designed
developed
made
in Germany

sematicon
INDUSTRIAL IT SECURITY

se.MIS™

Im Zeichen der IEC-62443

Wartungsmanagement und „Zero-Trust“ Remote Access für Industrie- und Steuerungsanlagen

sematicon

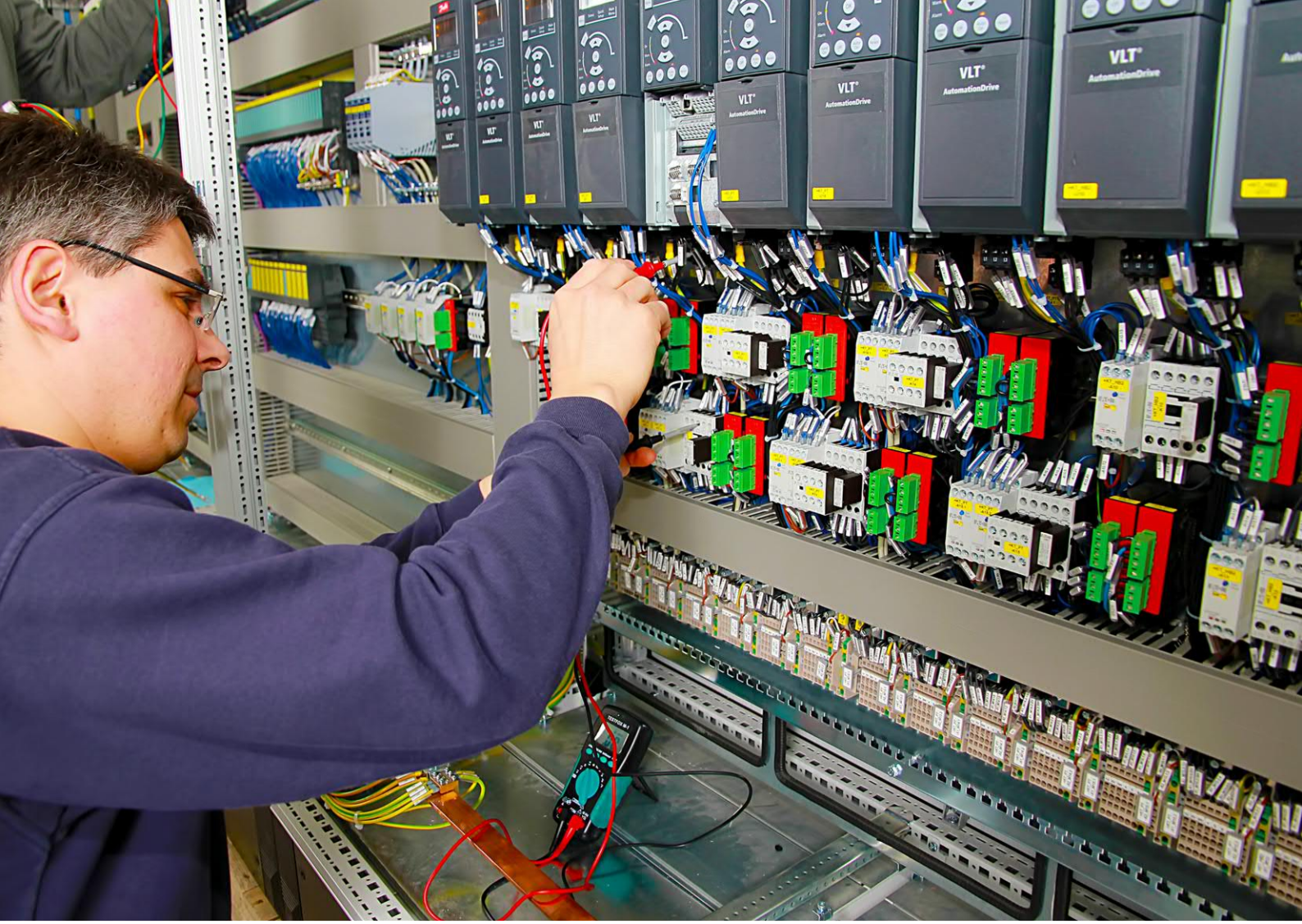
Das Unternehmen

Die **sematicon AG** ist ein Münchner Unternehmen mit Fokus auf Informationssicherheit und Kryptographie in Industrie, Elektronik sowie der IIoT-Welt.

Wir verbinden jahrzehntelange Erfahrung aus diesen Bereichen und eröffnen neue Horizonte, um dabei mit einem Dogma der IT-Branche zu brechen: **Sicherheit muss nicht kompliziert sein.** Benutzerfreundlichkeit und Systemsicherheit stehen bei uns an erster Stelle und schließen einander nicht aus.

