designed
developed
made
in Germany

sematicon
INDUSTRIAL IT SECURITY

se.MIS™

compliant to IEC-62443

Maintenance management and "Zero-Trust" remote access for industrial and control systems

sematicon

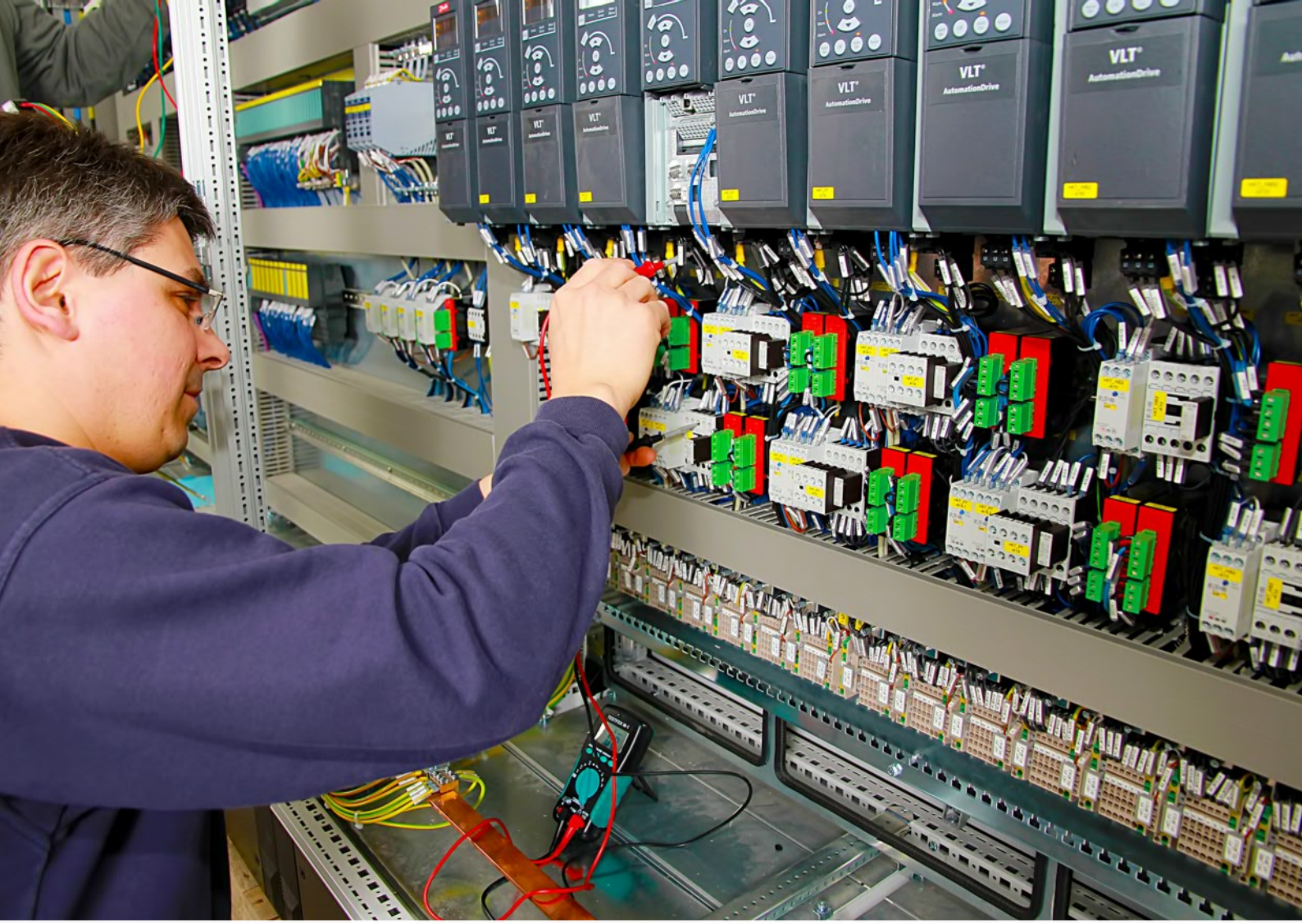
About us

sematicon AG is a Munich-based company focusing on information security and cryptography in industry, electrical engineering as well as IIoT environments.

We share years of experience in these areas and open new horizons, breaking with a dogma from the IT security industry: **security does not always have to be complicated**. User-friendliness and system security are our top priorities and do not exclude each other.

Our specialised and highly motivated team meets the current challenges of **Industry 4.0**. The solutions we develop allow secure access to industrial plants and at the same time ensure **integrity**, **authenticity** and **security** of digital data and processes. Our innovative solutions are still **unique on the market** at the moment.

We are your reliable partner and innovator in all matters and projects relating to a secure Industry 4.0 "**Made in Germany**".



Industrial automation in the age of Industry 4.0

In the past years, **digital transformation** has caused a significant change in the IT market landscape. Although many exciting possibilities in networking and digitisation turn up, there are also new challenges to deal with. One of these is certainly how to ensure the **security** and **authenticity** of all digital data and processes.

Digital transformation and new technologies gain more and more importance in industrial and manufacturing operations, too. Not only machine and production plants, but also numerous industrial businesses become increasingly part of a digitally-linked world.

We are currently facing a situation of radical change, in which digital control systems and automation technology become prominent. However, the existing concepts and strategies of the IT environment cannot be transferred to the industry environment so easily. IT systems are depreciated on average over three to five years, whereas industrial plants are amortised on a completely different scale. Systems often continue to operate even if their anticipated lifetime or the implemented software's support period have ended by then.

Installing updates necessary to maintain security in a digital world is already problematic during the system's lifetime - mainly because of the built-in proprietary software or incompatible hardware.

sematicon

Digital maintenance book and "Zero-Trust" remote access

Secure and reproducible access to assets

On the one hand it is a well-known fact that the majority of industrial systems are not kept up to the latest software standards by means of security updates. On the other side, even **legitimate product features** may present **a security risk**, if they are disregarded when planning a comprehensive industrial **security concept**.

