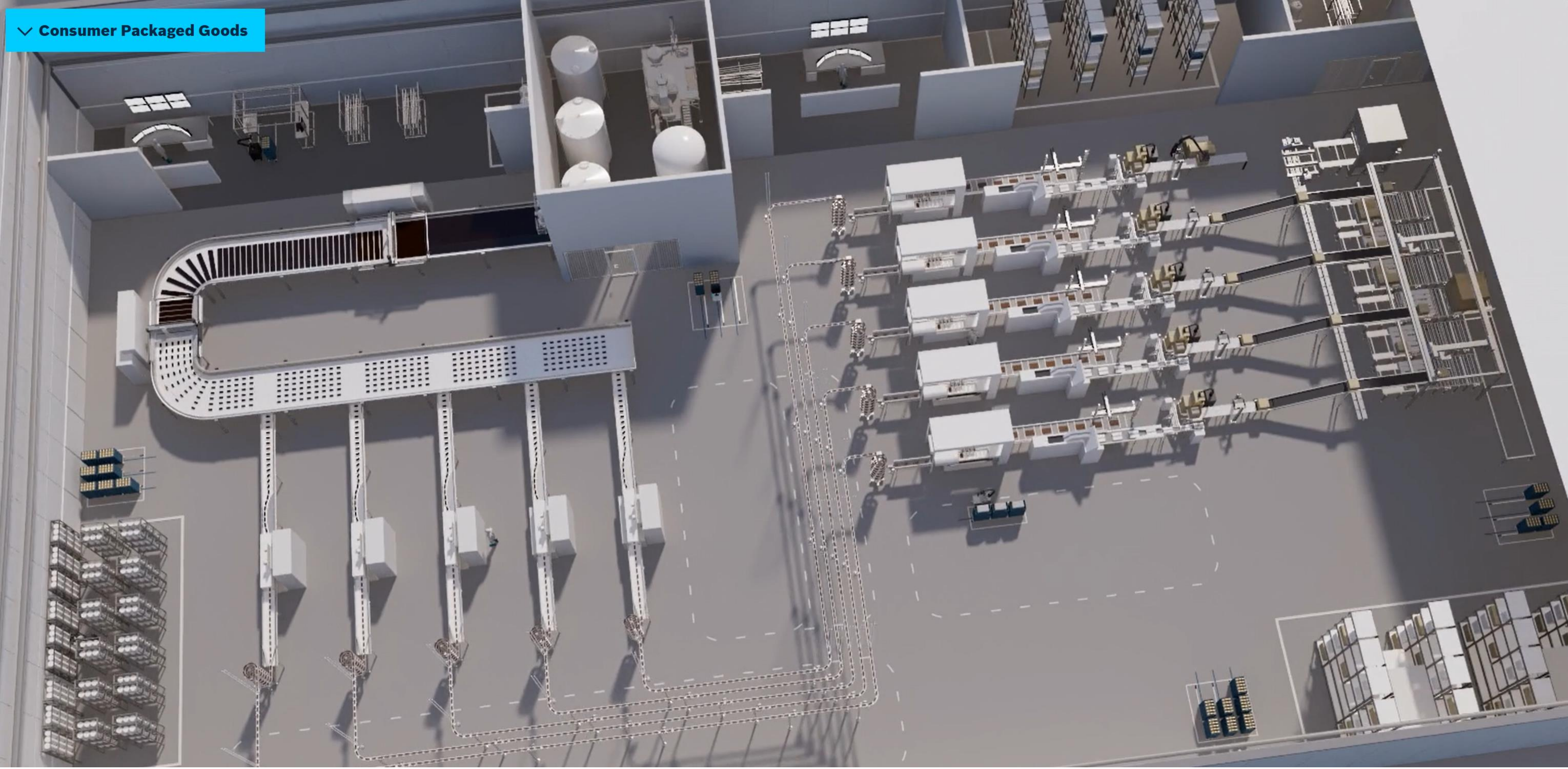
- Limit attack surfaces to a minimum
- Control & restrict access to attached devices

