Sontheim

COMhawk® xt

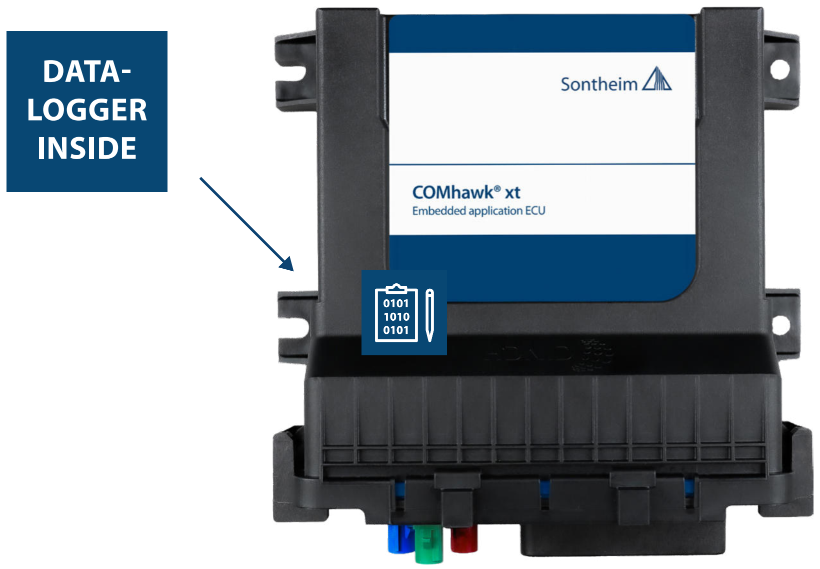
Control unit for embedded applications in mobile machines

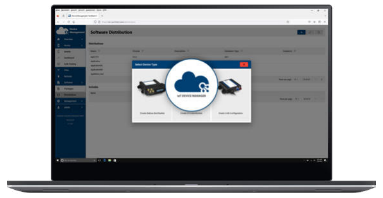
We live electronics!

We drive your business forward

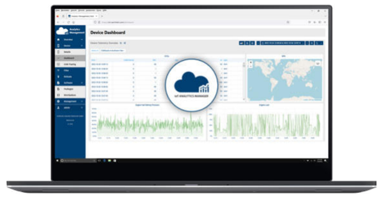
COMhawk® xt -
The OEM telematics solution

The COMhawk® xt ECU offers a seamless end-to-end solution with numerous expansion options. From the ECU with integrated data logger to the analysis software. Thanks to our modular approach, the COMhawk® xt fits seamlessly into any working environment.

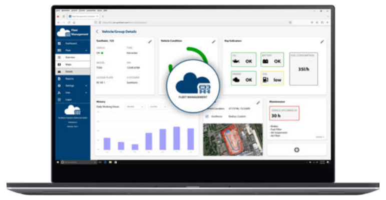




IoT Device Manager



IoT Analytics Manager



IoT Fleet Manager

NUMEROUS EXPANSION PRODUCTS:

Sensors (e.g., BT Beacon, wind sensors, tilt sensors, etc.), Communication Lifecycle Manager, Modular Diagnostic Tool 2.0, and much more.

Intelligently and systematically networking machines and vehicles

The networking of machines and vehicles has increased enormously in recent years, and will continue to be crucial to your success in the future. With the modular COMhawk® xt system, we offer a comprehensive Portfolio for networking and analyzing your machines and vehicles. With the help of various interfaces, you can create your own personal connectivity and diagnostic solution for on and off highway. With the intelligent linking of hardware and software, you can, for example:

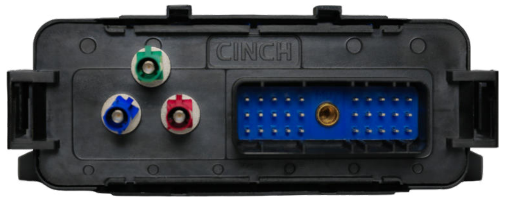
» Display, monitor, and check CAN data
» Parameterize, control, and regulate entire CAN networks
» Perform vehicle diagnostics
» Flash control units
» And much more

COMhawk® xt at the heart of the modular system

The COMhawk® xt embedded application ECU forms the heart of your system with up to four CAN interfaces, a powerful ARM Cortex A9 processor and Linux operating system. Developed for use in harsh conditions, it demonstrates its strengths as a standalone solution, as well as in conjunction with our comprehensive software solutions. It can be used flexibly as a telemetry and diagnostic module, as a gateway, and a data server or data logger.

Supplemented with the cloud-based IoT Device Manager, IoT Analytics Manager and/or the IoT Fleet Manager, you can analyze your vehicles in the field and visualize relevant data. You manage all units centrally, install remote updates, and benefit from live data monitoring.

COMhawk® xt



An ECU for your telemetry, diagnostics, and communication applications

The COMhawk® xt can be used for many applications, ranging from a simple data logger that transmits recorded operating data wirelessly, to a central communication and diagnostics ECU that combines different communication standards. Thanks to an operating range of -20 °C to +70 °C (-4°F to +158°F) and its compact housing with IP67 protection class, the device offers comprehensive protection, even in the presence of strong vibrations and harsh working environments.

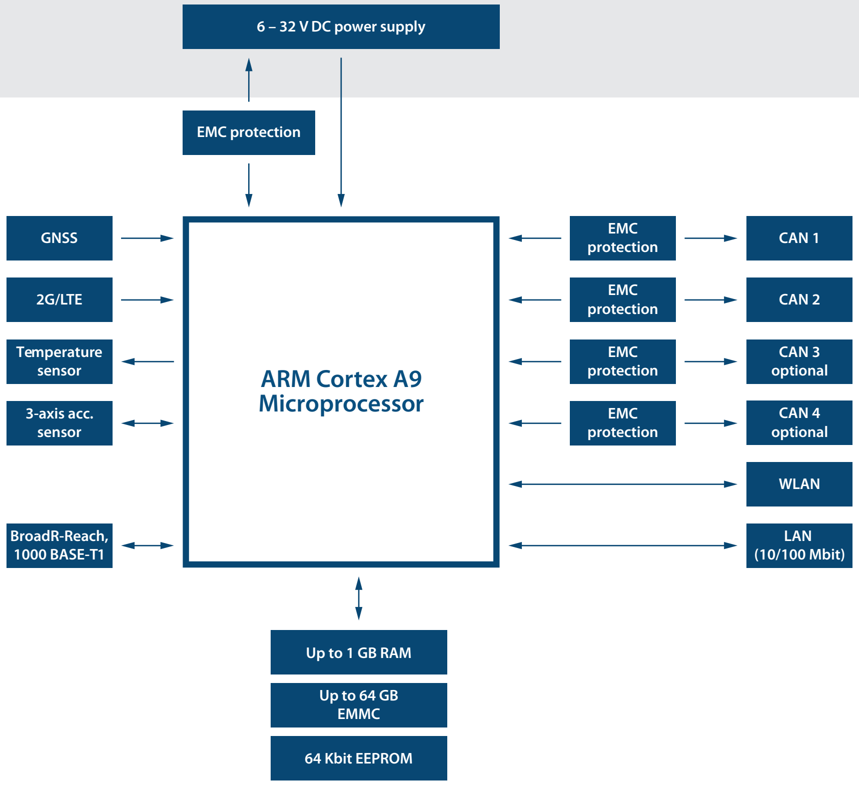
A Linux operating system provides a simple and optimal basis for fast OEM applications without additional costs.

Do you already use similar software?

Thanks to our modular approach, seamless integration of your existing software via interfaces is no problem. It is also possible to install your software directly on the device!

Interfaces and positioning

With four CAN channels and an Ethernet connection, the COMhawk® xt is comprehensively equipped.
For wireless data exchange, WLAN and an LTE CAT4 mobile connection are available. In addition, the ECU is equipped with a GNSS Receiver for positioning. Other features include four digital inputs and one digital output (500 mA).