Considerable threats in network environments may occur, leading to a tense relationship between IT and industry. The focus of the IT is to securely connect the systems to the network, whereas the industry is predominantly looking at the systems' end-to-end functionality. The situation is not easily manageable for both sides.

se.MIS™ has been developed in close collaboration with various industrial partners and their individual machine parks. Thus, the industry's concrete goals and expectations have been and still are centre stage at all times.

Our solution aims at securing and integrating the central control systems based on state-of-the-art IT standards - without changing these when new software or updates have to be added.

Our design criteria:

Zero-Trust - access to the machines is based on the principle „Zero-Trust“ in accordance with the recommendation of the BSI (German Federal Office for Information Security), stating that the following aspects must be taken into account when accessing an industrial machine:

Separation of responsibilities - this principle defines the idea that no person or device shall have comprehensive admission to all relevant and critical IT sources of a company.

Access with the least privileges - by applying this principle, only absolutely necessary rights are assigned to each admittance to the system. There is no point for a technician in having the whole control system at his disposal, when he only needs graphical access to the HMI-display, for example.

Micro-segmentation - the OT environment is divided into security zones. For each and every access to one of these security zones, another form of authentication is required.

Multi-factor authentication - this means that in addition to „knowledge“ (password), a „possession“ (one-time-password token or mobile-phone app) is required for the log-in.

„Just-in-Time“ access - a user is never granted permanent admission to a resource, but only for the time period needed to solve a specific problem.

Audit and tracking - all transactions and changes are precisely documented.

Full isolation of any access - the maximum protection of the system against any malware is ensured. In addition, this principle significantly reduces the attack vector for zero-day-attacks.

In contrast to classic VPN solutions, **se.MIS™** works in line with all recommendations of the BSI. Especially in industrial environments, VPN is regarded to be insecure because it connects the external technician using a "virtual network cable" directly to the network port of the machine. Our solution not only prevents the direct IP-access, but also fully records all system changes in the **digital maintenance book**.

This maintenance book and the maintenance planning are responsible for manual and automatic protocols. These include not only the recordings of screen sessions on video and network traces (PCAP-files) for IP-based sessions, but also the complete SPS-software with the support of the optional feature PLC-guard.

All the necessary information about the plant, the assigned technician and the required authorisations needed to access the plant are collected in the maintenance book. No matter whether a maintenance date takes place as scheduled or ad-hoc, the correct authorisation on the machine is ensured.

In particular the transfer and handling of external files pose a significant threat to industrial plants. It is often not possible to run a virus scanner. Apart from the permanent documentation and archiving of transferred files into the maintenance book, they can also be centrally checked through **se.MIS™** by third parties.

Any virus or content scanner used for this purpose is not part of the solution and can be chosen by the customer in accordance with their individual requirements and interfaces. A direct transfer is also excluded here, as all uploads are managed by the maintenance book.

se.MIS™ assists our customers to always keep the requirements of the **IEC-62443** directive in mind and therefore facilitates a potential future certification as best as possible.

se.MIS™ facilitates …

…the self-determination of IT and industry

IT and control system applications define different requirements of users and their rights. Classic IT users can be integrated via ActiveDirectory. Technicians and their authorisations in other directories or in the local database can be amended in order to ensure their autonomous management.

…the support of old and modern systems

No matter if old or new: support is available both for older systems, like MS-DOS or Windows CE, and for current operating systems and applications. Because of this flexibility, not only plants to be maintained, but also file servers, IT systems and other modern IT components from external locations can be integrated.

…a comprehensive audit

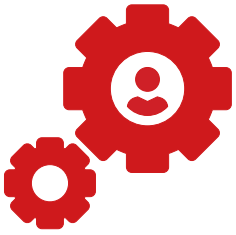
The digital maintenance book is key: all changes and every access are documented mandatorily, archived and can be reproduced and reviewed precisely at any time. An entry in the maintenance book is added automatically for all tasks and can be edited at your discretion. If necessary, it is also possible to record whole sessions.

…access for planning and control

A sophisticated planning tool ensures that a connection can only be made at a predefined point of time. The system "knows" when to allow or to deny access automatically. The planning tool and the digital maintenance book are independent from each other. This enables a technician to obtain comprehensive information about the machine before starting a task.

…most modern and highest security standards

Connections to the system as well as data are protected cryptographically against manipulation and unauthorised access. The most modern IT security guidelines have been applied. The encryption of data and connections and the requirements of the IEC-62443 directive are taken into account as well as a secure login using a one-time password (OTP).



…easy installation, integration and operation

When designing the solution, special emphasis was placed on simple operation and integration. Every user can set-up the solution on the spot. There is no need for extensive expert knowledge. The intuitive administration interface and a sophisticated automatism in the background minimise complexity significantly.

sematicon

Solution overview

Flexibility through a modular system without hardware

The **se.MIS™ Manager** is the heart of the solution and where the user interaction takes place. The system may be operated in the internal network or in the cloud and is ideally the only system allowing indirect access to the isolated machine network.