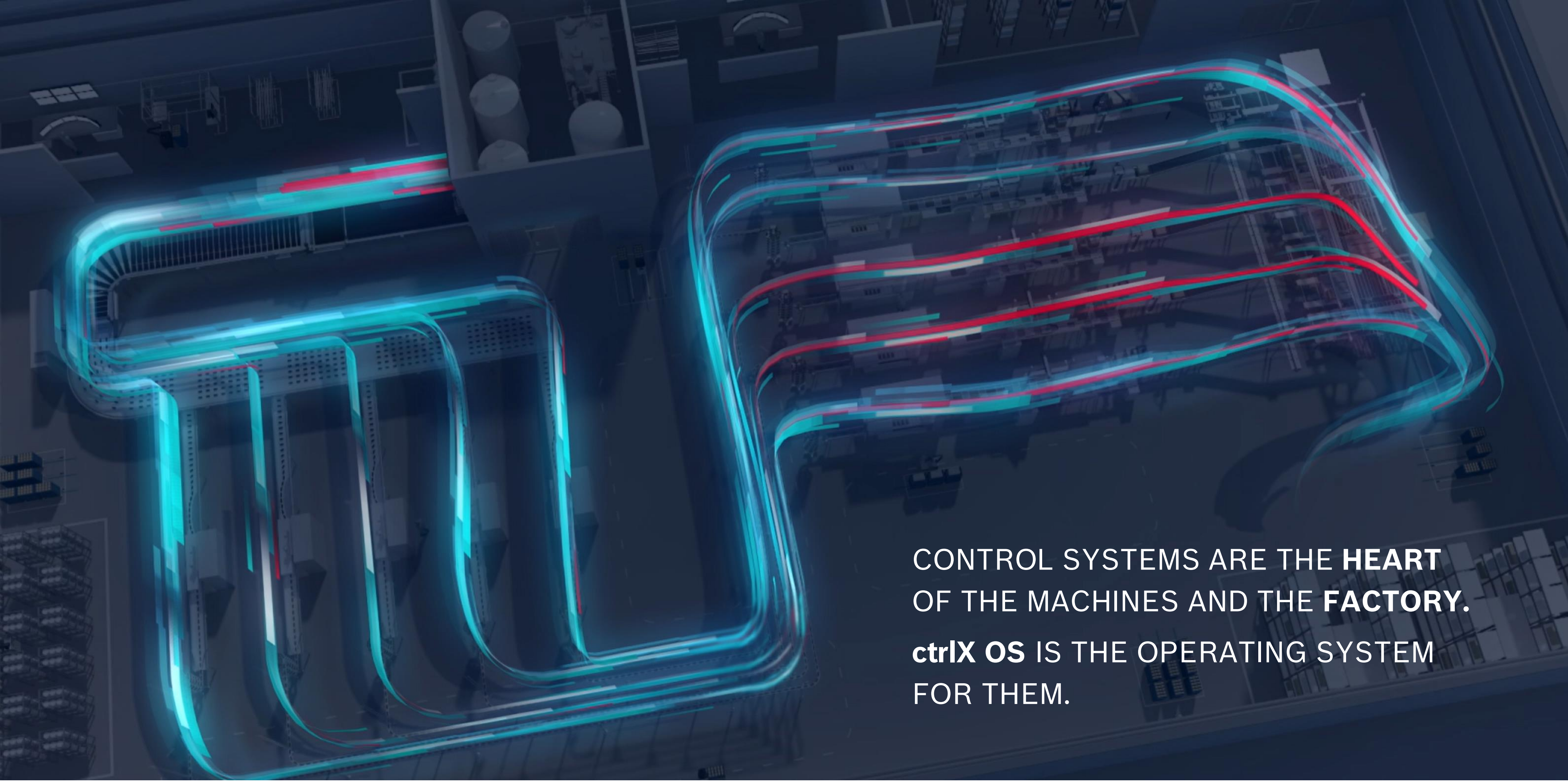
VPN Client
ctrlX OS

Secure remote maintenance

- Securely access your device(s) from external networks
- Restrict access
- Update/Patch machine remotely