Mit unserem spezialisierten und hoch motivierten Team stellen wir uns den aktuellen Herausforderungen der **Industrie 4.0**. Die von uns entwickelten Lösungen erlauben es, sicher auf Industrieanlagen zuzugreifen sowie die **Integrität**, **Authentizität** und **Sicherheit** der digitalen Daten und Prozesse zu gewährleisten. Unsere innovativen Lösungen sind bisher **einmalig am Markt**.

Daher sind wir Ihr zuverlässiger Partner bei allen Fragen zur sicheren Industrie 4.0„**Made in Germany**“.



Industrielle Automation im Zeitalter von Industrie 4.0

Die **digitale Transformation** hat die IT-Landschaft in den vergangenen Jahren stark verändert. Maschinen- und Produktionsanlagen sowie ganze Industriezweige bewegen sich zunehmend in einer digital vernetzten Welt. Wir befinden uns also in einem Umbruch innerhalb der digitalen Steuerungs- und Automatisierungstechnik. Neben den enormen Möglichkeiten, die in der Vernetzung und der Digitalisierung liegen, stellen sich auch neue Herausforderungen. Eine davon ist, vor allem die **Sicherheit** und **Unversehrtheit** der nun digital vorliegenden Daten und Prozesse zu garantieren.

Das Bewusstsein dafür entwickelt sich auch immer mehr im industriellen und produzierenden Gewerbe. Es ist nicht möglich, die bestehenden Konzepte und Strategien der IT-Welt einfach in die Industrie-Welt zu übertragen. Die Abschreibungszeiten von IT-Systemen betragen im Durchschnitt drei bis fünf Jahre. Jedoch gelten für Industrieanlagen völlig andere Größenordnungen. Oft laufen solche Anlagen auch dann noch, wenn die Lebensdauer bzw. der Support-Zeitraum der in den Steuerungen eingesetzten Software bereits lange überschritten ist. Ein weiterer Faktor ist das Installieren der für die Sicherheit in der vernetzten Welt notwendigen Updates. Dieser Vorgang gestaltet sich oft schon während der Laufzeit als problematisch. Dies liegt meist an der eingesetzten, proprietären Steuerungssoftware oder inkompatiblen Hardware.

sematicon

Digitales Wartungsbuch und „Zero-Trust“ Remote Access

Sicherer und nachvollziehbarer Zugriff auf Anlagen

Einerseits ist es eine bekannte Tatsache, dass die Mehrzahl der Systeme in der Industrie nicht mittels Sicherheitsupdates auf dem neuesten Softwarestand gehalten werden, andererseits stellen auch **legitime Produktfeatures ein Sicherheitsrisiko** dar, wenn diese bei der Planung eines umfassenden Industriellen **Sicherheitskonzeptes** außer Acht gelassen werden. Dadurch entstehen erhebliche Risiken in vernetzten Umgebungen, was ein Spannungsfeld zwischen der IT und der Industrie zur Folge hat. Die Anforderung der IT besteht besonders darin, die Systeme sicher ans Netz zu bringen. Der Fokus der Industrie hingegen gilt in erster Linie der durchgehenden Funktion der Systeme. Die Situation ist für beide Seiten nicht einfach zu bewältigen.

Die Entwicklung von **se.MIS™** erfolgte in enger Abstimmung mit unterschiedlichen Industriekunden und deren individuellen Maschinenparks. Damit sind konkrete Ziele und Erwartungen immer im Blickfeld.

Ziel unserer Entwicklung ist die Absicherung und Integration der Anlagen auf Basis moderner IT-Sicherheitsstandards, ohne diese durch zusätzliche Software oder Updates zu verändern.

Die Designkriterien bei der Entwicklung sind:

Zero-Trust - Der Zugriff auf die Anlagen selbst erfolgt nach dem Prinzip von „Zero-Trust“ entsprechend einer Empfehlung des BSI (Bundesamt für Sicherheit in der Informationstechnik) und bedeutet, dass beim Zugriff auf eine Industrieanlage u.a. nachfolgende Themen berücksichtigt werden sollen:

Trennung der Zuständigkeiten - Dieser Grundsatz beschreibt die Idee, dass keine Person oder kein Gerät vollständigen Zugriff auf alle wichtigen IT-Quellen eines Unternehmens haben sollte.

Zugriff mit den geringsten Privilegien - Dadurch wird erreicht, dass jeder Zugriff nur mit absolut notwendigen Rechten ausgestattet wird. So macht es wenig Sinn, wenn einem Techniker die gesamte Steuerung zur Verfügung steht, wenn er nur graphischen Zugriff auf das HMI-Display benötigt.