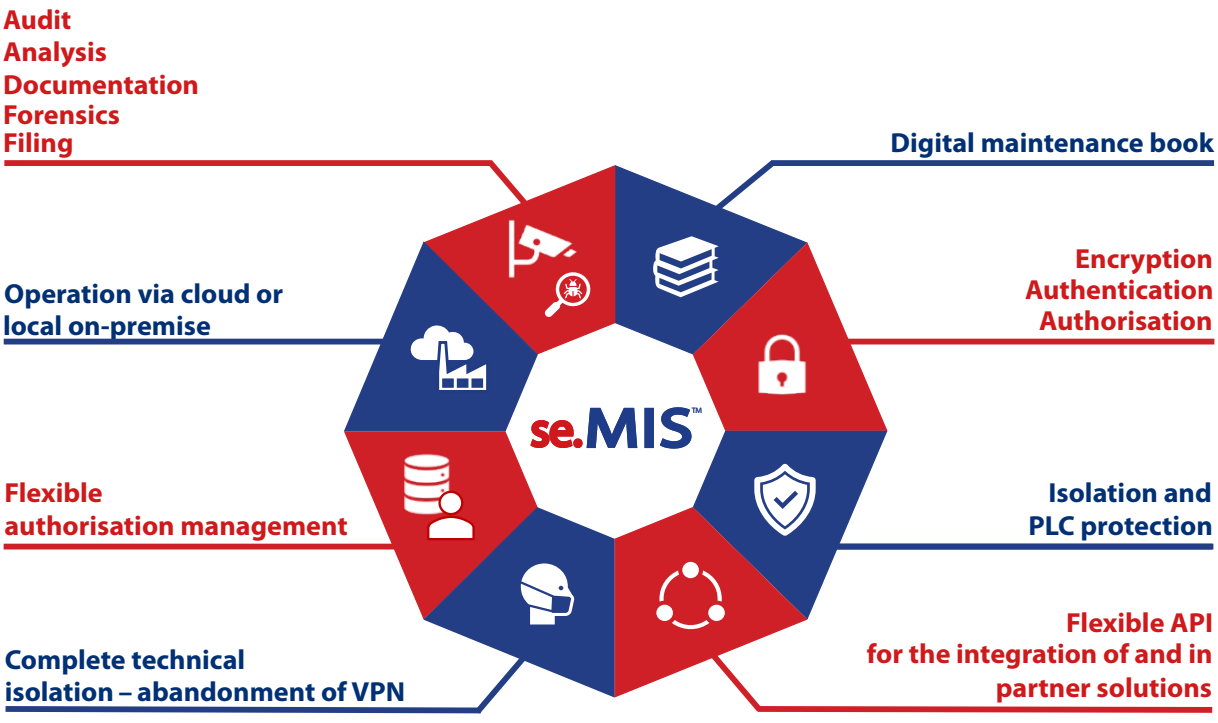
The **se.MIS™ Access Gateway** authorises external users from the internet to connect to the system without having to open the internal network's firewall first.

The **se.MIS™ Connector** enables secure access from the IT network into the machine network through an indirect connection. It also makes the adaptation of local systems to a cloud instance of **se.MIS™** easier. Like the overall solution, the connector is hardware-independent and along with the **Access Gateway**, it comes in different versions for the operation of a virtual machine as well as in the form of a docker container.

Furthermore, the **Connector** is available as a plug-in for renowned edge-gateways or industrial routers. All these options guarantee a maximum of flexibility without the additional use of hardware on an existing machine.

The **se.MIS™ KVM-Extender** (optional) allows access to systems which do not feature or even exclude network access. Keyboard, mouse and screen signals can be transferred digitally to the **se.MIS™ Manager** by using the **se.MIS™ KVM-Extender**.

The solution's core competencies



sematicon

Application operation and setup

“On-premise“ or “cloud-native“

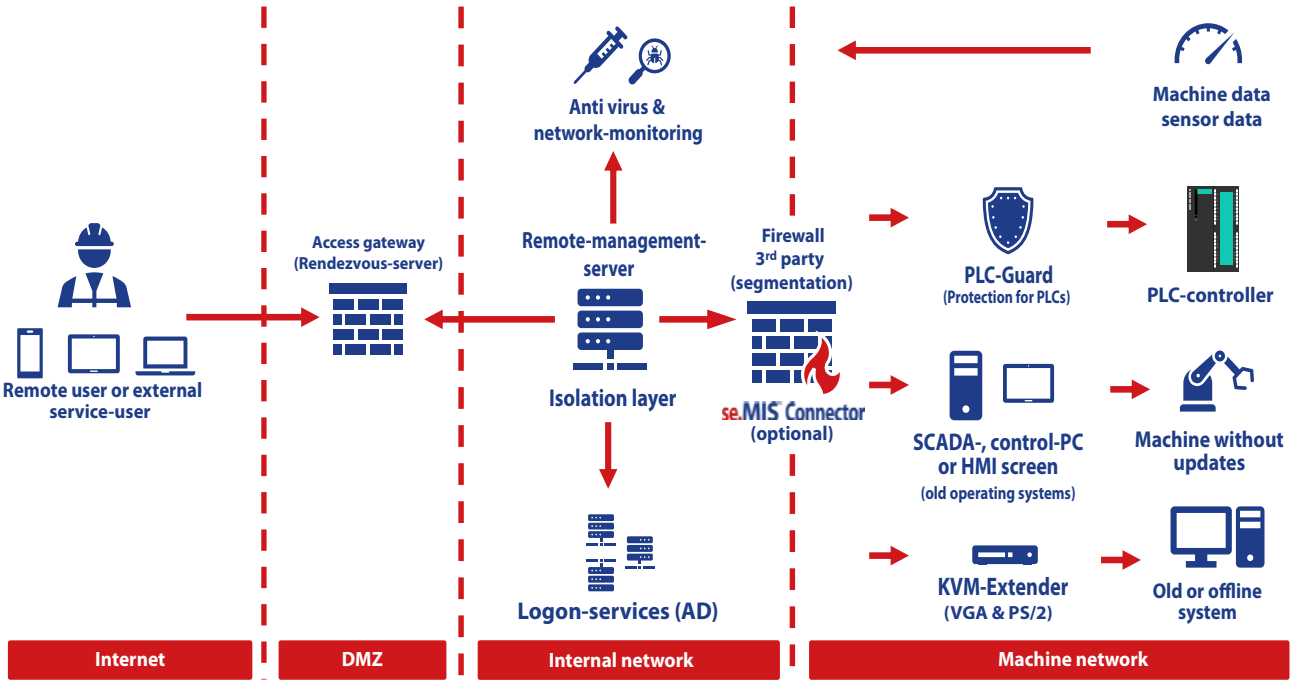
se.MIS™ can be fully installed on a **local system** outside the isolated machine network or in the **cloud**. The solution is already pre-installed and pre-configured and comes as a digital container or virtual machine (VM). The standard configuration is pre-defined by an internal and reliable data management. Operation and customisation are carried out via a lean and user-friendly web interface.

