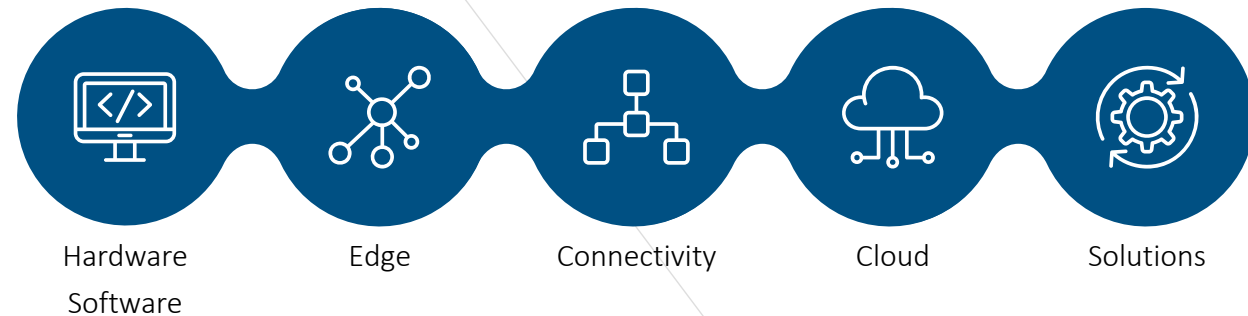# KontronOS

June 2024

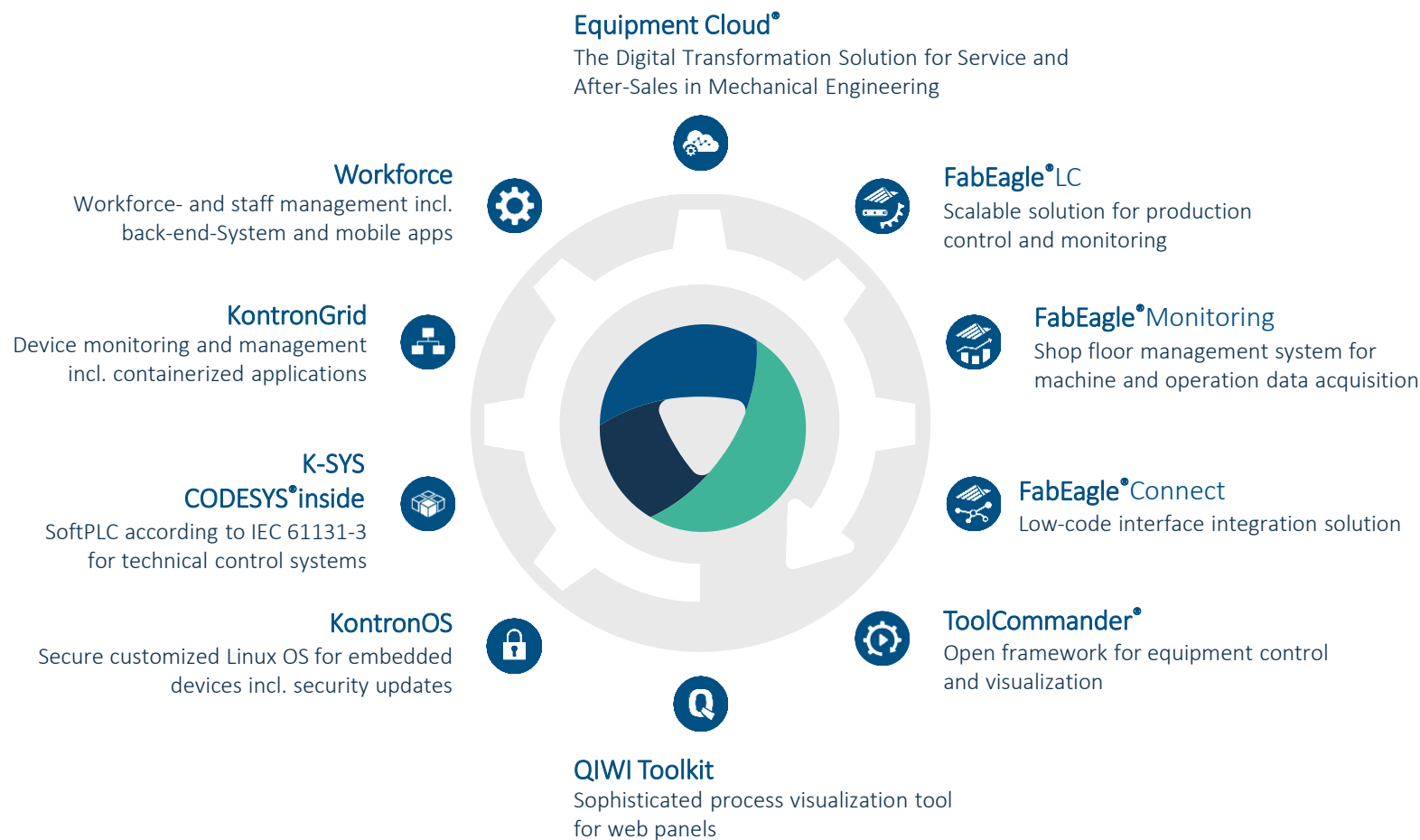# Kontron susietec®

The toolset of software, hardware and expertise

› Facilitated access to digitalization with the smart solution approaches from the kontron susietec® toolset

› susietec® brings together software, hardware and expertise - with the aim of exploiting the potential of IIoT and Industry 4.0 in a new way

› Support for and collaboration with customers from the high-tech, automotive and pharmaceutical industry and thus facilitated access to future-oriented business models

| Hardware Software | Edge | Connectivity | Cloud | Solutions |

Kontron susietec® Overview

Equipment Cloud®
The Digital Transformation Solution for Service and After-Sales in Mechanical Engineering