KEY FEAUTURES

- 32 bit — Powerful ARM Cortex A9
- CAN — 4× CAN interface according to ISO 11898
- GNSS
- 4G — 4G LTE / 2G
- WLAN — WLAN according to IEEE 802.11 b/g/n
- 1× Ethernet, 10/100 Mbit/s
- Data logging
- Vibration-resistant
- IP67
- Compatible with customised software
- FOTA (Flash-over-the-air)
- Cyber Security
- E1 — E1 KBA approval

DATALOGGER

Data logger for maximum flexibility

The COMhawk® xt comes equipped with our Sontheim data logger as standard. It allows logging of various data sources. Thanks to numerous interfaces and support for a wide range of protocols, it can be seamlessly integrated into any vehicle and IT environment.

In particular, the local storage option with FIFO management offers real added value in daily use.

Interfaces & protocols:

» CAN: Raw CAN (J1939, CANopen), XCP
  -> Send, filter, multi-channel, auto baud rate
» RS232: Read & write
» VIMS: Send INFO, CMND, RPC_PING

Data collected:

» Sensors: GPS, acceleration, gyroscope
» System information: temperature, Wi-Fi, memory, data rates, uptime

Storage & export:

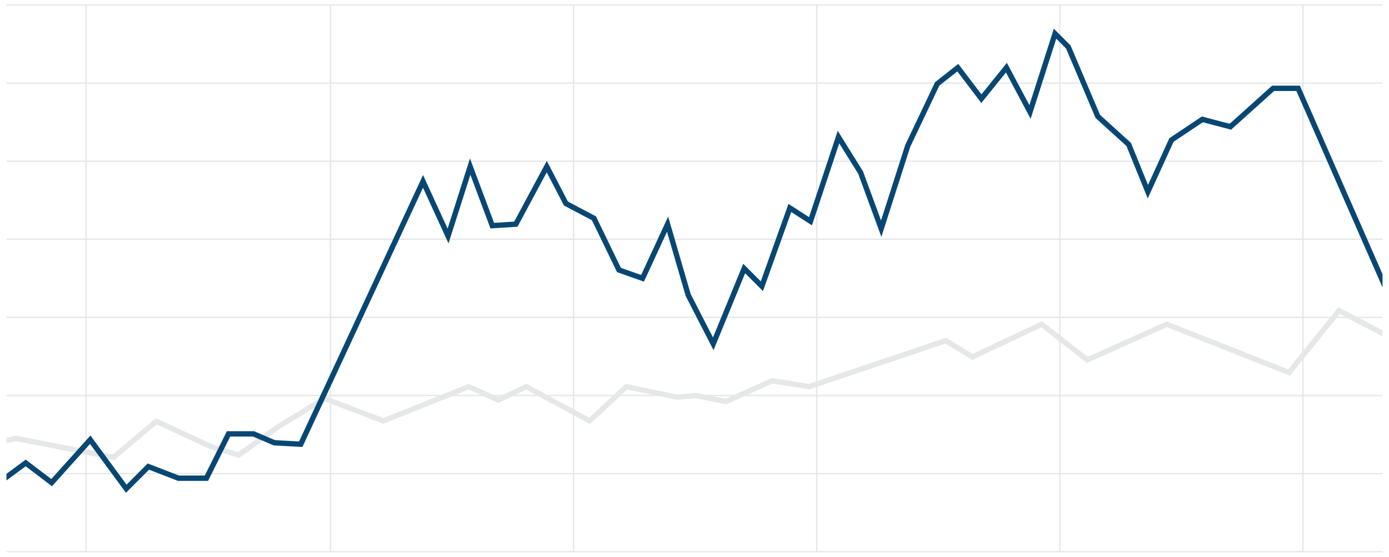
» Local storage with FIFO management
» Formats: JSON, Pickle, ASC
» Visualisation in near real time

Data transfer:

» Upload via HTTP POST, token-based
» Delay in case of missing connection
» Forwarding to other sie-dataloggers

Configuration & control:

» Modularly adjustable via web front end
» Start/stop via terminal 15, optional continued operation

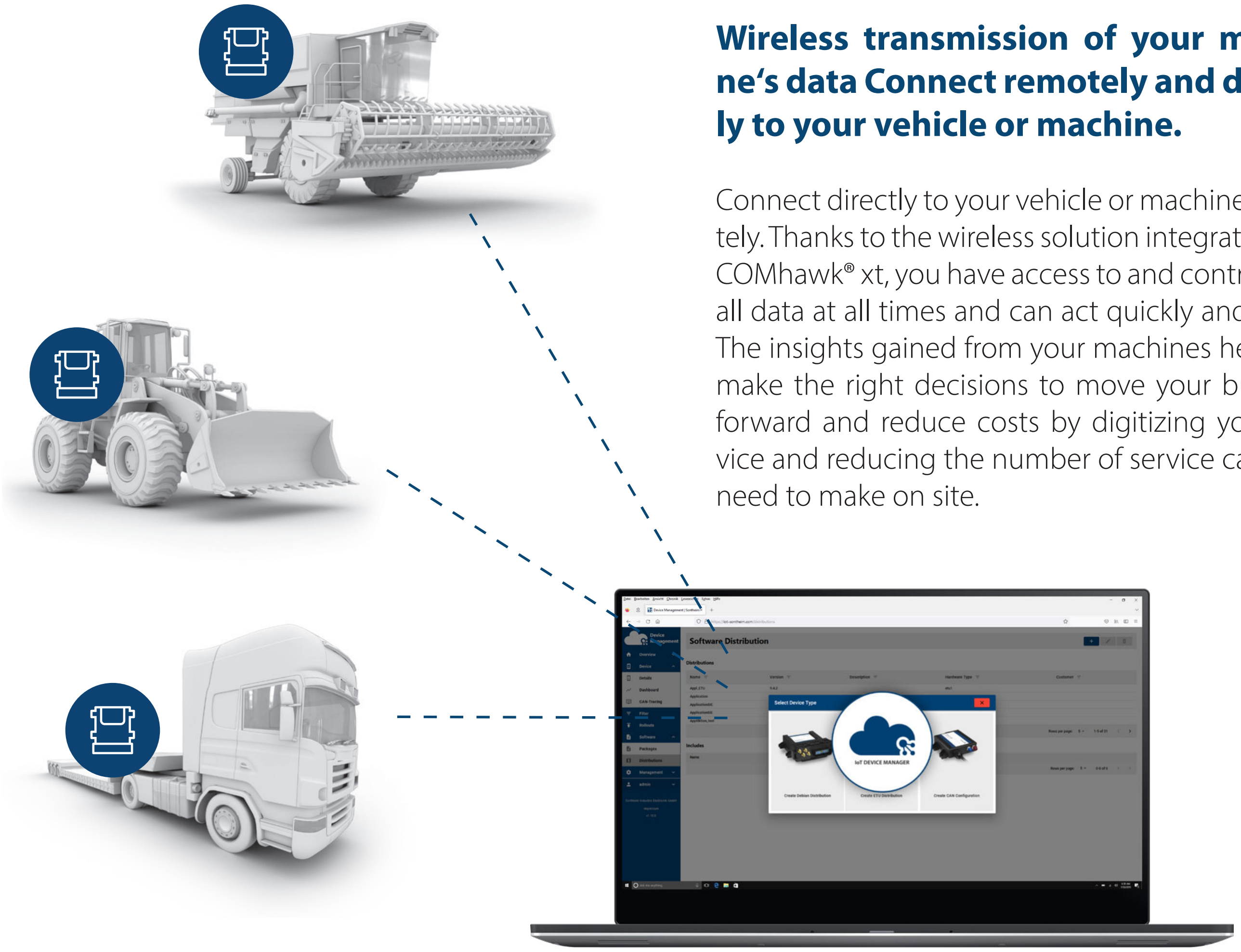


* Graph shows speed and temperature

COMMUNICATIONS SERVICE

Wireless transmission of your machine‘s data Connect remotely and directly to your vehicle or machine.

Connect directly to your vehicle or machine remotely. Thanks to the wireless solution integrated into COMhawk® xt, you have access to and control over all data at all times and can act quickly and easily. The insights gained from your machines help you make the right decisions to move your business forward and reduce costs by digitizing your service and reducing the number of service calls you need to make on site.



Integrated SIM card for worldwide use

The COMhawk® xt is equipped with a SIM card standard for mobile data transmission. You can conveniently customize the required data volume. The SIM card is activated for a wide range of countries.

Flash over the air update

Thanks to the Flash Over the Air (FOTA) update option, firmware, control units, and the IoT Manager are always up to date. Anomalies that restrict functionality can thus be rectified immediately and functionality enhancement updates can be scheduled at times when your machines are not in use.