Any required update can be installed with only a few clicks. Data and configuration details remain unaffected. It is therefore easy to keep the solution up-to-date at all times and adapt it to any requirements and threats.

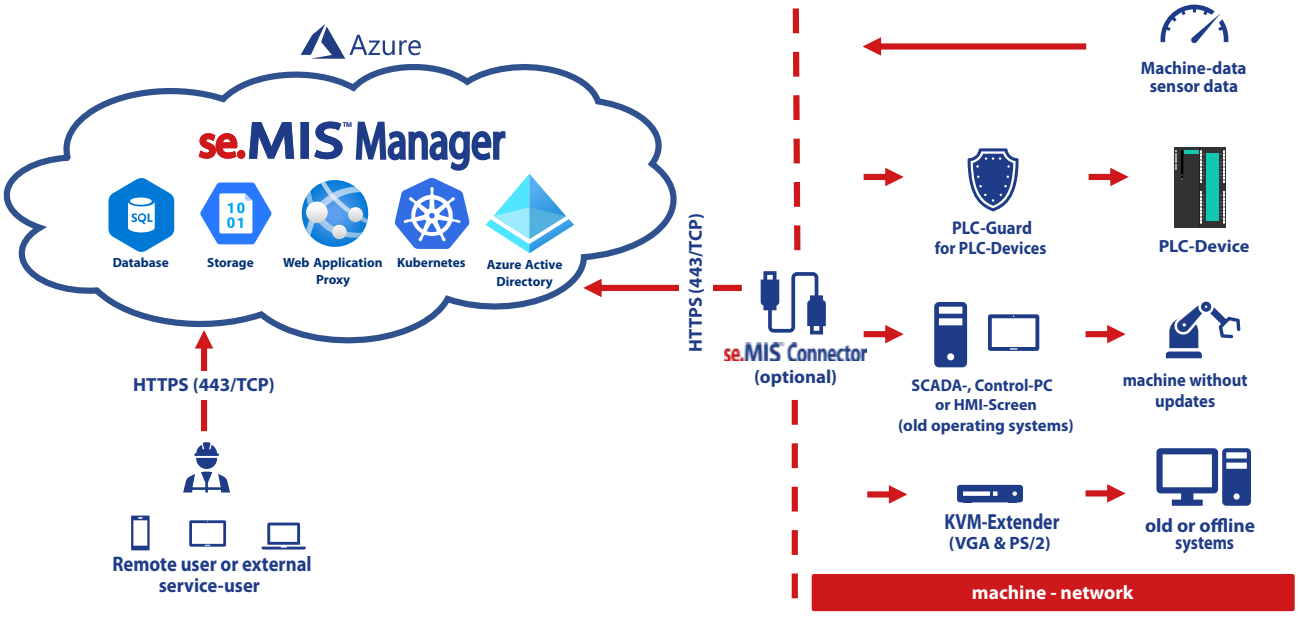
Above all, **se.MIS™** can be run as a “cloud native SaaS instance“ within the customer client, therefore granting maximum control over all data collected. All necessary resources can be obtained as a service from the cloud provider.

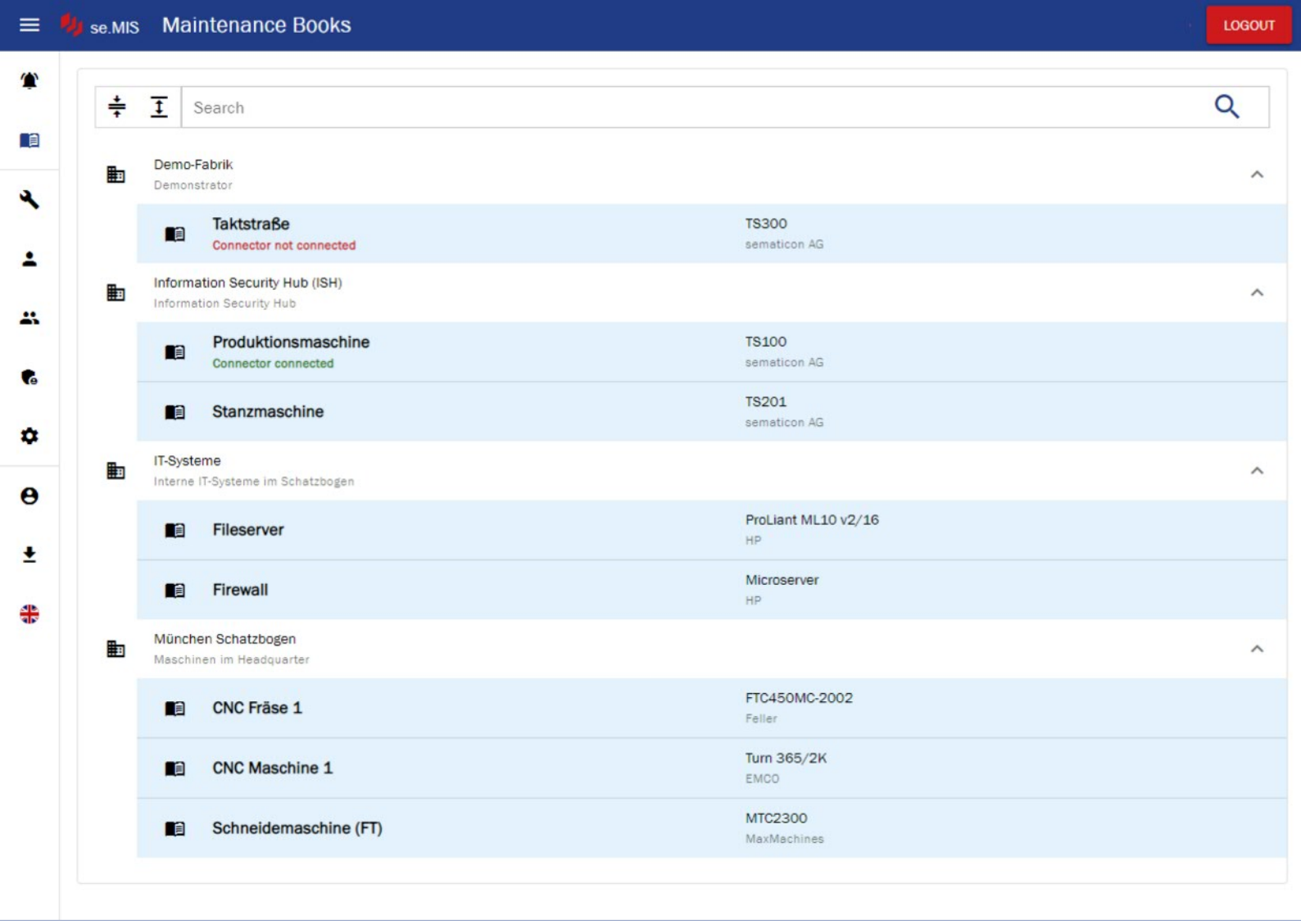
The concept of **se.MIS™** is that it can be used not only for the management of in-house machines, but also as a **“service provider“**. Setup scripts as well as the flexible API assist to quickly provide for separate client installations. The total amount of instances is not relevant for the licence. Only the number of machines is charged and billed on a monthly basis.