Workforce
Workforce- and staff management incl. back-end-System and mobile apps

FabEagle®LC
Scalable solution for production control and monitoring

KontronGrid
Device monitoring and management incl. containerized applications

FabEagle®Monitoring
Shop floor management system for machine and operation data acquisition

K-SYS CODESYS®inside
SoftPLC according to IEC 61131-3 for technical control systems

FabEagle®Connect
Low-code interface integration solution

KontronOS
Secure customized Linux OS for embedded devices incl. security updates

ToolCommander®
Open framework for equipment control and visualization

QIWI Toolkit
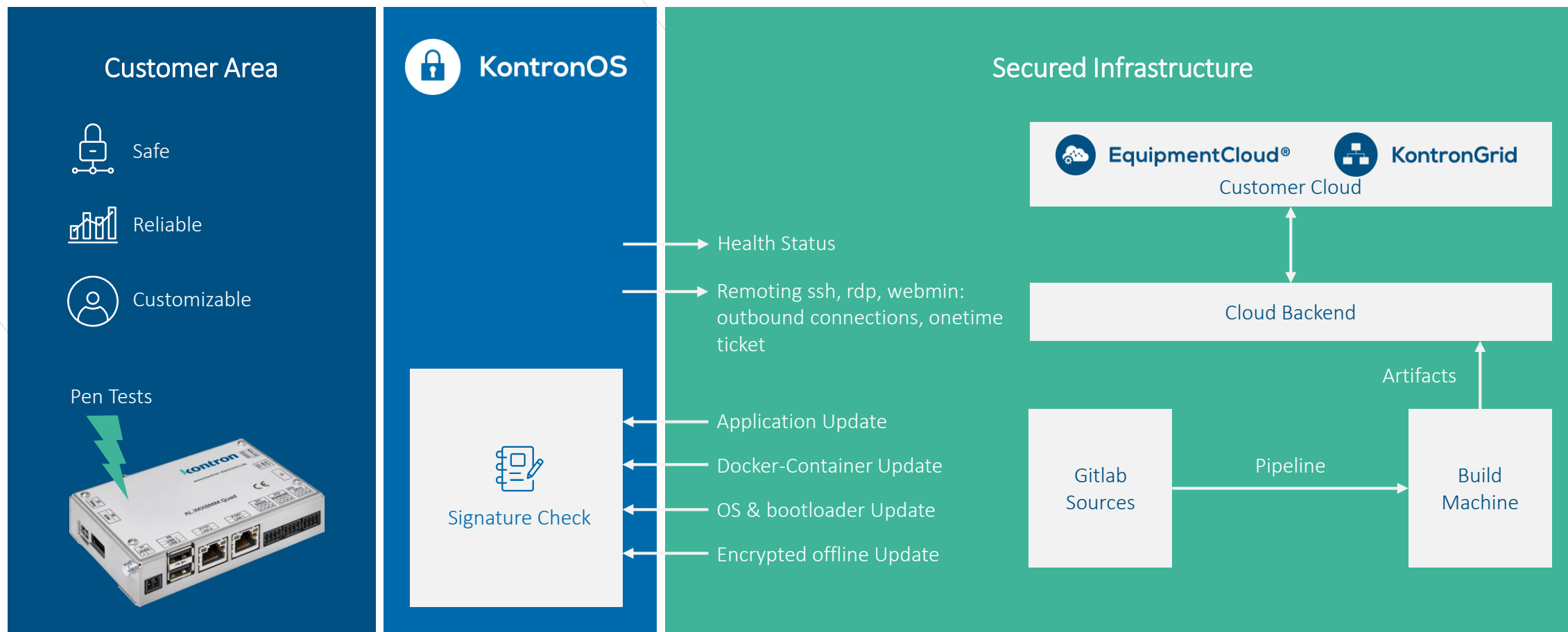Sophisticated process visualization tool for web panels