Mikrosegmentierung - Durch die Segmentierung wird erreicht, dass die OT - Umgebung in Sicherheitszonen aufgeteilt wird mit der Eigenschaft, dass für jeden Zugriff in eine andere Zone eine separate Authentifizierung erforderlich ist.

Mehrstufige Authentisierung - Das bedeutet, dass für die Anmeldung neben dem „Wissen“ (Passwort) auch ein „Besitz“ (Einmalpasswort-Token oder App für das Mobiltelefon) notwendig ist.

„Just-in-Time“ Zugriff - Ein Benutzer hat niemals permanenten Zugang zu einer Ressource, sondern ausschließlich für den Zeitraum, der benötigt wird, um eine Problemstellung zu lösen.

Audit und Nachverfolgung - Hierdurch wird sichergestellt, dass alle Vorgänge und Änderungen vollständig protokolliert werden.

Vollständige Isolation der Zugriffe - Dadurch wird der maximale Schutz der Anlage gewährleistet, da eventueller Schadsoftware kein Zugriff gelingt. Damit ist auch der Angriffsvektor für Zero - Day - Angriffe stark reduziert.

se.MIS™ erfüllt alle Empfehlungen des BSI im Gegensatz zu klassischen VPN-Lösungen. VPN gilt vor allem im industriellen Einsatz als unsicher, da es wie ein „virtuelles Netzwerkkabel“ den externen Techniker direkt an den Netzwerkport der Anlage anbindet. Unsere Lösung verhindert nicht nur den direkten IP-Zugriff, sondern protokolliert auch alle Änderungen am System vollständig in einem **digitalem Wartungsbuch**.

Dieses Wartungsbuch ist neben der Wartungsplanung auch für die manuelle sowie automatische Protokollierung verantwortlich. Dazu gehören die Aufzeichnung der Bildschirmsitzungen als Video bis hin zu Netzwerk-Traces (PCAP-Files) für IP-basierte Sitzungen oder die komplette SPS-Software mit Unterstützung des optionalen Features PLC-Guard.

Das Wartungsbuch beinhaltet auch alle notwendigen Informationen über die Anlage sowie die für die Anlage zuständigen Techniker und die notwendigen Berechtigungen für den Zugriff auf die Anlage. Egal ob eine Wartung geplant oder Ad-Hoc stattfinden muss, eine korrekte Autorisierung an der Maschine ist somit immer sichergestellt.

Besonders die Übertragung und Handhabung von externen Dateien stellen bei Industrieanlagen eine große Gefahr dar. Oft ist es nicht möglich einen Virenscanner zu betreiben. Neben der permanenten Dokumentation und Archivierung der übertragenen Dateien im Wartungsbuch können diese vor der Übertragung zentral über **se.MIS™** durch Dritthersteller überprüft werden. Der dafür verwendete Viren- bzw. Content-Scanner ist nicht Teil der Lösung und kann vom Kunden ausgewählt werden, sofern bestimmte Anforderungen und Schnittstellen vorhanden sind. Eine direkte Übertragung ist somit auch hier ausgeschlossen, da alle Uploads über das Wartungsbuch geführt werden.

Mit **se.MIS™** haben Sie auch immer die Anforderungen einer **IEC-62443** im Blick, damit einer künftige Zertifizierung nichts im Wege steht.

se.MIS™ ermöglicht…

…Selbstbestimmung von IT und Industrie

IT- und Anlagenanwender definieren unterschiedliche Anforderungen an Benutzer und deren Rechte. Klassische IT-Benutzer können mittels ActiveDirectory eingebunden werden. Weiter besteht die Möglichkeit, Techniker und deren Berechtigungen aus anderen Verzeichnissen oder der lokalen Datenbank zu ergänzen, um diese selbstbestimmt zu verwalten.

…Unterstützung für alte und moderne Systeme

Die Unterstützung ist für alte Systeme wie MS-DOS oder Windows CE genauso gegeben wie für aktuelle Betriebssysteme und Anwendungen. Durch diese Flexibilität können neben den zu wartenden Anlagen auch Datei-Server, IT-Systeme und andere moderne IT-Komponenten externer Standorte eingebunden werden.

…vollständige Dokumentation aller Zugriffe

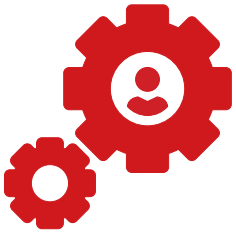
Alle Änderungen und Zugriffe werden obligatorisch im digitalem Wartungsbuch dokumentiert, archiviert und lassen sich somit exakt nachvollziehen. Ein Eintrag wird bei jedem Zugriff auf die Maschine automatisch angelegt und kann nach Belieben manuell ergänzt werden. Es können bei Bedarf sogar komplette Sitzungen forensisch aufgezeichnet werden.