Reference architecture (local installation)



Cloud reference architecture (using Azure as an example)





Easy worldwide use according to IT standards

When **se.MIS™** was designed, special attention was also paid to its optimal use within IT organisations. The solution can thus be perfectly integrated in already existing infrastructures.

The **microservice architecture** of **se.MIS™** guarantees operation not only in a classic virtual infrastructure, but also natively in a cloud environment.

Data base and storage for the audit data and the configuration of the solution can be dynamically customised.

By speaking of **graphical audit data**, we do not understand classic video files. Only modified pixels and screen areas are stored. When working on the classic desktop, only very few KB per minute are thus accumulated.

All access to **se.MIS™** are TLS-encrypted and routed over port 443/TCP (HTTPS). As the solution works like a **web service**, it is easily installed. Well-known and potentially existing security solutions complement the clients' web server security architecture of **se.MIS™**.

Open standards and an easy-to-use licence model referring only to machines enable a harmonised and safe operation of **se.MIS™** across all sites worldwide.

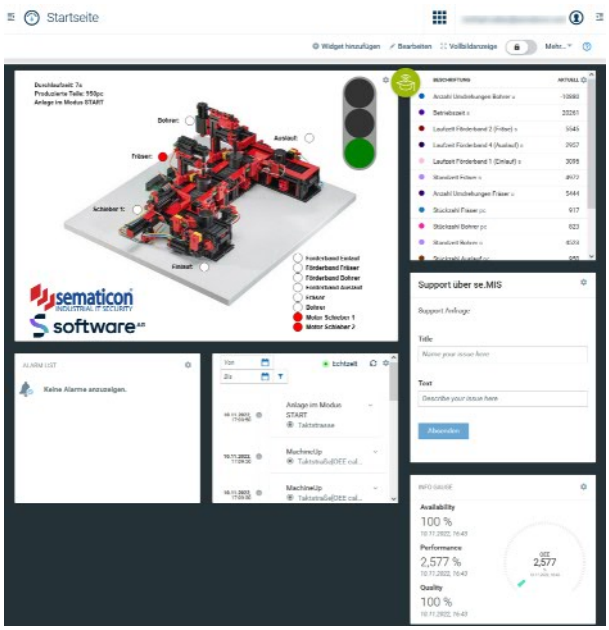
sematicon

Condition monitoring and “machine as a service“

se.MIS™ and industrial IoT applications

Software AG‘s **Cumulocity IoT cloud** is a tool to collect, display and process data intelligently from machines and system controls. Apart from the basic visualisation of data in “Zero-Code-Dashboards“, Software AG provides also for a seamless integration of Cumulocity into **se.MIS™**.

The appliance consequently allows machines to be monitored around the clock. In addition, Cumulocity offers a variety of possibilities to detect anomalies - starting from simple tresholds up to runtime systems for complex machine-learning-models. Cumulocity can also be employed to react to malfunctions in the SPS directly.



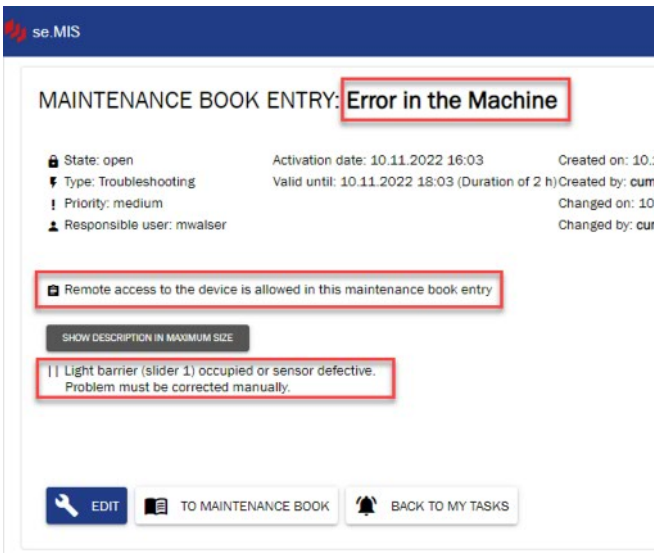
When a problem is detected, it is transmitted securely to **se.MIS™**. During this process, Cumulocity cannot access information about the responsible technician or machine details.