Consumer Packaged Goods

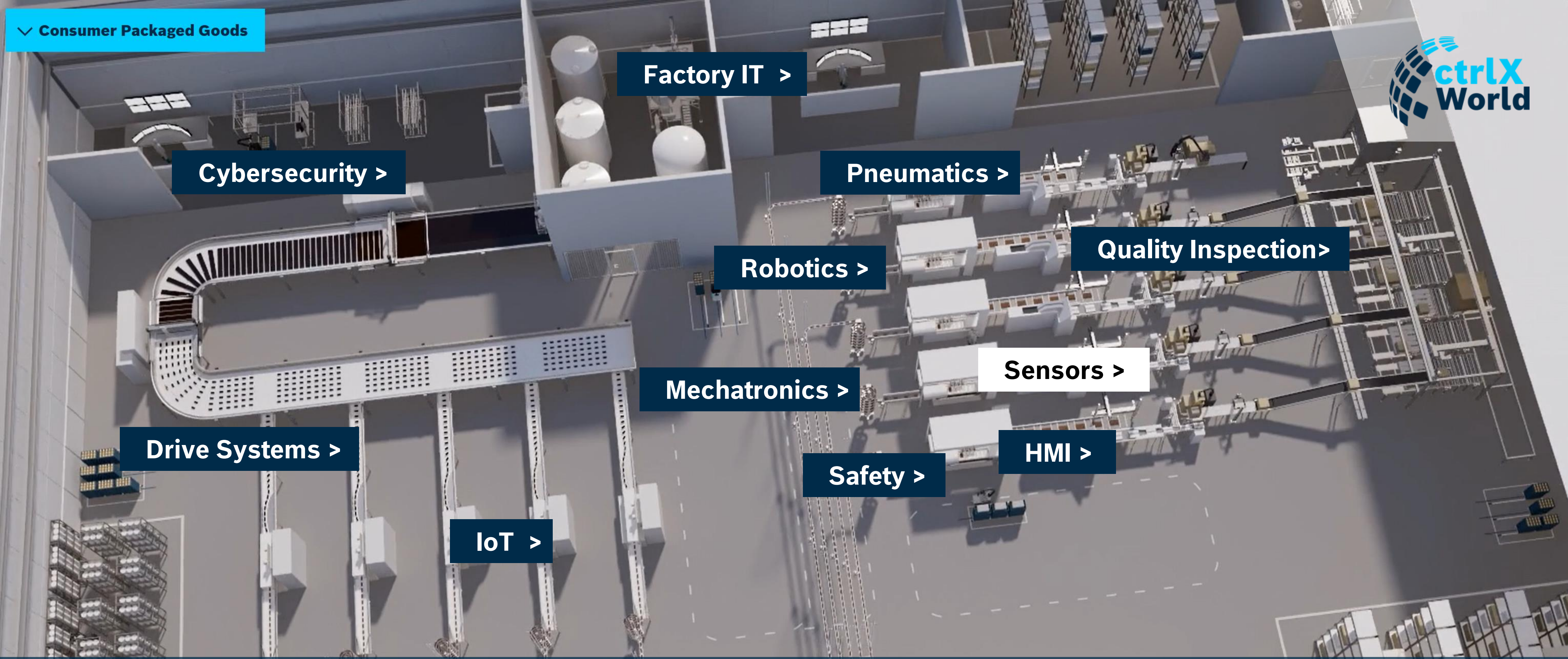




CONTROL SYSTEMS ARE THE **HEART** OF THE MACHINES AND THE **FACTORY.**

ctrlX OS IS THE OPERATING SYSTEM FOR THEM.

Consumer Packaged Goods



AUTOMATION CONSISTS **OF MORE.** INTERACTION AND INTEGRATION OF ALL AREAS **MUST BE EASY.**
ctrlX OS ECOSYSTEM WITH ITS **ctrlX World PARTNERS** UNITES ALL FOR **THE BENEFIT OF ITS USERS.**

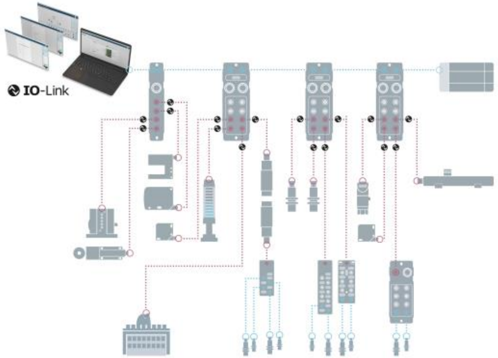
ctrlX World
Balluff GmbH

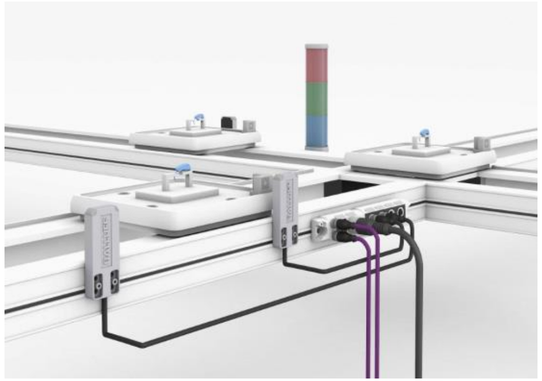
IO-LINK - SENSOR INTEGRATION

Easy Integration of intelligent sensors and actuators via IO-Link.
Optional use of additional condition monitoring data

TRACEABILITY IN PRODUCTION

Easy and safe Identification of products or tools via RFID. Additional Condition Monitoring data from each Read/Write head supports an easy and safe commissioning as well as predictive maintenance.