The elements of the kontron susietec® toolset can be combined to tailor individual solutions for different applications.
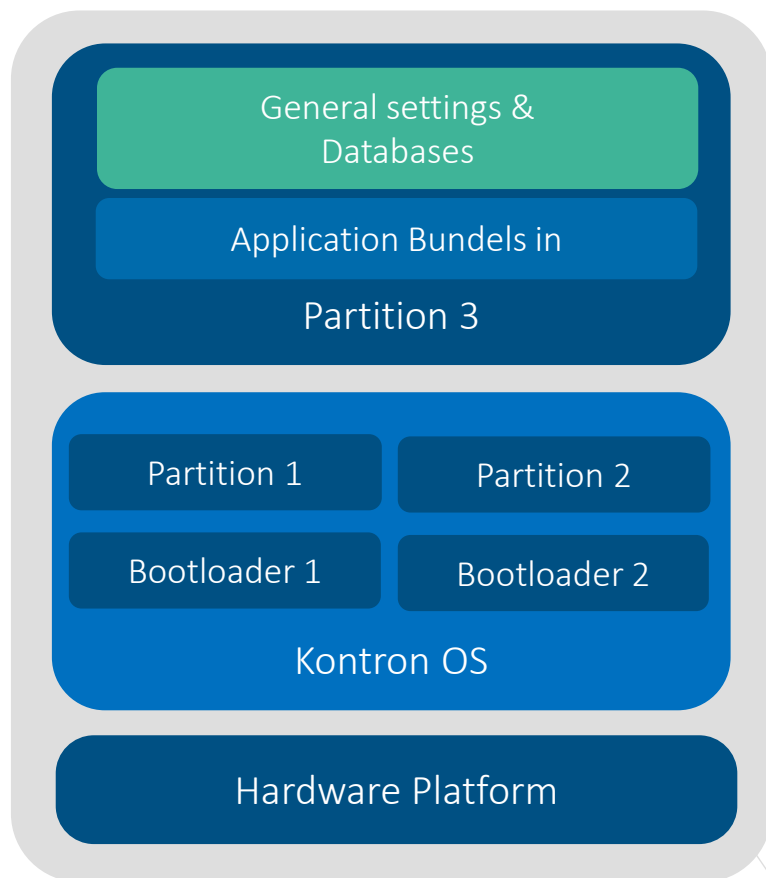
KontronOS IoT-Bundle

› In critical environments, security for integrated devices is the top priority. The growing number of autonomous devices without an operator represent a significant attack surface for companies.