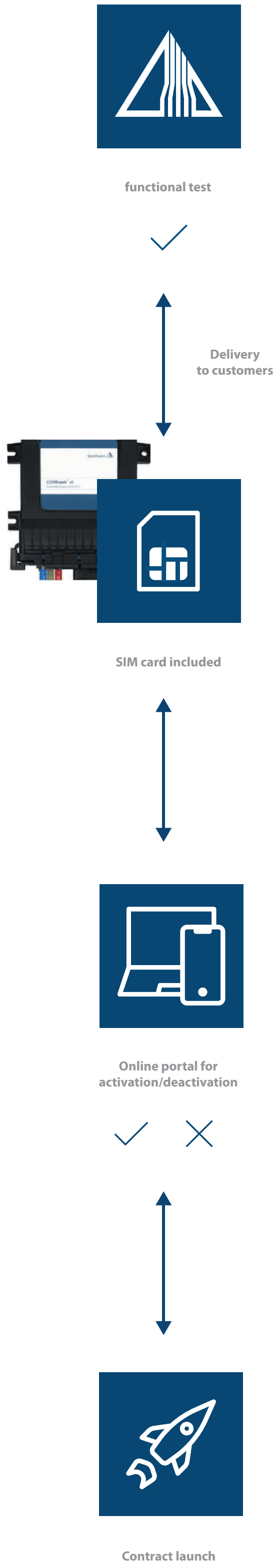
If necessary, updates can also be installed via a direct connection on site.

Mandatory functional test before delivery

Every COMhawk® xt is supplied with a working SIM card as standard. You decide which country zone and data volume the card should be equipped with. Before delivery, we test every COMhawk® xt telematics unit for functionality. The data volume required for this, approx. 20 kB, does not count towards your allowance. The test does not result in the card being ‘activated’ and incurring costs for you. If you wish, you can also choose your own SIM card provider.
(Additional costs may apply for this)

Easy management of SIM cards in the online portal

We provide you with an online portal for convenient management of your SIM cards. There you can activate and deactivate the cards. The contract period begins when the card is activated for the first time. Thanks to the online portal, you can keep track of the status of each individual SIM card at any time in a transparent and straightforward way. SIM cards that have not been activated six months after delivery will be invoiced even without activation. Unused data volume is automatically made available to other SIM cards in the same data package.