ADVANTAGES

- Now part of ctrlX World:
  IO-Link portfolio with countless products for your factory automation
  Largest industrial RFID portfolio for almost every of your application
- Balluff is preferred supplier for Bosch worldwide
- Strong service- and support-structure, #Service Matters
- Global presence in 61 countries worldwide

TARGET INDUSTRIES

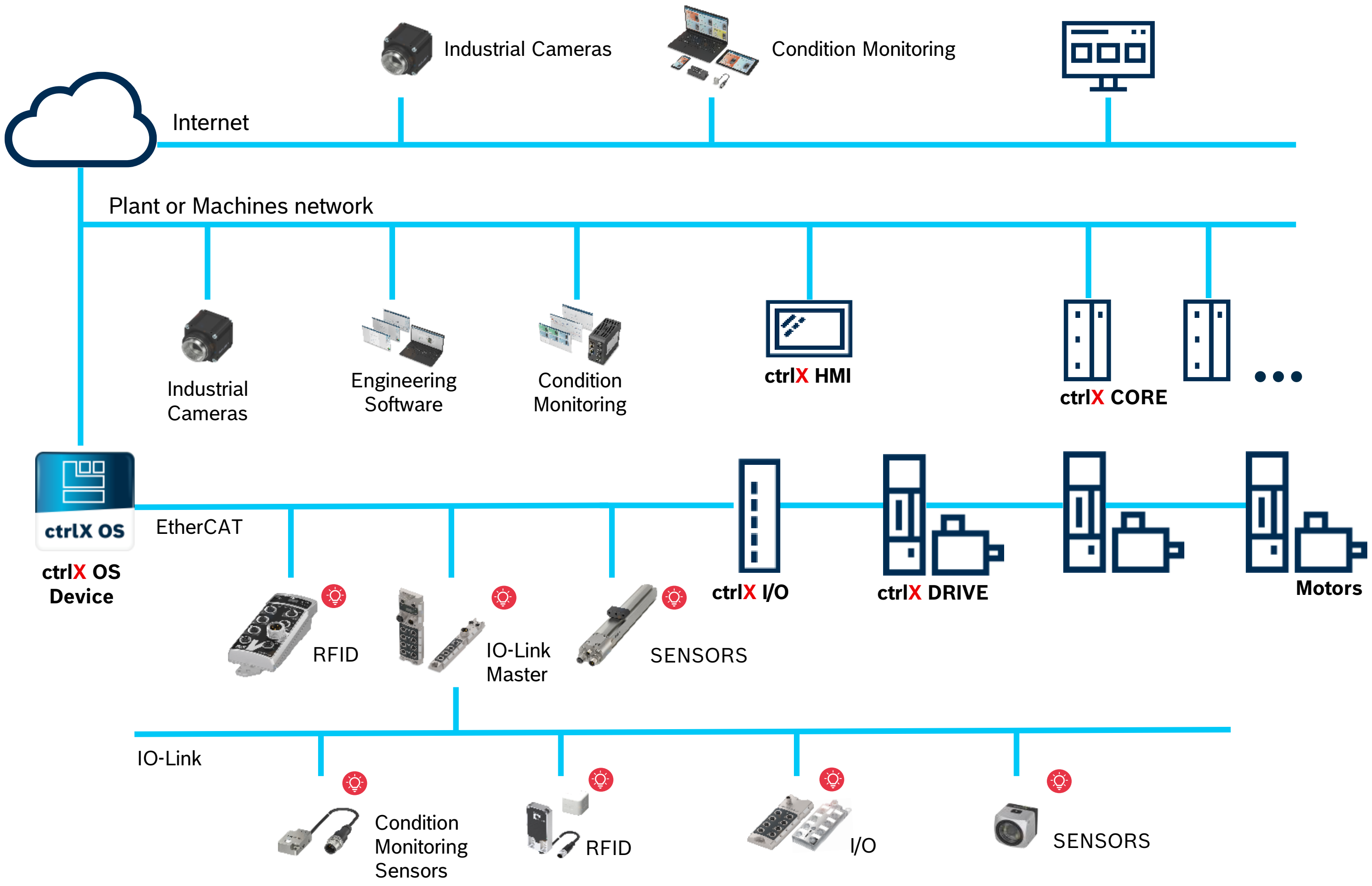
- Automation, robotics, assembly
- Metal processing
- Mobility
- Packaging, food & beverage

TARGET CUSTOMERS

Machine builder ☒

Machine operator □

ctrlX World
Balluff GmbH



BALLUFF SENSORS INTEGRATION

Balluff sensors easily connect to ctrlX OS and provide vital machine data.

ctrlX World
Partner Security Solutions

ctrlX World

SECURE REMOTE MAINTENANCE

IXON Cloud – end-to-end IIoT solution for all your remote service and maintenance needs: from hardware to the cloud.