…Planung und Steuerung von Zugriffen

Ein umfangreiches Planungssystem stellt sicher, dass Zugriffe ausschließlich zum vordefinierten Zeitpunkt durchgeführt werden können. Auf dieser Basis erlaubt oder entzieht das System den Zugang vollautomatisch. Zugriffe auf die Maschine sowie das Wartungsbuch sind frei und unabhängig voneinander konfigurierbar. Dadurch kann sich ein Techniker vor dem Auftrag umfassend über die Maschine informieren.

…modernste und höchste Sicherheitsstandards

Der Zugriff auf das System sowie alle Daten sind kryptographisch gegen Manipulation und Fremdzugriff auf Basis modernster Sicherheitsrichtlinien der IT geschützt. Die Verschlüsselung aller Daten und Verbindungen sowie die Anforderungen der IEC-62443 sind dabei ebenso gewährleistet wie eine sichere Anmeldung mittels Einmalpasswort-App (OTP) oder hardwarebasierter Kryptoschlüssel.



…einfache Installation, Integration und Betrieb

Beim Design der Lösung wurde besonderer Wert auf die einfache Bedienung und Integration gelegt. Die Installation selbst kann vor Ort von jedem Nutzer vorgenommen werden. Umfangreiches Fachwissen ist dabei nicht notwendig. Möglich wird das durch ein intuitives Administrations-Interface sowie umfangreiche Automatismen im Hintergrund.

sematicon

Lösungsübersicht

Flexibilität durch ein modulares System ohne Hardware

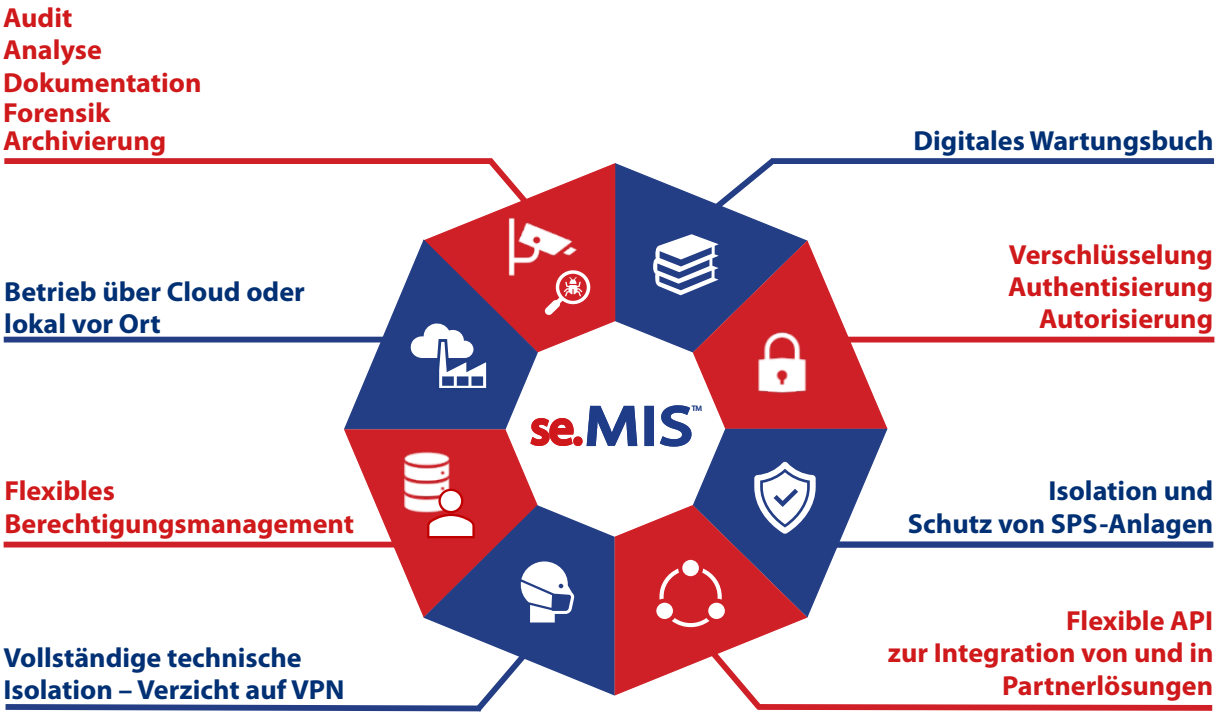
Der **se.MIS™ Manager** ist das Kernstück der Lösung. Hier findet die Benutzerinteraktion statt. Das System wird im internen Netz oder in der Cloud betrieben und ist im Idealfall das einzige System mit indirektem Zugriff auf das isolierte Maschinen-Netzwerk.