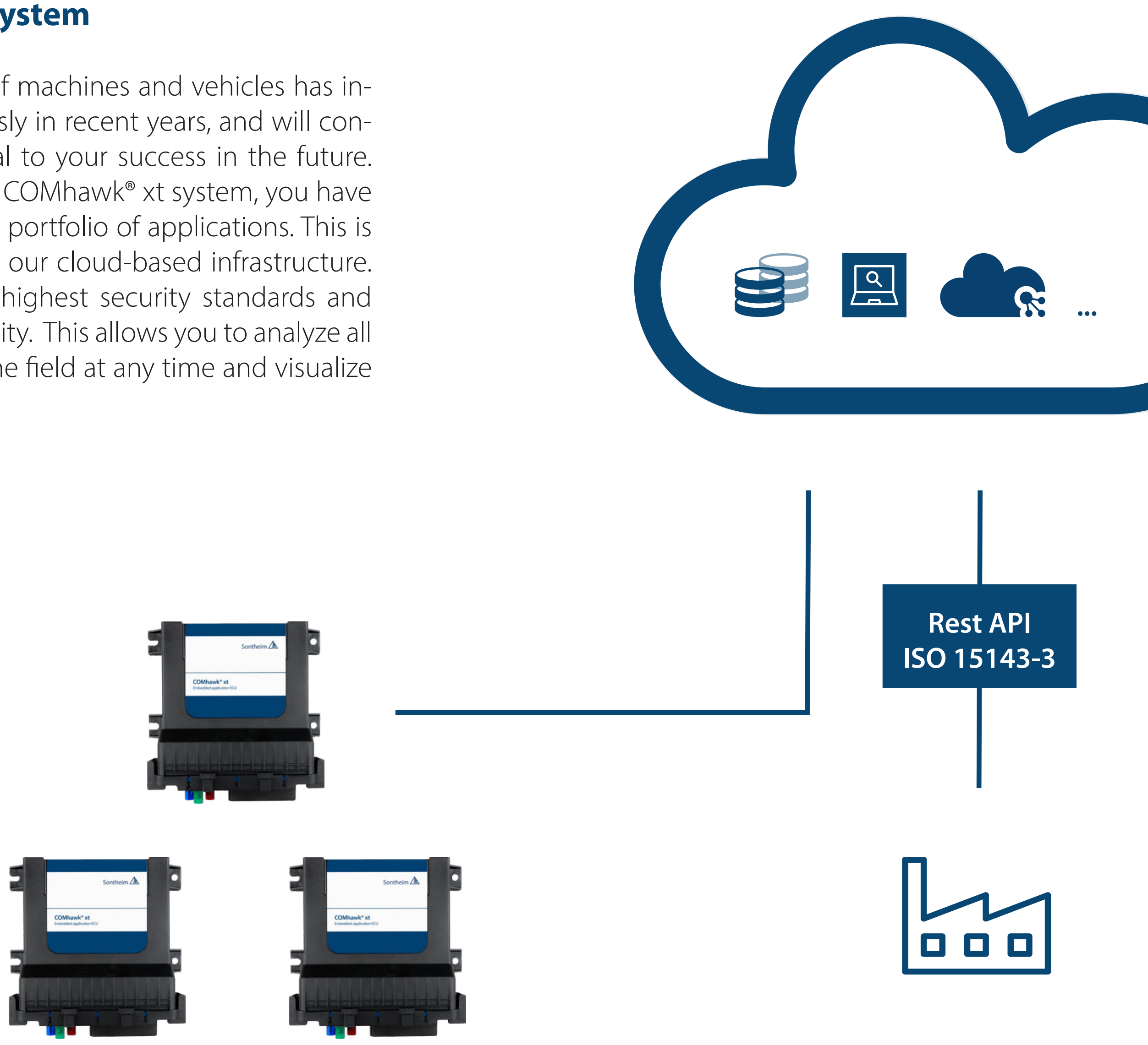


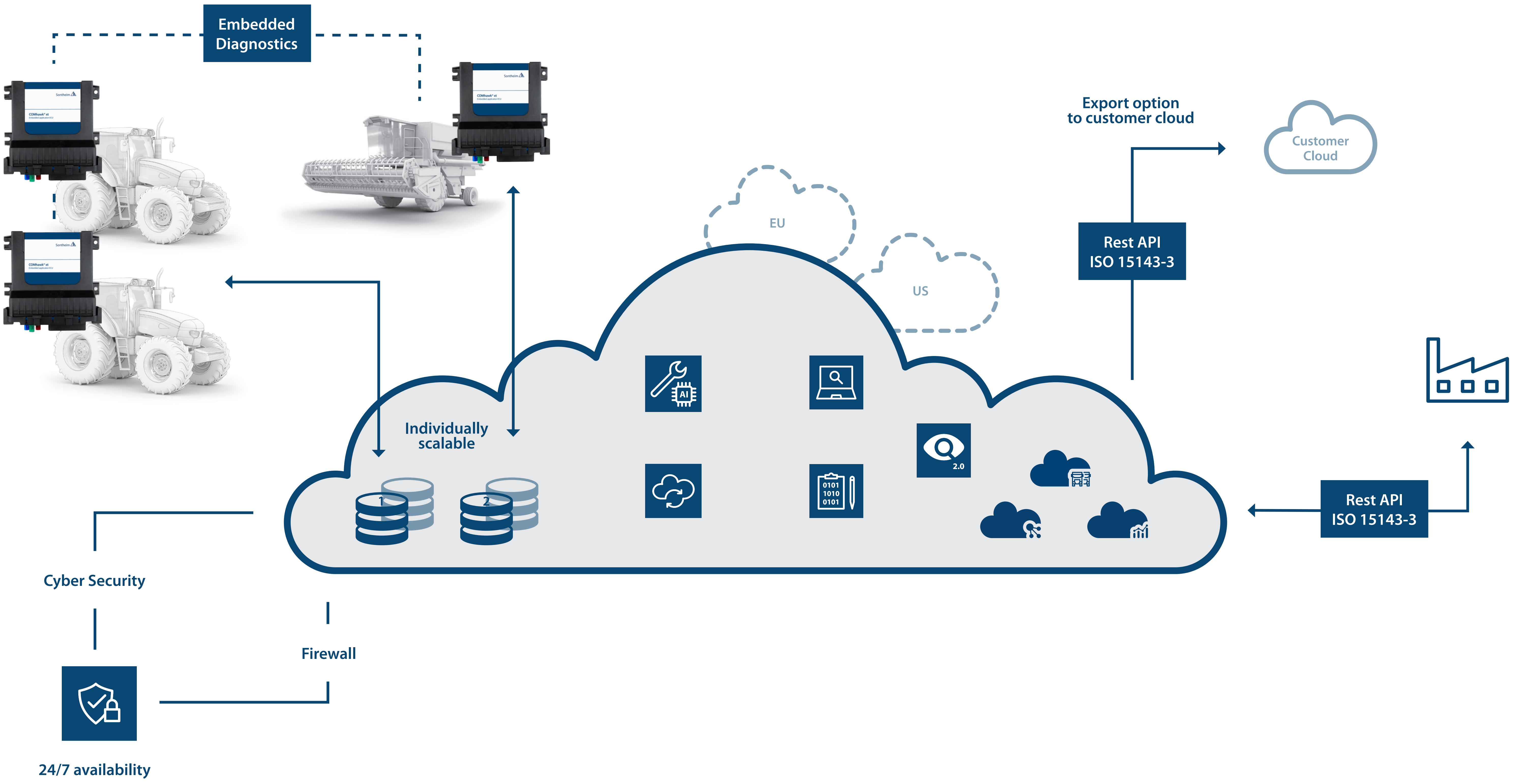
COMhawk® xt CLOUD

OVERVIEW

The cloud as a central element of the entire system

The networking of machines and vehicles has increased enormously in recent years, and will continue to be crucial to your success in the future. With the modular COMhawk® xt system, you have access to a whole portfolio of applications. This is made possible by our cloud-based infrastructure. Benefit from the highest security standards and maximum scalability. This allows you to analyze all your vehicles in the field at any time and visualize the relevant data.





Database

AI Predictive Maintenance

Remote Diagnostics

MDT 2.0

Fleet Manager

Cloud expansion

FOTA

Data Logger

Device Manager

Analytics Manager

DATA COLLECTION & COMMUNICATION

DIAGNOSTICS & ANALYSIS

MDT® 2.0 DIAGNOSTIC TOOL

Embedded Diagnostics
or optionally on a PC, mobile device, directly in the vehicle, or in the cloud.

Future-proof diagnostic tool chain – based on standards

The Modular Diagnostic Tool 2.0 (MDT® 2.0) is a standardized tool for accessing diagnostic data. It offers various options for creating, structuring, and executing diagnostic workflows based on the industry standard OTX (Open Test Sequence Exchange format) in accordance with ISO 13209. The ODX standard (Open Diagnostic Data Exchange) guarantees the re-usability of diagnostic services. In addition, MDT® 2.0 supports native RMI and offers the innovative ODW wizard (Sontheim OTX Diagnostic Wizard) which provides an extremely convenient simplification of OTX processing without violating the ISO standard.

Additional options thanks to the MDT® Service Cloud and Communication Lifecycle Manager 2.0

The MDT® Service Cloud enables secure data exchange for your diagnostic application. It has been integrated into the Modular Diagnostic Tool (MDT®) for even simpler and more effective diagnostics. An update tool can be used to download and install updates for the diagnostic application. In addition, specific data can be uploaded or downloaded from the diagnostic application. This means that session logs, vehicle file information, reports, HEX files, etc. can be easily loaded or saved in the cloud. The data formats and content to be transferred can be freely defined.

MDT® Authoring System
SiE Setup Tool
MDT® Service Cloud

CLCM
CLC Manager
ODX Editor

CE4
CANexplorer 4

Flash tools
End-of-line (EOL)

Protocol stacks

ECU
ECU flash and bootloader

MT-API
Multithread API

VCIs/CAN Interfaces

Web-based management of all fieldbus-based data

The CLCM 2.0 is the central system for Managing and creating diagnostic and communication descriptions of ECUs and entire vehicles. It is a client-server-based web application that enables multiple users to work together on a project. No client installation is required, and the server can be accessed from various platforms via a browser.
The CLCM 2.0 can be integrated into the existing infrastructure and development process. This allows it to optimally support all steps in the development of ECUs and vehicles.

KEY FEAUTURES

ODX ISO 22901-1 — ODX according to ISO 22901-1

OTX ISO 13209 — OTX according to ISO 13209

Multi-platform support

ISO — Supported standards: CANopen, SAE J2534, SAE J1939, ISO 15765 (KWP2000 on CAN), UDS, DoIP, …

Easy data exchange for your diagnostic application (uploads and downloads)

Management of session logs, vehicle file information, HEX files, reports, etc.

✓ Direct connection to an ERP system

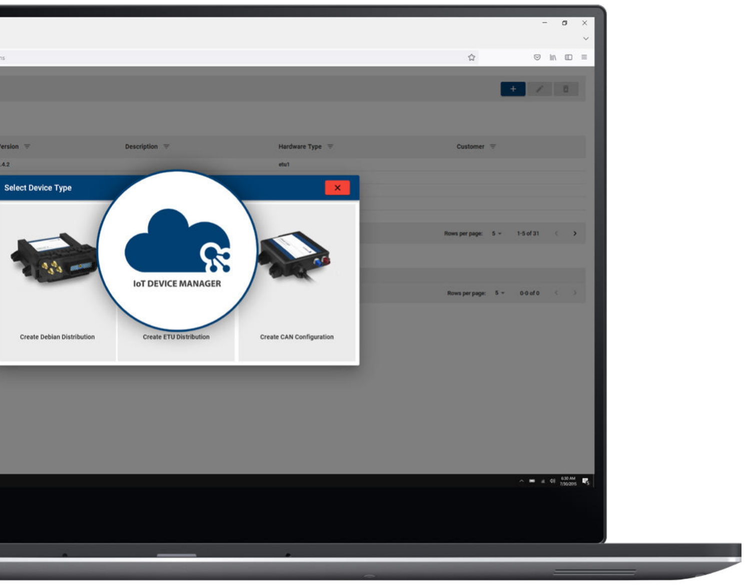
Management of all fieldbus-based data from specification to release

Development, mapping, and maintenance of communication interfaces for ECUs

Description of the entire data flow between ECUs and within the ECU itself

IOT DEVICE MANAGER

The IoT Device Manager is a prerequisite for using the IoT Analytics Manager and the IoT Fleet Manager.



KEY FEAUTURES

- Management of all telematics units
- Live data monitoring
- Rapid data usage analyses
- Simple configuration of all devices
- Management of over-the-air updates
- Drag and drop functionality

The IoT Device Manager is a cloud-based tool for simple and clear Management of your telematics units in the field.

You can group and structure your devices using drag and drop and manage software packages for wireless over-the-air updates.