OPTIONAL

Firewall

ctrlX OS

SECURE REMOTE MAINTENANCE

Securely access your device(s) from external networks.

Restrict access based on machinery state and onsite approval.

OPTIONAL

Firewall

ctrlX OS

EDGE IPS NETWORK PROTECTION

To be used at the entry point of the machine/plant to analyze the traffic, identify potential threats and protect the machine blocking them.

txOne networks

NETWORK MONITORING

Monitoring of IT; OT and IoT networks in real-time. Shows alerts, error sources, and even bandwidth peaks at a glance in a dashboard.

PAESSLER
THE MONITORING EXPERTS

Download on the ctrlX OS Store

ctrlX AUTOMATION | rexroth A Bosch Company

ctrlX World
110+ partners

ctrlX World

COMMUNICATION

BOSCH
MB CONNECTLINE
MBS
SwarmGuard INDUSTRIAL
TOSIBOX

SECURITY

Rhebo a Landis+Gyr company
txOne networks

MECHATRONICS

SCHUNK
WITTENSTEIN

MOTION

COGNIBOTICS
FuzzyLogic
vorausrobotik

HMI

HELIO
MGA
SMARTHMI
SpiderControl
Weidmüller GTI Software

ENGINEERING

CORDIS SUITE
EPLAN
FACTORY I/O
FANUC
F.EE
GEFAZ AUTOMATION
ISG
KUKA
machineering THE TIMESAVER COMPANY
MAIROTEC
MathWorks
NEXEED
realvirtual.io
Selmo
SOFTWARE DEFINED AUTOMATION
TwinStore
wepall

IOT

Actility
AnyViz
cedalo
Cybus
FlowFuse
FUJITSU
i-flow
influxdata
ixon
KATULU
mosquitto
OROBIX WE MAKE AI HAPPEN
salesforce
S.
SQL4AUTOMATION
timecho
VEL energy unveil your hidden energy
APP NOW

DEVICE

ARDUINO PRO
autonox Robotics
BALLUFF
BELDEN
CoreTigo
Elmo Motion Control
EMERSON AVENTICS
Edmund optics
FAULHABER
FESTO
HAILO
ifm
kassow robots strong · fast · simple
KEBA Automation by innovation.
Lanner
LAPP
LENORD+BAUER Finding solutions. Founding trust.
LinMot
LUCID VISION LABS
maxon
MOXA
PEPPERL+FUCHS
SCHMERSAL THE DNA OF SAFETY
SEW EURODRIVE
SICK Sensor Intelligence.
SMC Expertise – Passion – Automation
synapticon
TURCK
WAGO
zodiac robotics

SENSE & VISION

elunic
LANDING AI
vathos robotics
HD VISION
36ZERO VISION
xis.ai

PLC

CODESYS
logiccloud
neuron AUTOMATION

FACTORY IT

ARKITE
FORCAM smart factory experts
mpdv
oee.ai
PAESSLER THE MONITORING EXPERTS
servicenow
TULIP
NC VISION Business Success, Automated.

SERVICES

.ATINA
AUNOVIS
robotizerd
Canonical
etteplan
HMI Project
ITQ
infoteam software
iteratec
M&M software
mm1
SIMON
UID
UNIVERSITY 4 INDUSTRY
XITASO

TECHNOLOGY

intel
NOKIA
vmware by Broadcom

rexroth
A Bosch Company

Cybersecurity
Summary

- ✓ ctrlX OS is compliant to IEC62443-4-2 SL2
- ✓ Secure by design & secure by default
- ✓ Protects data which is stored or transmitted or otherwise processed
- ✓ Provides the platform to distribute and to apply vulnerability patches without delay and side effects
- ✓ Robust, resilient and ready for the CRA
- ✓ ctrlX OS devices are secure
- ✓ Further security apps – Download on ctrlX OS Store
- ✓ Cybersecurity consulting

Security Scanner ctrlX OS

Firewall ctrlX OS

VPN Client ctrlX OS

txOne networks

PAESSLER THE MONITORING EXPERTS

Download on the ctrlX OS Store

Cyber Resilience Act ready

ctrlX AUTOMATION | rexroth A Bosch Company

Let's go CRAzy! Secure.

YOUR CONTACTS

Hans Michael Krause
hans-michael.Krause@boschrexroth.de
+49 175 26 92 135
Director Partner Ecosystem
Bosch Rexroth AG