Das **se.MIS™ Access Gateway** ermöglicht es externen Benutzern aus dem Internet auf das System zuzugreifen, ohne dass aus dem internen Netz heraus die Firewall geöffnet werden muss.

Der **se.MIS™ Connector** ermöglicht einen sicheren Zugriff vom IT-Netz in das Maschinen-Netz durch eine indirekte Verbindung. Auch kann der Connector genutzt werden, um lokale Systeme an eine Cloud-Instanz von **se.MIS™** anzubinden. Der Connector ist wie die Gesamtlösung hardwareunabhängig und steht wie das Access Gateway in verschiedenen Varianten für den Betrieb in einer virtuellen Maschine oder als Docker Container zur Verfügung. Des Weiteren ist der Connector auch als Plug - In für diverse namhafte Edge-Gateways oder Industrie-Router bereit. Damit ist maximale Flexibilität ohne zusätzlichen Hardwareeinsatz an der vorhanden Maschine gewährleistet.

Der **se.MIS™ KVM-Extender** (optional) ermöglicht den Zugang auf Systeme, die über keinen Netzwerk-Zugriff verfügen bzw. wenn dieser organisatorisch ausgeschlossen ist. Mit dem **se.MIS™** KVM -Extender ist es möglich, Tastatur-, Maus- und Bildschirmsignale digital in den **se.MIS™** Manager zu übergeben.

Kernkompetenzen der Lösung



sematicon

Applikationsbetrieb und Setup

„On-Premise“ oder „Cloud-Native“

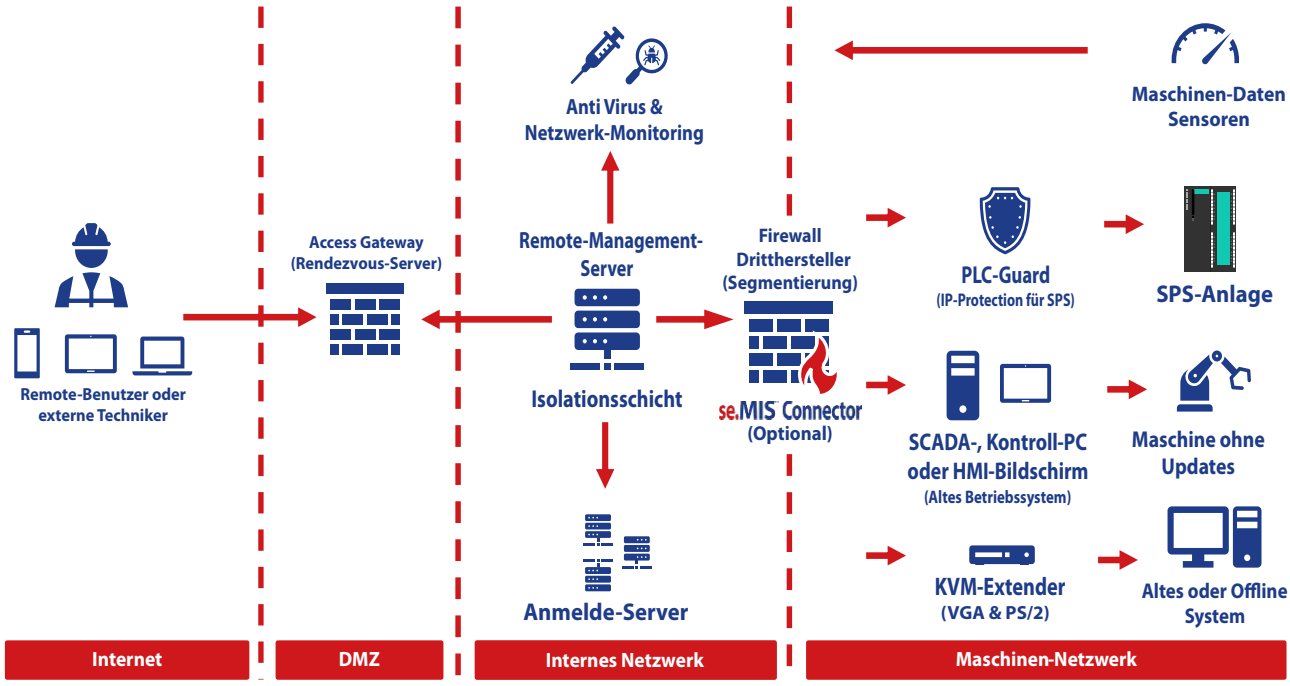
se.MIS™ kann vollständig auf einem **lokalen System** außerhalb des isolierten Maschinen-Netzwerks oder in der **Cloud** installiert werden. Die komplette Lösung wird als digitaler Container oder Virtuelle Maschine (VM) vorinstalliert und vorkonfiguriert ausgeliefert. In der Standardkonfiguration ist eine interne, zuverlässige Datenverwaltung vordefiniert. Die Bedienung und Konfiguration der Lösung erfolgt über ein schlankes, benutzerfreundliches Web-Interface.