› The KontronOS IoT bundle provides maximum security and actuality of Linux-based embedded device in the field for a reliable operation of customer applications over the entire product lifecycle.

› The hardened KontronOS operating system protects IoT solutions in critical environments from compromise, external access and uncontrolled updates, so that containerized or native applications can run securely and without interruption.

› The automated update process ensures that the system is always up to date. Especially with a large number of devices, we ensure that all devices in the field are at the same update level, despite different schedules and threat scenarios.
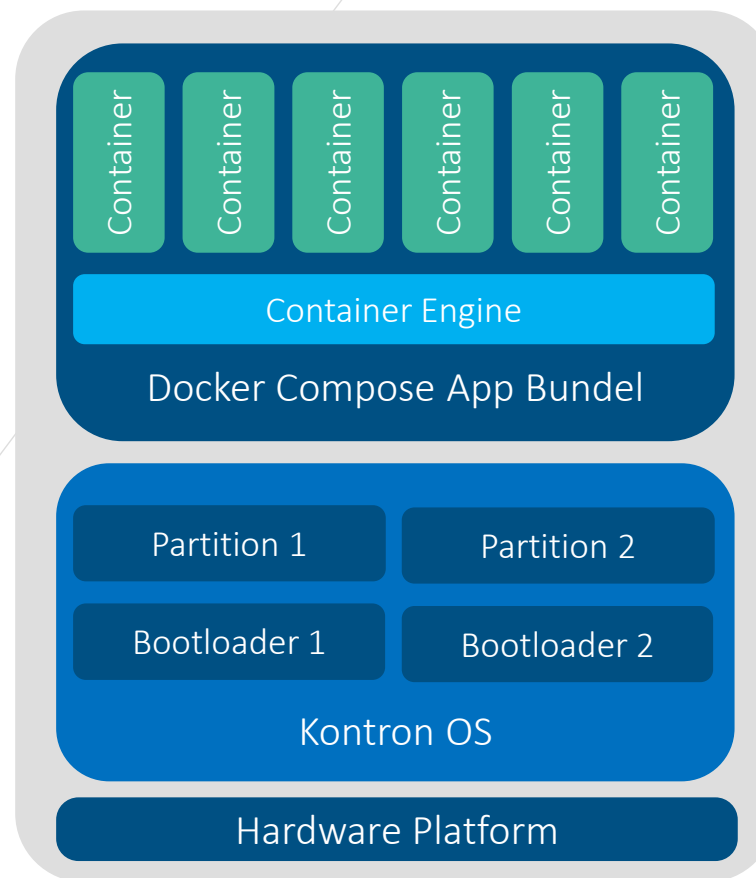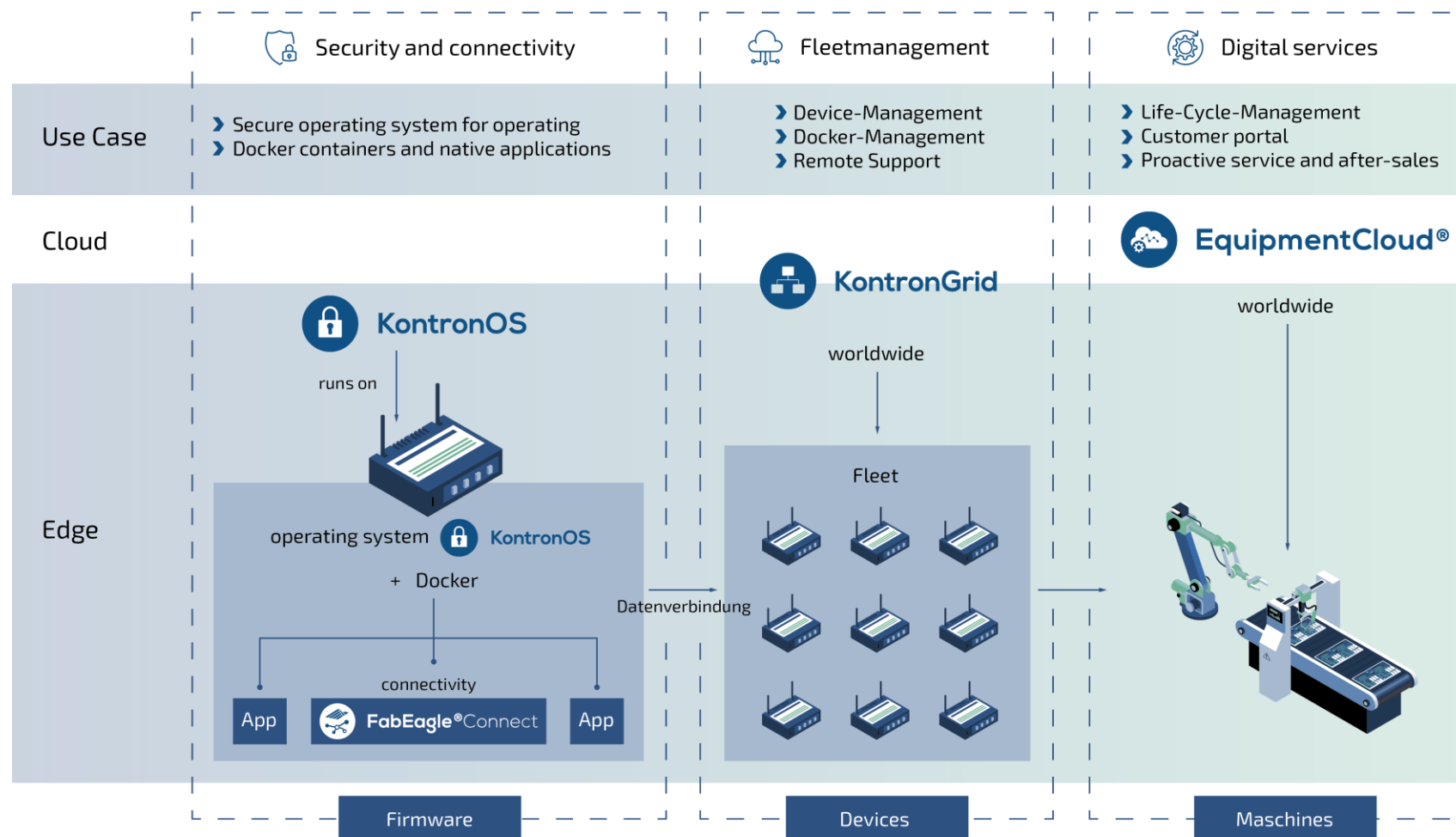
IoT Security by Design