This information is found in the **se.MIS™** maintenance book. When the disruption is identified, the authorised technician or the contractor are notified automatically.

Access to the control system is made possible by means of the maintenance order "**Just in Time**" and with the **minimum rights necessary** for problem solving. After having corrected the error, Cumulocity will know immediately and revokes access to the system by closing the maintenance order. If required, the order can be retrieved and controlled any time later due to the automatic documentation.

To transfer the data to a ticket system, an ERP or any other system used for example for automated billing including the whole proof-of-work through the audit log, does not present any challenge.

Since access is isolated at all times, the technician on-duty can use any device.



sematicon

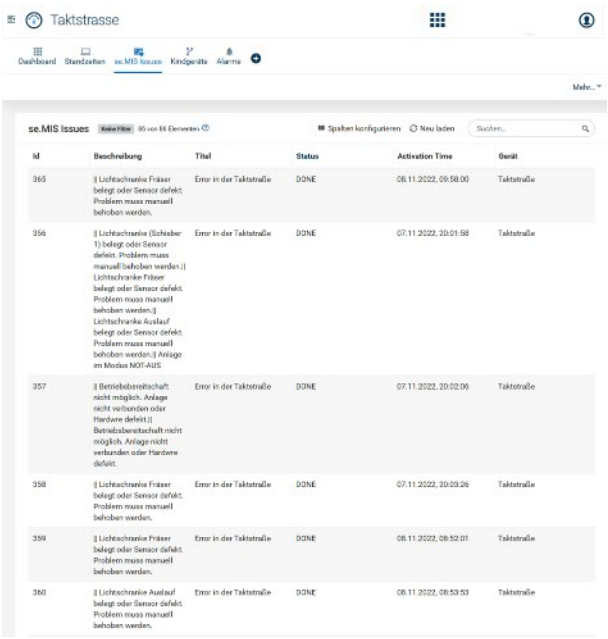
Integration into third-party-solutions - our flexible REST-API

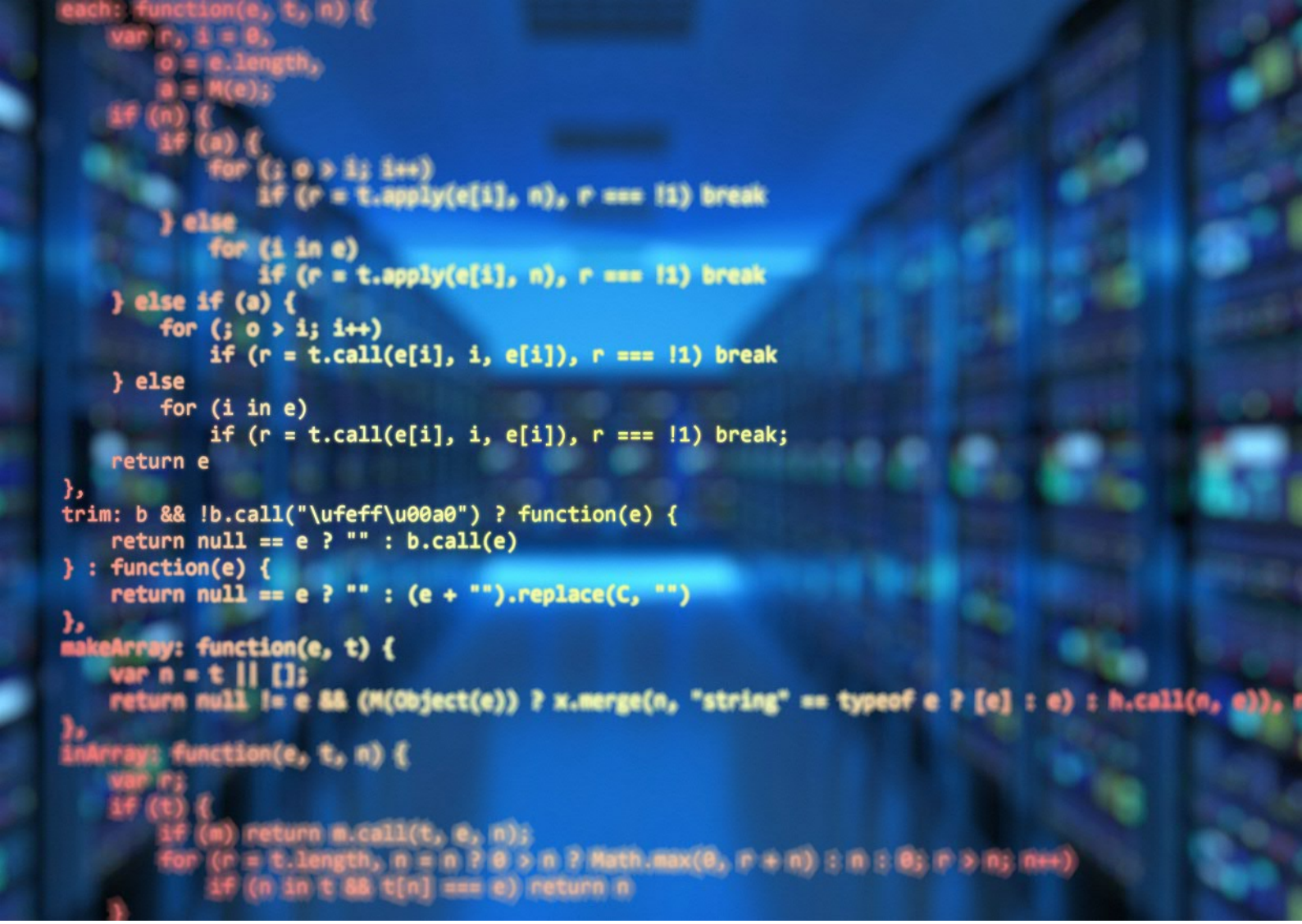
se.MIS™ as a platform - part of the overall solution

Thanks to the flexible API and our “API-first“ approach, **se.MIS™** can be integrated effortlessly and seamlessly into any other solutions. It is possible to either allow maintenance orders to be placed externally or to process them externally after a maintenance order has been closed.