Steht ein Update an, ist dieses mit wenigen Klicks installiert. Daten und Konfigurationen bleiben unberührt. So ist es einfach, die Lösung stets aktuell zu halten und an die jeweiligen Anforderung- und Bedrohungslagen anzupassen.

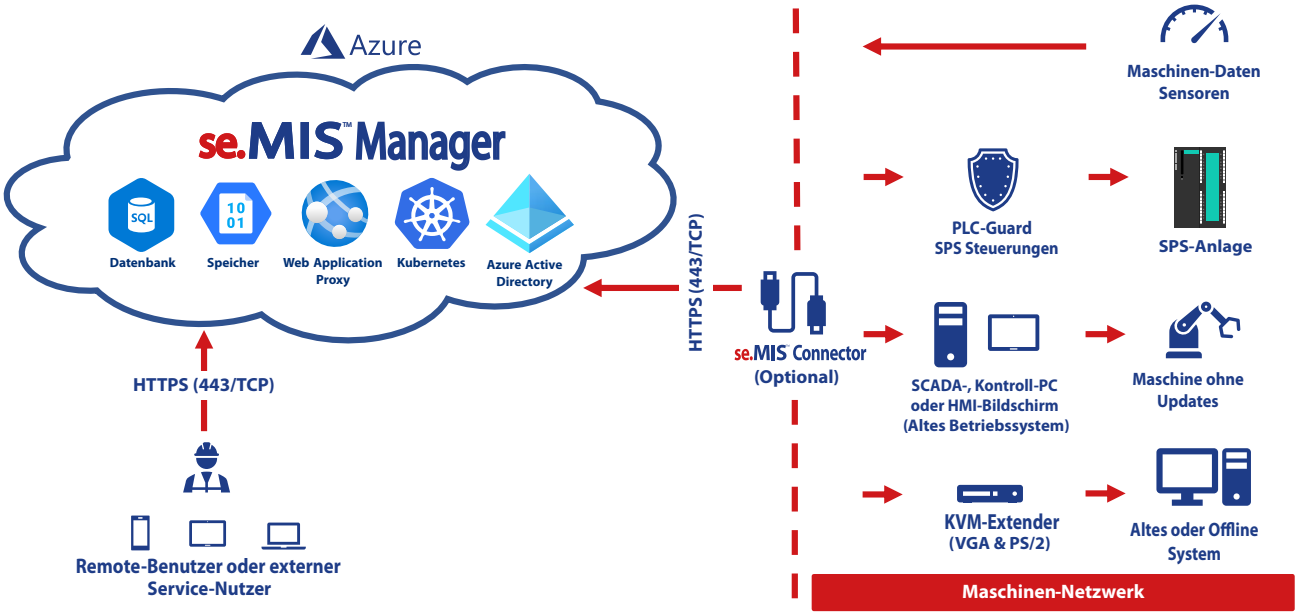
se.MIS™ kann außerdem als „Cloud Native SaaS Istance“ innerhalb des Kunden-Mandanten betrieben und erlaubt somit maximale Kontrolle über alle erhobenen Daten. Alle notwendigen Ressourcen können als Service vom Cloud-Provider bezogen werden.