Collect live data during vehicle Operation or flash:

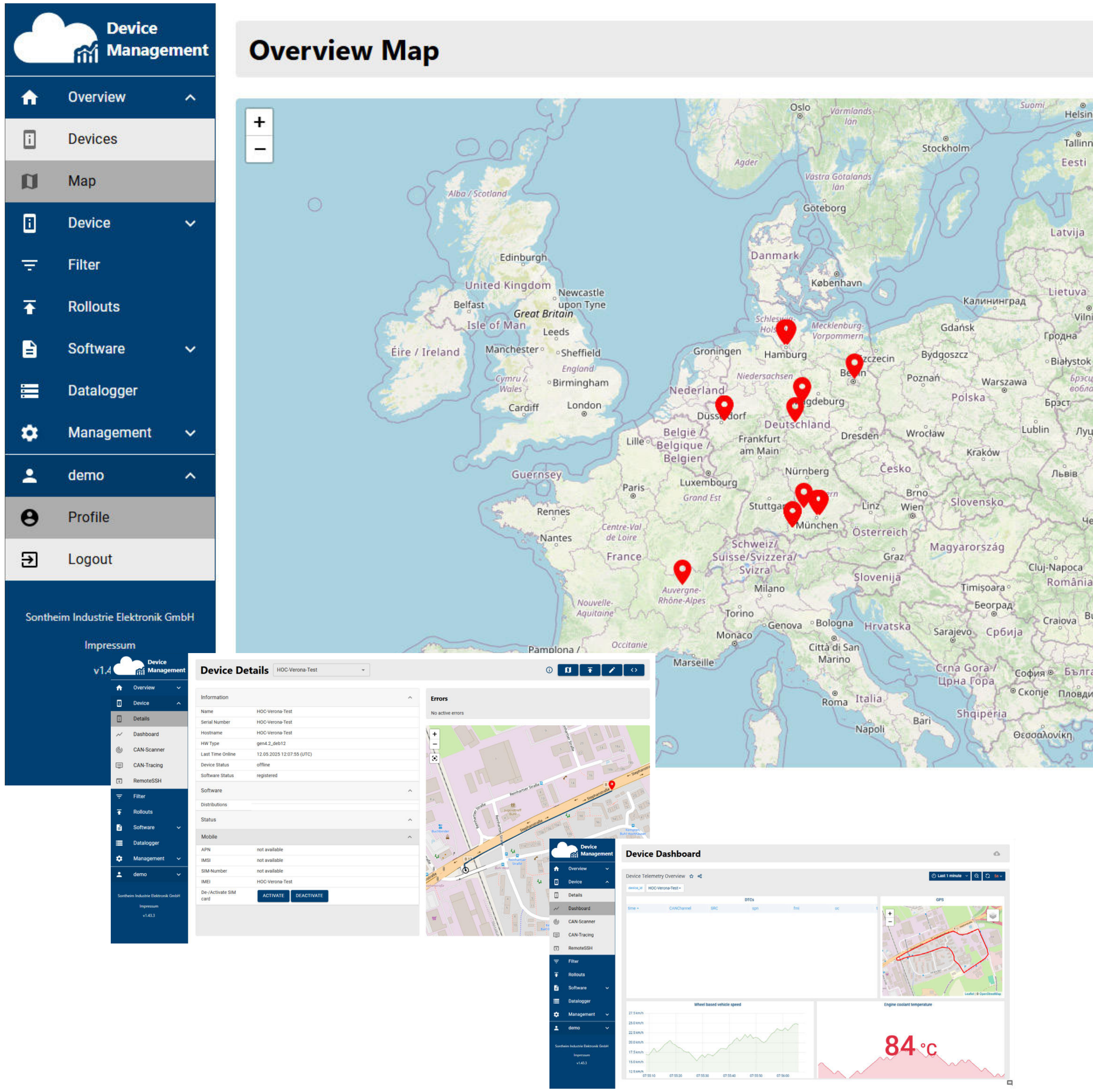
» Mobile networks (4G/LTE/2G)
» Wi-Fi

Store telemetry data for further analysis and support the following functions:

» QA statistics
» Usage statistics
» Planning of service intervals
» Vehicle lifecycle support

Save telemetry data and check Information such as:

» SIM card number (IMSI)
» Serial number of the LTE device
» Last connection to the server
» Signal quality
» Network bandwidth
» Device configuration



*Screenshot from the Sontheim IoT Analytics Manager

IOT ANALYTICS MANAGER

Cloud-based platform for data visualisation and analysis

The IoT Analytics Manager is a cloud-based tool for storing and visualizing your operating data (big data). OEM data can be analyzed and evaluated in various configurable dashboards, Widgets and histograms. The data volume and data traffic can be individually adjusted for different use cases. In addition, live data integration for real-time Monitoring is possible and can be configured individually.

The IoT Analytics Manager can be hosted on a server on the Sontheim side or seamlessly integrated into an existing customer infrastructure. Secure data transfer is ensured thanks to SSL/TLS certification and can also be expanded according to individual customer requirements. The IoT Analytics Manager can be branded specifically for OEMs. This gives the user the option of creating different user levels to enable viewing with different rights or simple integration of sub-supplier views.

KEY FEAUTURES

- Analysis and evaluation charts
- Storage and visualisation of device and vehicle data
- Drag and drop functionality
- Live data monitoring
- Configurable dashboards, widgets, and histograms
- Individual configuration

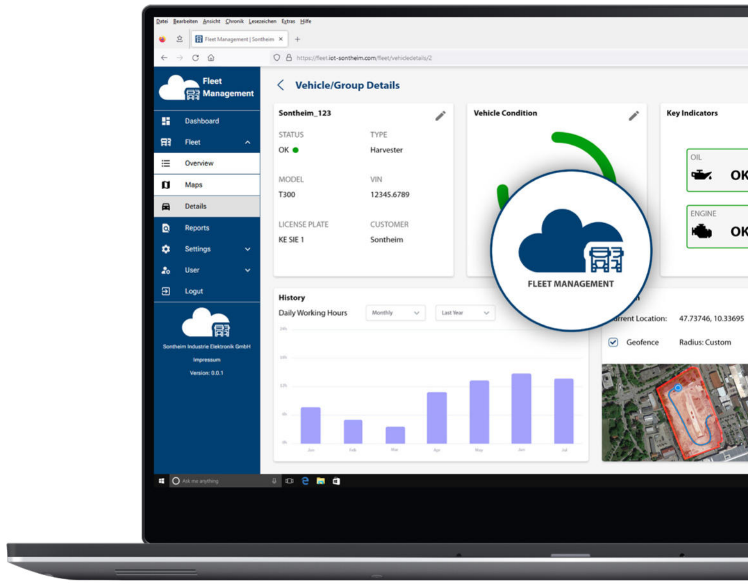
IOT FLEET MANAGER

Modern fleet management with vehicle tracking

Complementing the IoT Device and IoT Analytics Manager, the IoT Fleet Manager focuses on individual vehicles or customized vehicle groups. This enables modern fleet management, e.g. for specialist dealers, workshops, or vehicle rental providers. Seamless integration with the IoT Device and IoT Analytics Manager is guaranteed throughout thanks to the modular approach.

API standardized in accordance with ISO 15143.3. The modern authorization management – at user or role level – also allows the administration of small units, so that each user only sees the content that is relevant to them.

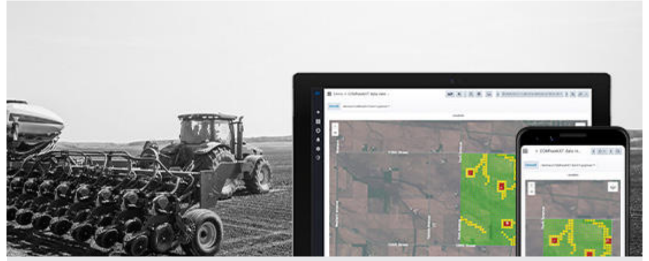
With the help of the IoT Fleet Manager, the digital vehicle file can be kept in view at all times.
From route documentation, real-time GPS tracking, and geofencing, to the management of service Appointments or the detection of faults and warning messages – including user-defined warning messages are available. All data can be visualized in individually configurable dashboards with various widgets such as diagrams, GPS maps, or overview tables. The IoT Fleet Manager also offers extensive options for uploading your own documents. Extended data retrieval is possible via a programming interface. The IoT Fleet Manager is available as a standalone solution or can be integrated into other systems.



KEY FEAUTURES

- Extension for specialist dealers and workshops
- Storage and visualisation of device and vehicle data
- Management of individual vehicles or vehicle groups
- Live data monitoring
- Customisable user interface with personalisation options
- Easy management of user rights

CASE STUDIES



Precision Farming

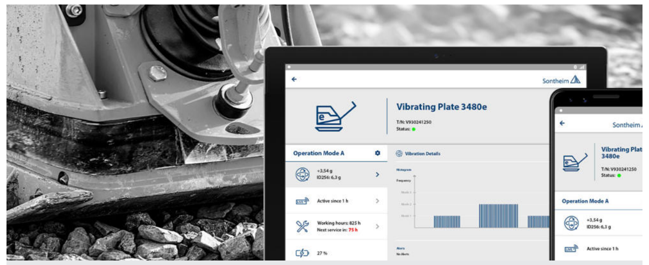
The COMhawk® xt in use on agricultural land. In the case study, it collects data and visualises it on various end devices in order to cultivate farmland precisely and with maximum yield.