Due to the intelligent microservice architecture of **se.MIS™**, even our GUI is not needed.

se.MIS™ also provides support in informing external systems about an upcoming maintenance requirement. Because **se.MIS™** covers the usecase “man - machine“, it is likely that complementary solutions, which constantly monitor the network to detect any anomalies, for example, are needed.





These **network monitoring solutions** are notified by cases of maintenance issues and thus avoid alarms caused by the technician's intervention.

In micro-segmented networks, **se.MIS™** is able to enforce **temporary port disconnections** using supporting third-party **firewalls** - after authorisation and only during an open maintenance order. "Gaps" within the network segmentation during runtime operation can be consequently avoided.

If an **existing ticket system** should be connected or it is necessary to process information with external **ERP systems** to charge orders, we provide you with our REST-API documentation in OpenAPI.

In case any changes of the HMI-display should be made and tracked at the same time, the API can be used as well.

With the assistance of our **se.MIS™ U200** USB hardware security modules for industrial use, a **cryptographic operation mode selector switch** can be realised. Mechanical keys are therefore no longer needed. The acting user is unmistakeably identified and their authorisation verified in real time.

se.MIS™ becomes a platform through the API and serves as a link for secure machine system access.

sematicon

Protecting SPS systems with PLC-guard

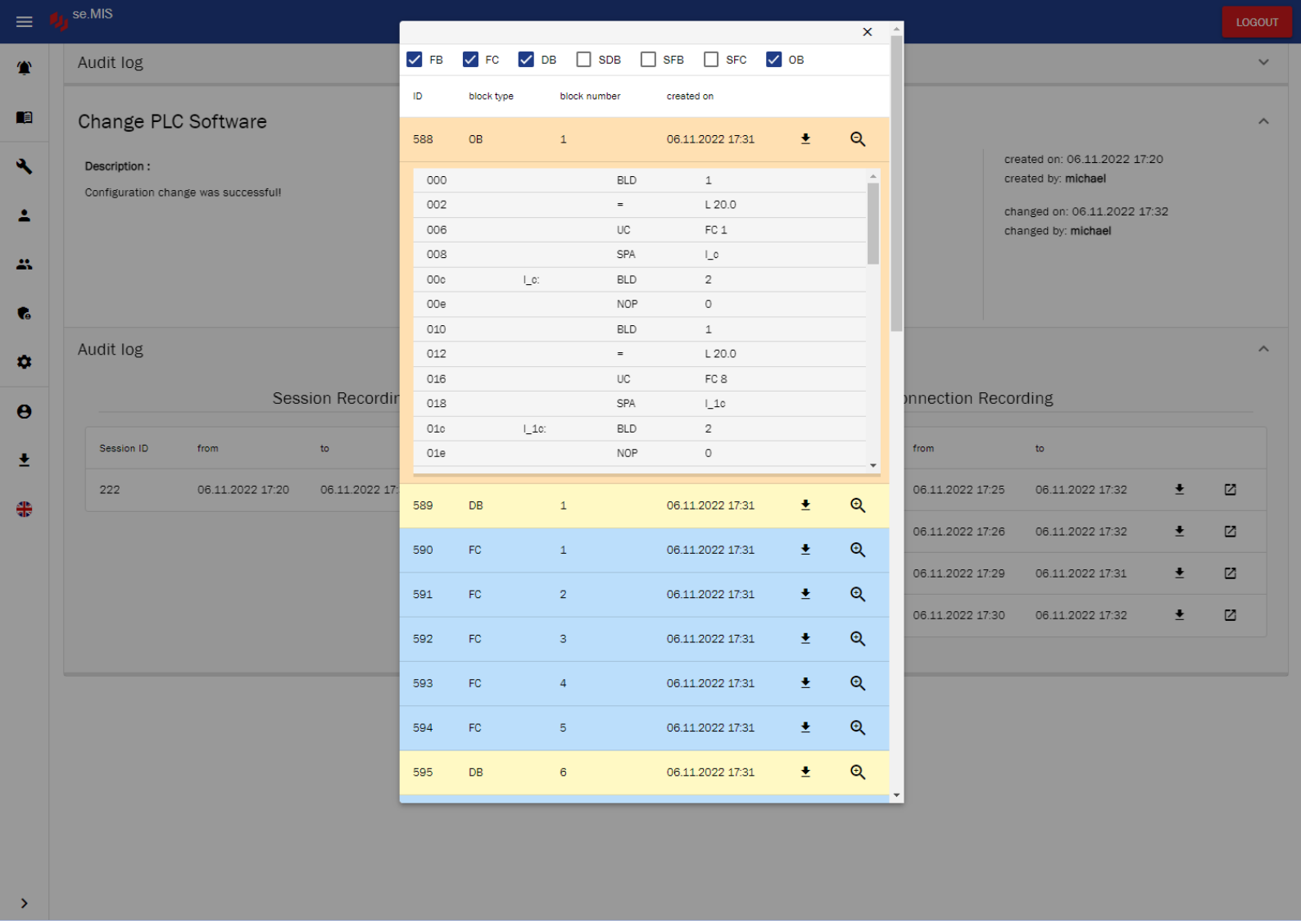
se.MIS™ and isolated access to SPS control systems

Due to their design, SPS control systems are particularly susceptible to attacks from the outside. Very often, a network connection is enough to end or change programme parts of the SPS.