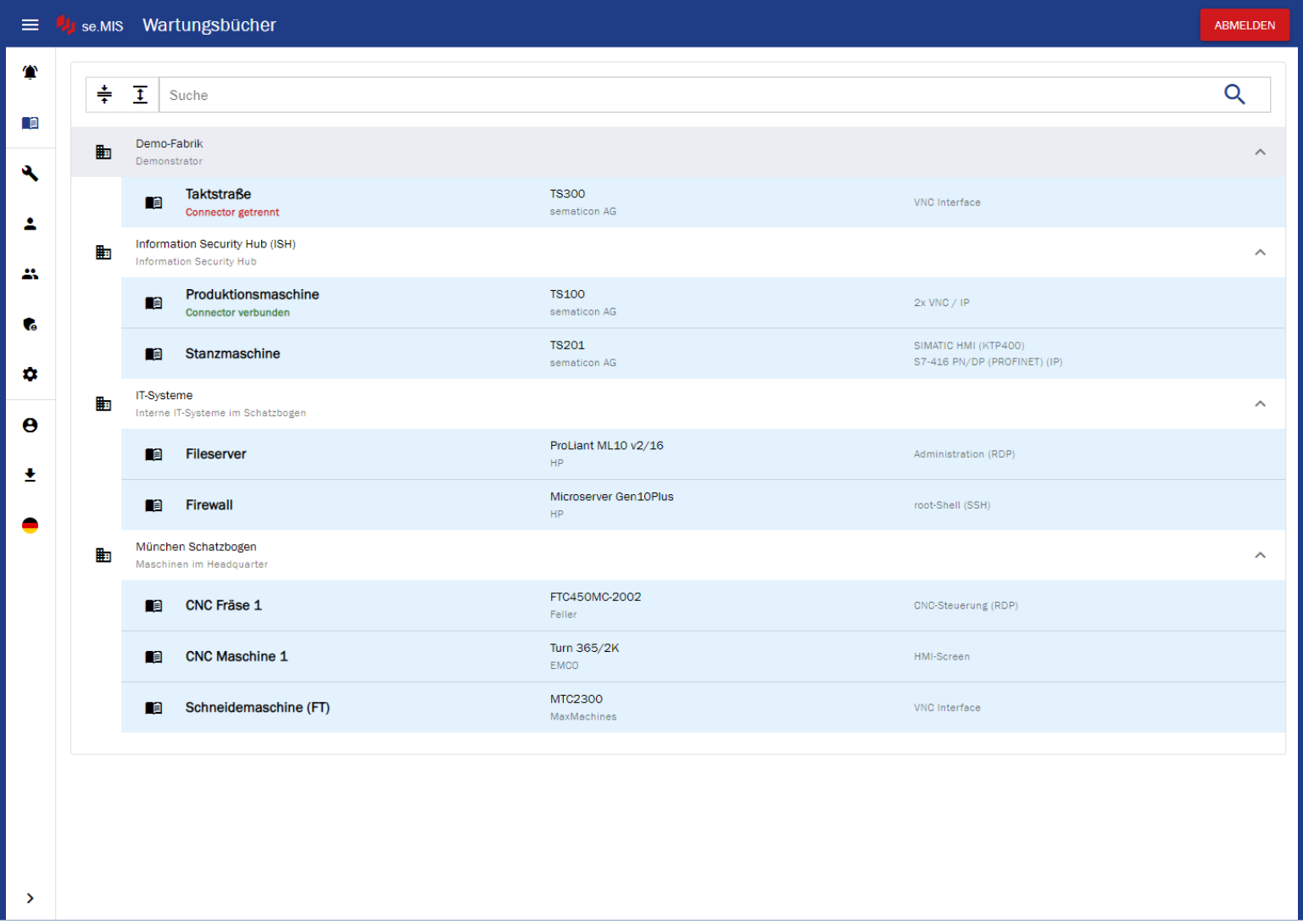
se.MIS™ wurde so konzipiert, dass es neben der Verwaltung der hauseigenen Maschinen auch für Kunden als „**Service-Provider**“ verwendet werden kann. Dabei stehen Setup-Scripte sowie die flexible API zur Verfügung um getrennte Kunden-Installationen schnell zur Verfügung zu stellen. Die Anzahl der Instanzen ist dabei für die Lizenz unerheblich. Nur die Anzahl der Maschinen wird monatlich erhoben und abgerechnet.

Referenzarchitektur (Lokale Installation)



Referenzarchitektur (Cloud Setup am Beispiel von Azure)





Einfacher weltweiter Einsatz nach IT-Standards

Bei der Entwicklung von **se.MIS™** wurde auch auf einen optimalen Einsatz innerhalb des IT-Betriebs geachtet. Die Lösung lässt sich somit perfekt in bestehende Infrastrukturen eingliedern.

Die **Microservice-Architektur** von **se.MIS™** gewährleistet den Betrieb sowohl in einer klassischen virtuellen Infrastruktur als auch nativ in einer Cloud-Umgebung.

Datenbank und Storage für die Audit-Daten sowie für die Konfiguration der Lösung lassen sich dynamisch konfigurieren.

Bei den **graphischen Audit-Daten** handelt es sich außerdem um keine klassischen Video-Dateien, sondern es werden nur geänderte Pixel und Bildschirmbereiche gespeichert. Bei der Arbeit am klassischen Desktop fallen daher nur wenige KB pro Minute an.

Alle Zugriffe auf **se.MIS™** verlaufen über den Port 443/TCP (HTTPS) und sind mittels TLS verschlüsselt. Da sich die Lösung wie ein **Webservice** verhält, ist die Installation denkbar einfach zu realisieren. Zusätzlich ergänzen bekannte und eventuell schon vorhandene Sicherheitslösungen auf Kundenseite die Web-Server-Sicherheitsarchitektur von **se.MIS™**.