Real-time analysis and FOTA

The COMhawk® xt in use on agricultural land. In the case study, it collects data and visualises it on various end devices in order to cultivate farmland precisely and with maximum yield. The IoT Device Manager and IoT Analytics Manager help to optimise processes by visualising and evaluating machine data in real time. The ability to perform over-the-air updates (FOTA) also creates real added value for customers.

Bus fleet manager

The COMhawk® xt provides valuable data on the existing fleet for the research Project at Kempten University of Applied Sciences, such as movement profiles, measurements and the number of passengers transported, so that after evaluating the data, the fleet can be converted to electric drive in the future. The COMhawk® xt provides valuable data on the existing fleet for the research project.

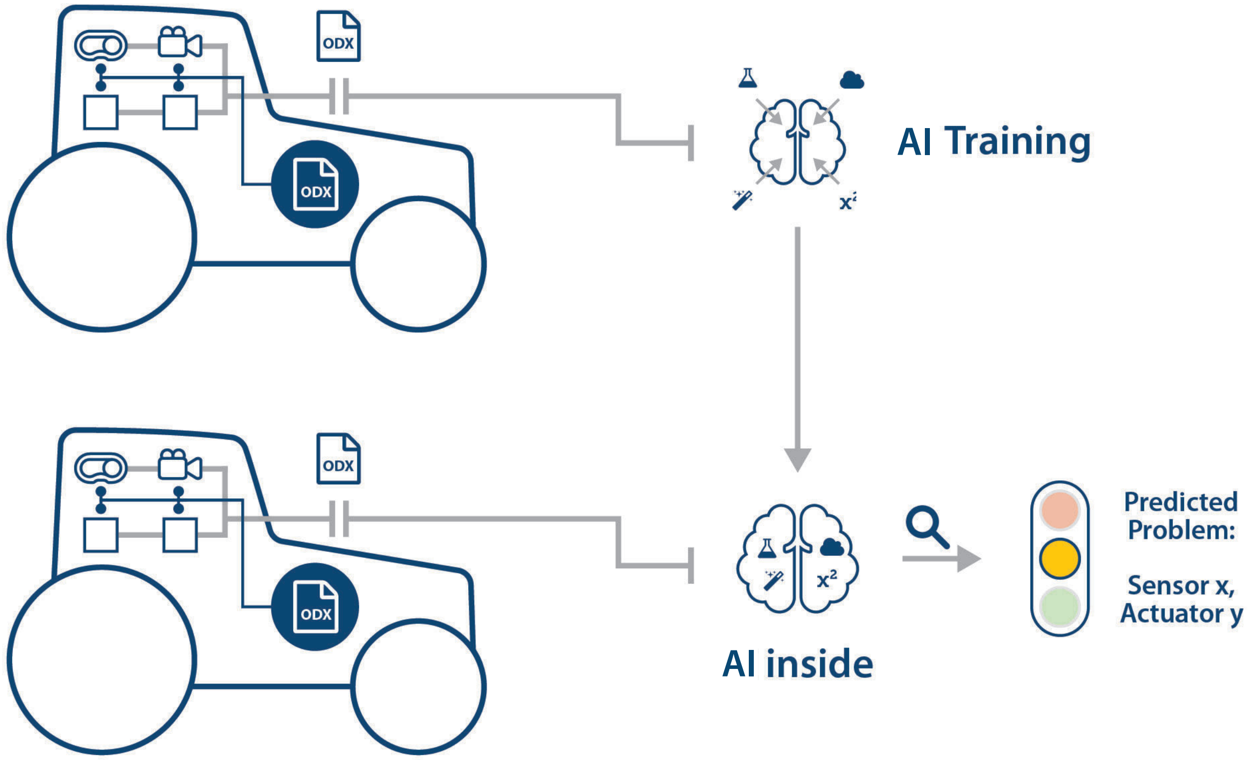


Beacon BT module in 24/7 operation

Count operating hours, measure vibrations and shocks, and document any unusual deviations. The low-energy BT module collects data 24/7 and allows conclusions to be drawn about the condition of rental equipment and machines in daily use. Precisely visualized on the corresponding end devices.

FUTURE DEVELOPMENTS

Condition monitoring / Predictive maintenance / AI-based AI Training



CASE STUDIES:

CYBER SECURITY

Security Lifecycle Management – Security across the entire supply chain

Cybersecurity is much more than just protecting your machines. When implemented in a targeted manner, it creates a clear and tangible competitive advantage. It brings clarity and reliability through future-proof and legally compliant solutions.

Below, we provide you with an overview of the key regulations and Show how we can support you in meeting the challenges so that you, as an OEM, can implement the regulations in practice.

Security by Design – Security as a central component of the development process

The integration of security aspects into all phases of hardware and software development is at the heart of our Security by Design concept. Consistent and comprehensive security thinking in all phases of the product life cycle. From the initial idea to the end of life.

By considering security aspects at an early stage, we ensure that the occurrence of vulnerabilities is reduced to a minimum later in the life cycle. Regular (penetration) tests and the implementation of mitigation strategies for digital products ensure maximum security until the end of the product's life cycle.
At the same time, the Security by Design approach forms the basis for responding quickly and easily to new threat scenarios, changing legal requirements or any gaps identified during vulnerability monitoring.

What machine manufacturers must guarantee in future:

Manufacturers must also check existing products for compliance with regulatory requirements. For new developments, 'security by design' must be firmly integrated into the development process. Security measures must accompany the process throughout the entire life cycle of the machine.
In addition, continuous testing (including penetration tests) is required for digital products in order to identify existing security gaps and implement appropriate countermeasures. Effective strategies for dealing with damage must also be developed.

With increasing regulations that tighten cybersecurity requirements for manufacturers of machines and devices, it is essential to build up the relevant expertise and hire or provide targeted training for cybersecurity specialists. The requirements demand a considerable investment of resources, but are unavoidable for the future viability of modern machines.

UNECE R155

(Effective date: 01/2021 – Mandatory from 07/2022)

» EU Regulation R155 regulates the security of automotive electronic systems with regard to cyber security.
» It requires systematic cyber security processes, continuous risk and vulnerability analyses, omprehensive security measures throughout the life cycle, and vidence of vehicle cyber security.

RED-DA: Radio Equipment Directive Delegated Act 2022/30

(Effective date: 10/2021 – Mandatory from 08/2025)

» Applies to manufacturers of products with radio interfaces.
» Applies to devices that communicate via Wi-Fi, mobile communications or Bluetooth, such as telemetry devices, but also to products that can communicate with the internet via a third-party device.
» Relevant standard: EN 18031 Cybersecurity for radio equipment.

EU Regulation 2019/2144

(Effective date: 01/2020 – Mandatory from 07/2022)

» Sets out administrative provisions and technical requirements for the type approval of new vehicles, systems and components in the EU area.
» Describes the risks of 'over-the-air updates' and defines binding application definitions to enable secure software updates and prevent unauthorised remote Access to vehicle data.

MVO: EU Machinery Regulation (EU) 2023/1230

(Effective date: 11/2024 – Mandatory from 01/2027)

» Affects manufacturers, importers and distributors – Applies across all EU countries.
» Covers both hardware and software.
» Machinery and control systems must be protected against hacker attacks
» Obligation to provide evidence of software attacks and modifications.

CRA: Cyber Resilience Act (EU) 2024/2847

(Effective date: 11/2024 – Mandatory from 12/2027)

» Combines RED-DA and MVO with regard to cybersecurity. Applies to all hardware and software with 'digital elements/components'.
» Cybersecurity must be taken into account throughout the entire product life cycle. Security updates for at least 5 years.
» Mandatory reporting of vulnerabilities and incidents.

CYBER SECURITY

How we can support you:

Initiation phase / Joint exchange

The aim is to determine requirements and document the current situation in a joint exchange. The initiation phase lays the foundation for successful collaboration. It can take the form of an on-site or off-site meeting, or a short workshop. Following the initiation phase, a transparent offer and a project roadmap can be drawn up. Our team of experts is on hand to provide support with their specialist knowledge right from the initiation phase.