Functions important for operation, such as software changes or the "device discovery" can also be used improperly to cause harm to the system. The "device discovery" feature, for example, helps to identify the SPS clearly. If the model and the connected modules are known, an attacker is able to intervene the running code. For instance, all outputs of the SPS can be activated using only one single command. The destruction of the plant is then very likely.

There is not much effort needed to write such a software. Furthermore, the technical footprint is also very small and difficult to detect.

Stuxnet was even more resourceful in compromising the SPS. By manipulating the network driver during programming, a part of the programme was appended before leaving the network interface. Before reaching the system development environment, exactly this part was cut off when the programme check took place. The discovery was thus difficult, if not impossible.



se.MIS™ supports any kind of SPS control system due to its IP functionality as long as it can be configured and programmed via the network.

In this case, the audit log only stores the network traffic for later analysis. The optionally licensable **PLC-guard** sets completely new standards in this respect. It permits access to the SPS communication and the verification of the source code before the code reaches the SPS.

The check is carried out directly in the **se.MIS™ Manager** and independently from the technician's PC. According to the "Zero-Trust" principle, the technician's PC is a threat by definition. Having been once connected to the internet, the risk of it being compromised by malware increases.

se.MIS™ isolates the technician's access, who establishes a connection only to a **virtual SPS**, which is emulated within **se.MIS™**. When a programme download to the SPS is carried out, the machine code is intercepted and disassembled by **se.MIS™**. All blocks as well as the content in the form of the instruction list (IL) are made visible again.

As a result, any unplanned changes are identified on the "last mile" before reaching the SPS. Thus, it is ensured that only the intended code reaches the control system.

In addition to purely documenting the downloads, the system operator also has the option of withholding the code and releasing it manually.

Definable workflows allow the identification of changes to the previous versions and the uploading of backups of any previous stage directly from the digital maintenance book to the SPS.

At the moment, PLC-guard supports the market leader SIEMENS S7 - further models follow as required.

sematicon

Integration of old systems without network access

se.MIS™ and access to old systems

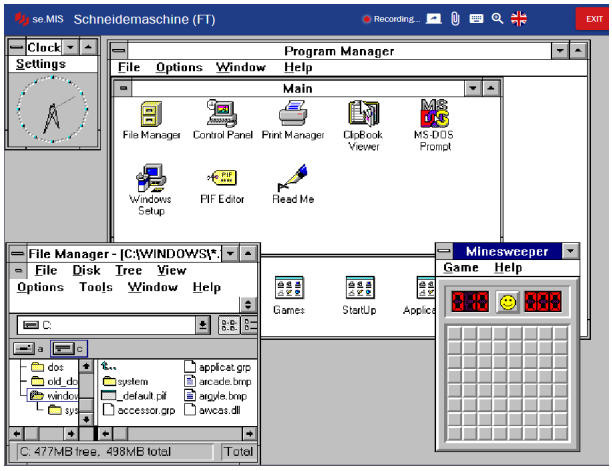
In order to cover as many installations and systems as possible, **se.MIS™** provides the opportunity of implementing systems without network connection using the optionally available **KVM-Extenders**.

They pave the way to include any machine regardless of their age and operating system. All that is required is a PS/2 and VGA-port or a DVI-port with USB.

The **se.MIS™ KVM-Extender** digitises any analogue screen signals, keyboard and mouse inputs.

Even modern systems can be connected with the **se.MIS™ KVM-Extender**.

This is necessary for systems, for example, where network access must be technically prevented. The extender limits access only to screen, keyboard and mouse.



The **se.MIS™ KVM-Extender** series

The **se.MIS™ KVM-Analogue-Extender** allows the direct connection of a control PC's keyboard, mouse and screen to the machine. No matter if you are working with MS-DOS, Windows CE or another system: all kinds of devices featuring VGA and PS/2 can be remotely controlled by this extender.

Resolutions for up to 1600 x 1200 pixels can be easily digitised and transmitted. Power is supplied either by the PS/2 connection or by an optional power supply (5 V DC) and is therefore independent of other power sources.

Compared to the analogue-version, the **se.MIS™ KVM-Analogue-Duo-Extender**'s advantage is that it can be connected to an additional local screen or a local HMI-panel. The control PC shall be connected to the input and the local screen to the output.

Resolutions for up to 1600 x 1200 pixels can be easily digitised and transmitted. Power is supplied either by the PS/2 connection or by an optional power supply (5 V DC) and is therefore independent of other power sources.

The **se.MIS™ KVM-Digital-Extender** can be connected to any digital systems by DVI or HDMI. When connected with a USB-port, the device behaves like a USB-keyboard or a USB-mouse. USB-Virtual-Media-Support can be upgraded by acquiring an additional licence.*

Resolutions for up to 1920 x 1200 pixels are possible. Power is supplied by a USB-port or by an optional power supply. The USB-port is a USB 2.0 Type B.

*Not available in all **se.MIS™** versions. Please request separately.

We are a Munich-based company focusing on IT security and cryptography in industrial environments.

We offer support for:

Secure management of industrial plants

encrypted, reproducible and secure connections on
critical microprocessor, industrial and central control systems

Cryptography for IoT, IIoT and Embedded Systems

conception and support of as well as monitoring during the
development of secure IIoT, IoT and embedded systems

Training and consulting

all about certificates (PKI), cryptography, encryption
and secure key storage (HSM)

sematicon AG
Schatzbogen 56
81829 Munich
Germany

Phone: +49 (89) 413 293 - 000
Fax: +49 (89) 413 293 - 199

E-Mail: sales@sematicon.com
www.sematicon.com

sematicon
INDUSTRIAL IT SECURITY

V4.0 EN 2022