NIS2

KontronOS Setup

Native Applications

- General settings & Databases
- Application Bundels in
- Partition 3
- Partition 1 | Partition 2
- Bootloader 1 | Bootloader 2
- Kontron OS
- Hardware Platform

Docker Container

- Container | Container | Container | Container | Container | Container
- Container Engine
- Docker Compose App Bundel
- Partition 1 | Partition 2
- Bootloader 1 | Bootloader 2
- Kontron OS
- Hardware Platform

Interplay and differentiation of susietec® products

	Security and connectivity	Fleetmanagement	Digital services
Use Case	❯ Secure operating system for operating ❯ Docker containers and native applications	❯ Device-Management ❯ Docker-Management ❯ Remote Support	❯ Life-Cycle-Management ❯ Customer portal ❯ Proactive service and after-sales
Cloud			EquipmentCloud®
Edge	KontronOS runs on operating system 🔒 KontronOS + Docker connectivity App — FabEagle®Connect — App	KontronGrid worldwide Fleet Datenverbindung	worldwide
	Firmware	Devices	Maschines

The Challenge NIS2

› The vast majority of EU companies have been compromised by cyberattacks in the last 3 years.

› The goverment fears that a cyberattack can paralyse an important area from the population.

› The fear is that chaos, unrest and escalation which can endanger public safety to a high degree.