Security Risk Analysis (TARA)

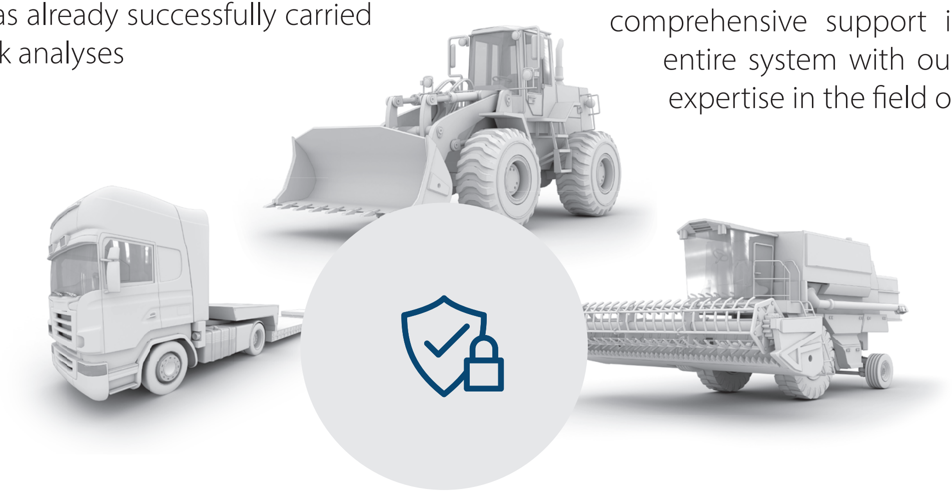
With the TARA threat and risk analysis, we identify potential threats and vulnerabilities for individual components or an entire system. As part of the analysis, the possible effects of attacks are evaluated and the potential damage to various user groups is assessed. After prioritisation based on probability and potential damage, potential countermeasures can then be developed and implemented, and monitoring measures can be defined.

The TARA risk analysis is a customised measure that is carried out explicitly for your circumstances. You benefit from the experience of our team of experts, which has already successfully carried out numerous risk analyses

Penetration testing & regular vulnerability scanning

Early detection of security gaps through continuous monitoring and Penetration testing of systems. If security risks arise during your tests – which are related to the hardware and/or software we use – our Product Security Incidence Response Team (PSIRT) is your competent point of contact. As part of regular vulnerability scans, our systems and components are regularly subjected to intensive testing.

The aim is to discover vulnerabilities and close them immediately in order to ensure maximum security. The PSIRT team also provides comprehensive support in securing the entire system with our many years of expertise in the field of cyber security.



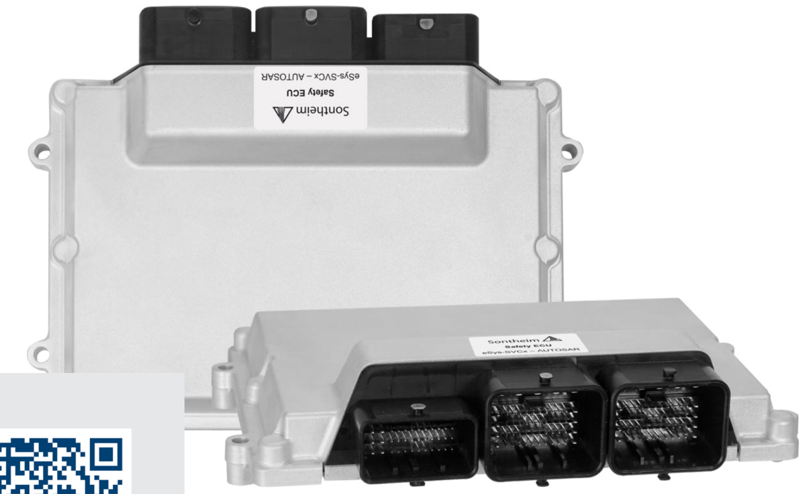
Best practice example – Development of our ASIL-C control unit with AUTOSAR

for a well-known manufacturer. The control unit is intended for use in vehicles in accordance with ISO 26262.

The system controls x-by-wire systems and is intended as a platform for control Systems in conjunction with appropriate safety requirements. The safety ECU is scalable and has approval as a generic control unit.

In addition, Sontheim supplies software in accordance with AUTOSAR-compliant specifications.

The Software platform enables the rapid development of application software in accordance with functional safety-related aspects. The control system achieves a safety Level in accordance with ISO 26262 ASIL-C and is TÜV-certified accordingly.



TO THE TECHNICAL ARTICLE HANSER AUTOMOTIVE:

TECHNICAL DATA

CPU	32-Bit microcontroller, Cortex-A9 (single/dual core)
RAM	512 MB DDR3 RAM (opt. up to 1 GB)
Flash Storage	16 GB eMMC NAND Flash (opt. up to 64 GB)
CAN	4× CAN according ISO 11898
Ethernet	1× Ethernet, 10/100 Mbit/s
Wi-Fi	1× IEEE 802.11 b/g/n; Client- and Accesspoint-modus (FAKRA E green)
GNSS	GPS/GLONASS, Beidou (FAKRA C blue)
2G/LTE	LTE CAT4 (FAKRA D purple)
IOs	4× DI, 1× DO (500 mA)
RTC	With 2 weeks buffering
Connector	30-pol. Automotive plug
Antenna Connector	external; 3× FAKRA (opt. SMA)
Operating system	Linux
Housing	IP67
Dimensions (l×b×h)	ca. 130 mm × 124 mm × 38 mm
Weight (l×b×h)	ca. 375 g
Operating Temperature	-20 °C to +70 °C (higher temperature class on request possible)
Storage Temperature	-40 °C to +85 °C
Power Supply	6-32 V DC, incl. Load Dump Protection
SIM card	Inclusive Sontheim SIM card
Country Approvals	multiple country approvals worldwide - Full list on Site 32/33
Safety Standards	ECE R10, ECE R155 ready, ECE R156 - planned

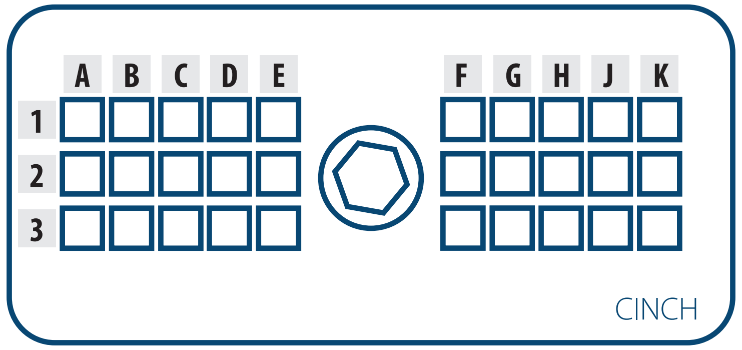
RF SPECIFICATION

technologies	Max. power [dBm] Performed	Antenna gain max.: [dBi]
E GPRS 900 MHz	33dBm±2dB	0.03
E GPRS 1800 MHz	30dBm±2dB	3.12
LTE FDD 1 1950 MHz	23dBm±2dB	2.17
LTE FDD 3 1800 MHz	23dBm±2dB	3.12
LTE FDD 7 2600 MHz	23dBm±2dB	3.2
LTE FDD 8 900 MHz	23dBm±2dB	0.03
LTE FDD 28 700 MHz	23dBm±2dB	1.57
LTE FDD 40 2300 MHz	2G23dBm±2dB	3.52
Wi-Fi 2450 MHz	15.0	3.0

technologies	Max. power [dBm] Output	Antenna gain max.: [dBi]
E GPRS 850 MHz	31dBm±2dB	
E GPRS 1900 MHz	28dBm±2dB	
LTE FDD 2 1900 MHz	23dBm±2dB	1.87
LTE FDD 4 1750 MHz	23dBm±2dB	3.12
LTE FDD 5 850 MHz	23dBm±2dB	0.91
LTE FDD 12 700 MHz	23dBm±2dB	0.95
LTE FDD 13 700 MHz	21dBm±2dB	2.23
LTE FDD 25 1900 MHz	23dBm±2dB	1.87
LTE FDD 26 850 MHz	23dBm±2dB	0.91
LTE TDD 41 (38) 2600 MHz *	22dBm±2dB	2.90
LTE FDD 66 2150 MHz	23dBm±2dB	3.12
Wi-Fi 2450 MHz	15.0	3.0