› Therefore, the EU has adopted the Network & Information Security (NIS) guidelines and has released NIS2

› These are currently being transposed into national law and industry-specific requirements.

› NIS2 requirements will become mandatory for EU in q4 2024

› They will become mandatory for critical facilities of energy, water, transportation, digital services and more

› So many Kontron customers will face discussion about NIS2 and cybersecurity and these tasks:

› How ensuring the operation of a system and restoring its function?

› How to prevent foreign software from running on my device?

› How do I ensure that the devices can be updated in the long term?

› How to implement intrusion detection and notifications?

Cyber Security

Steady increase of legal requirements

› 1990 BSI Errichtungsgesetz
  › Act on the Establishment of the Federal Office for Security in Information Technology
› 2004 ENISA
  › European Union Agency for Cybersecurity
› 2015 IT Sicherheitsgesetzt
  › Act to increase the security of information technology system
  › Inclusion of critical infrastructures
› 2016 NIS Directive
  › Directive on Security of Network and Information Systems
› 2016/ 2018 GDPR
  › DSGVO General Data Protection Regulation
› 2018 Nachweisprüfung
  › First verification test of sector: Energie, Wasser, IT&TK, Ernährung
› 2019 EU Cybersecurity Act
  › European cybersecurity certification framework
› 2021 IT-Sicherheitsgesetz 2.0
  › Second law to increase the security of information technology systems

› 2021 BSI-Kritisverordnung
  › Regulation on the designation of critical infrastructures
› 2023 NIS Directive II
  › Directive on Security of Network and Information Systems
  › Released 18/10/24
› 2024 EU Cyber Resilience Act
  › common cybersecurity standards for hw & sw products in the EU
  › Released Q4/26
› 2024 BSI-Kritisverordnung
  › Upcoming Update
› ISO/IEC 27001
  › Information technology – Security techniques – Information security management systems – Requirements
› IEC 62443
  › Industrial communication networks – Network and system security

Major Benefits of KontronOS

Security at the highest level

Cyber Security

› tailored to use case and hardened Operating System
› Quarterly KontronOS Security Release Cycles with Pen-Tests
› Secure Boot / HAB and encrypted OS Partition
› Auto-configured, DNS-Table based firewall
› All connections are encrypted

Update Mechanism

› Redundant bootloader and OS Partition
› In addition encrypted offline updates
› delta updates for low bandwith transfer

Fail Safe Mechanism

› Automatic fallback process
› Signature check of all updates (bootloader, OS or applications)

KontronOS

An operating system tailored to the smooth operation of Docker Containers

Highest operating time

› Two redundant partitions (active and passive) ensure maximum uptime in the event of a failure, an interruption or a failed update, the uptime is maximized

Reduced to the essentials

› A minimal Linux-operating system with all the necessary functions it needs to ensure a smooth operation

Tailored for Costumer Applications

› Containerized applications are lightweight and ideal for connected devices, KontronOS creates a secure environment for them

Hardware-independent and easily customizable

› KontronOS on Yocto Linux® basis flexible for Intel® x86 & Arm® based devices applicable

Pricemodel - License

› used or delivered devices during performance period

› performance period is normally annual

› license is due before performance period

› Standard Product: no additional development cost

› Customized Product: initial non-recurring engineering costs

KontronOS

Simplified handling of multiple customer applications

› Channel: Kontron Europe

› Configuration:
  › Customized Kbox-A250 (IP54, housing extension, integration of modified connectors) & integration of open-source implementation Google OpenThread

› Volume: 100 (2023) / 300 (2024)

› Customer Products: mechanical seals and seal supply systems, magnetic couplings, carbon floating ring seals, expansion joints and flat gaskets, ATEX environment, Oil & Gas industry

› Application: OpenThread integration into the susietec® KontronOS operating system for enabling OpenThread Border Routers and AI inference. Handling of up to 30 dockers per IoT gateway. Managing setup-specific AI models using KontronOS with remoting and device management.