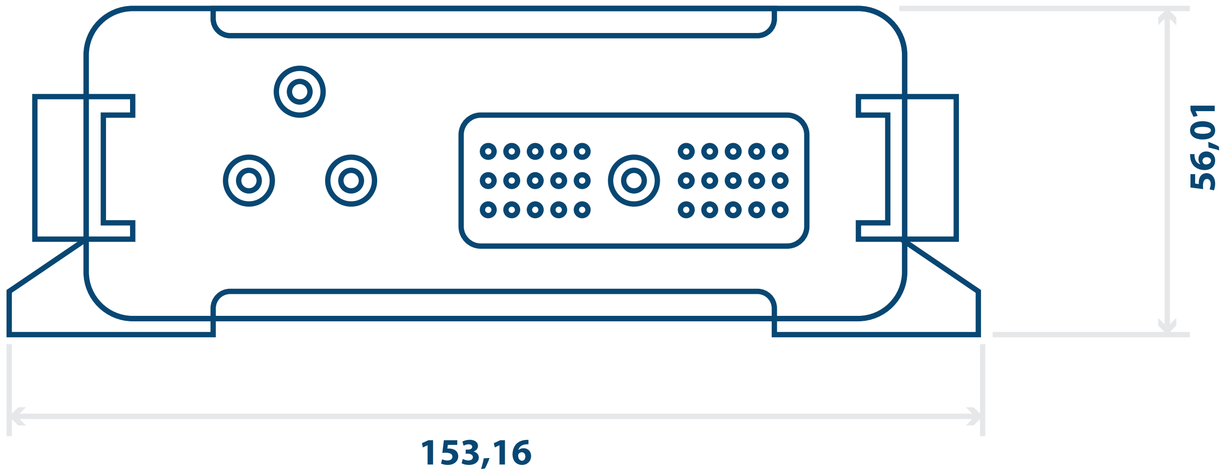
* Canada only: Volume 38 is used instead of Volume 41.

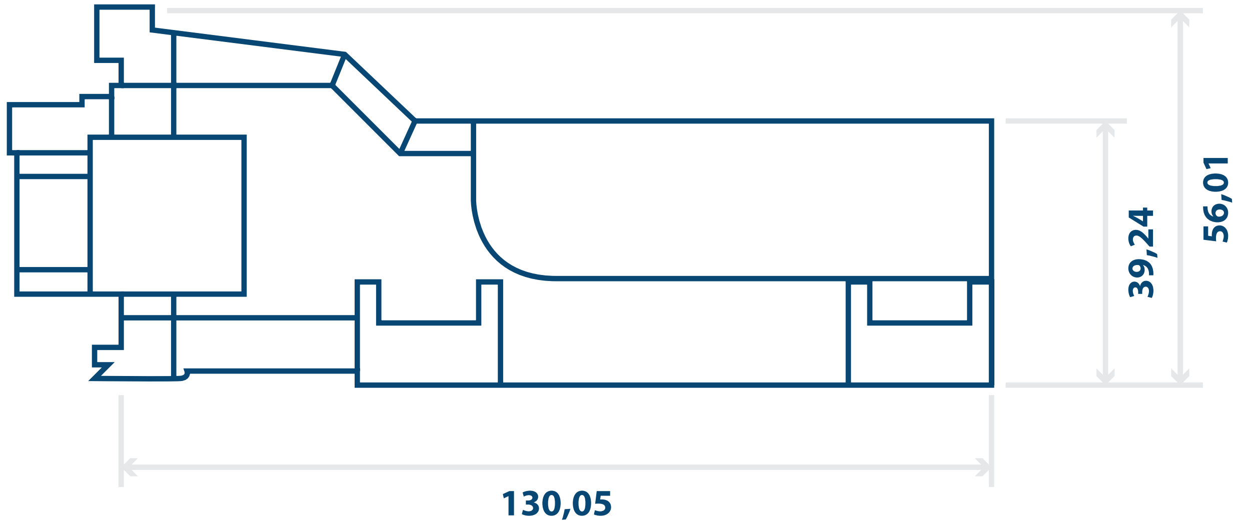
TECHNICAL DATA



PIN ASSIGNMENT

1A	LAN_RX-	**1F**	ANAIN0
1B	LAN_TX-	**1G**	ANAIN1
1C	CAN3_high	**1H**	ANAIN2
1D	CAN3_low	**1J**	ANAIN3
1E	LIN	**1K**	KL30
2A	LAN_RX-	**2F**	ANAIN4
2B	LAN_TX-	**2G**	ANAIN5
2C	CAN1_high	**2H**	ANAIN6
2D	CAN1_low	**2J**	ANAIN7
2E	KL15	**2K**	KL31
3A	CAN0_high	**3F**	OUT0
3B	CAN0_low	**3G**	OUT1
3C	CAN2_high	**3H**	SIGNAL 1
3D	CAN2_low	**3J**	SIGNAL 0
3E	TP	**3K**	Analog Ground





***all dimensions in millimetres**

COUNTRY APPROVALS

EUROPE

Andorra	✓
Albania	✓
Austria	✓
Belarus *	✓
Belgium	✓
Bosnia and Herzegovina	✓
Bulgaria	✓
Croatia	✓
Cyprus	✓
Czech Republic	✓
Denmark	✓
Estonia	✓
Finland	✓
France	✓
Germany	✓
Georgia	✓
Gibraltar	✓
Greece	✓
Greenland	✓
Hungary	✓
Iceland	✓
Ireland	✓
Italy	✓
Kazakhstan *	✓
Latvia	✓
Liechtenstein	✓
Lithuania	✓
Luxembourg	✓
Malta	✓
Monaco	✓
Netherlands	✓
Norway	✓
Poland	✓
Portugal	✓
Romania	✓
San Marino	✓
Serbia	✓
Slovakia	✓
Slovenia	✓
Spain	✓
Sweden	✓
Switzerland	✓
Great Britain/ Northern Ireland	✓
Turkey	✓
UK Guernsey	✓
UK Isle of Man	✓
UK Jersey	✓
Vatican City	✓

* until 22 June 2027

AMERICAS

Canada	✓
United States of America	✓
Dominican Republic	✓
Chile	✓
Peru	✓
Uruguay *	✓

ASIA

Japan	✓
Thailand	✓

AUSTRALIA

Australia	✓
New Zealand	✓

* until 8 June 2037

TEMPORARILY DEACTIVATED

(Activation with time delay possible again!)

- Israel
- Saudi Arabia
- United Arab Emirates

Further country approvals required?

In addition to the existing country approvals, further approvals can be applied for. The process takes approximately three months to complete. Costs on request (depending on the desired country).

FAQ

Question	Answer
Must the SIM provider offered be used?	The provider can be changed upon request. However, it should be noted that this may incur one-off costs for the changeover (up to 50k euros).
Is it possible to run self-developed software on the COMhawk® xt in parallel with the Sontheim software?	Yes, this is possible. Linux (DEBIAN) is required for this. We recommend attending a relevant workshop with us beforehand.
How often are anomalies corrected?	Serious errors are fixed immediately. Minor bug fixes or product enhancements approximately every six months after Prior notification by email.
How long is the product life cycle of the COMhawk® xt?	The product life cycle of the current Generation is seven years. The COMhawk® xt will continue to be manufactured for a maximum of 1.5 years after the end of the product life cycle. After that, cybersecurity can no longer be guaranteed.
Is there such a thing as obsolescence management?	Yes, we have obsolescence management. This involves periodic Monitoring of all components.
Does Sontheim offer technical support or is there a support portal?	Sontheim provides its own support portal. Technical support is provided by at least three employees. The support portal is available 24 hours a day, 7 days a week.
Is there a guarantee of subsequent delivery of spare parts after the series has been discontinued?	We agree individual delivery guarantees with each customer.

Mobile Automation

Industrial Automation

Diagnostics

Connectivity

We look forward to receiving your enquiry!

Sontheim Industrie Elektronik GmbH

Georg-Krug-Straße 2
D-87437 Kempten

Phone:	+49 (0) 831 575900-0
Email:	info@s-i-e.de

Sontheim Electronic Systems L.P.

201 West 2nd Street
Davenport, IA 52801, USA

Phone:	+1 563 888 1471
Email:	info@sontheim-esys.com

www.s-i-e.de