› Customer Advantage
  › Fast setup of complete solution with docker container management
  › Customized integration and modification of hardware, trust in our hardware & software compatibility
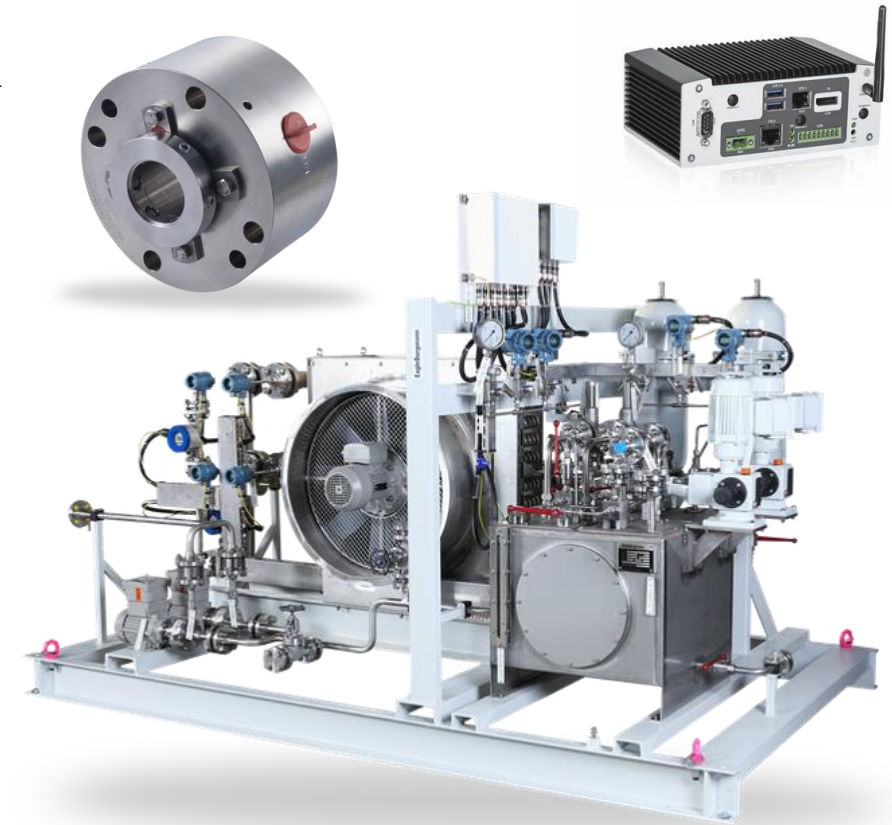
IoT device with docker management

› Channel: Kontron Electronics

› Configuration: Customer Specific IMX8

› Volume: 150 installed base / 150 (2023) / 250 (2024)

› Customer product: Tool refinement for surface hardening and special applications

› Application: KontronOS and connection own cloud solution, docker containers are generated and configured in Docker Compose, management & update roll-out docker and images via KontronOS, devices are managed, remoting access is being used

› Need: Overview of all installed IoT devices and machines and its production data

› Customer Advantage
  › KontronGrid functionality was convincing and one GUI for all services
  › Successful transfer from obsolete device management system to KontronOS & integration of existing Docker Compose configuration
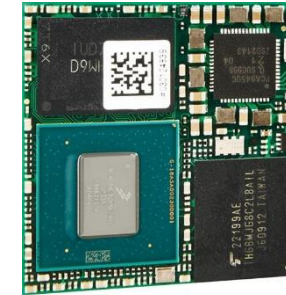
Children's Toys with flexible programming of actuators and sensors

› Channel: Kontron Electronics

› Configuration: Customized STM with M4 including customer specific baseboard for flexible IO connection

› Volumen: 10.000 per year

› Customer product: children's toy, controller offers plenty of different connection options for actuators e.g. motors, servos, compressor, LEDs and sensors e.g. button, magnetic and light sensors, heat sensor, ultrasound sensor, usb camera

› Application: qt app for touch display and swipe gestures with the possibility to load and run self created programs to setup the own solution

› Customer Advantage
  › Complete customer specific solution including hardware and software parts with KontronOS bases
  › Implementation of a large number of actuators and sensors

Thank you for your attention!