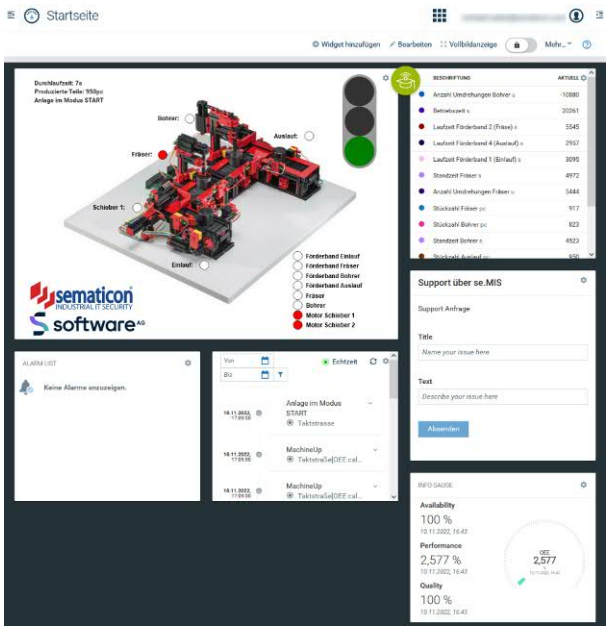
Offene Standards sowie ein flexibles und einfaches Lizenzmodell, welches sich nur auf die Maschinen bezieht, ermöglichen einen harmonisierten und sicheren Betrieb von **se.MIS™** über alle Standorte weltweit.

sematicon

Condition Monitoring und „Machine As A Service“

se.MIS™ und Industrial IoT-Anwendungen

Die **Software AG** stellt mit ihrer **Cumulocity** IoT Cloud ein Werkzeug bereit, um Daten von Anlagen und Steuerungen zu erheben, anzuzeigen und intelligent zu verarbeiten. Neben der einfachen Darstellung von Daten in „Zero-Code-Dashboards“ hat die Software AG für Cumulocity eine nahtlose Integration in **se.MIS™** bereitgestellt. Somit lassen sich Maschinen rund um die Uhr überwachen. Cumulocity bietet eine Vielzahl an Möglichkeiten, um Anomalien zu erkennen. Das beginnt bei einfachen Tresholds bis hin zu Laufzeit-Umgebungen für komplexe Machine-Learning-Modelle. Über Cumulocity kann auch direkt auf Störungen der SPS reagiert werden.



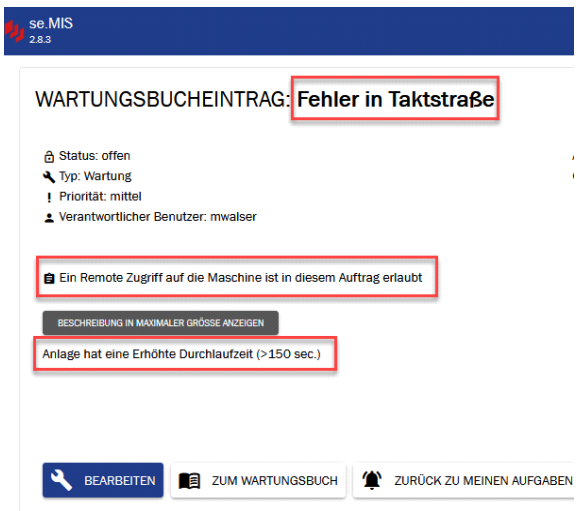
Wird eine Störung erkannt, kann diese auf sicherem Wege an **se.MIS™** übertragen werden. Dabei hat Cumulocity keine Kenntnis über den zuständigen Techniker oder Details über die Maschine.

Diese Informationen sind im Wartungsbuch von **se.MIS™** vorhanden. Wenn eine Störung erkannt wird, wird der berechtigte Techniker oder Vertragsfirma automatisch verständigt.

Der Zugriff auf die Anlage wird mittels Wartungsauftrags „**Just in Time**“ mit den **minimal notwendigen Rechten** zur Problemlösung zur Verfügung gestellt. Nachdem die Störung beseitigt wurde, erkennt dies Cumulocity und entzieht den Zugang auf die Anlage durch automatische Quittierung des Wartungsauftrages. Sofern gewünscht, kann der Auftrag durch die automatische Dokumentation jederzeit eingesehen und kontrolliert werden.

Die Weitergabe von Daten an ein Ticket- System, ERP-System oder andere Systeme für z.B. automatisierte Abrechnungen inklusive vollständigem Arbeitsnachweis durch das Audit-Protokoll stellt auch kein Problem dar.

Da der Zugriff zu jederzeit isoliert stattfindet, kann der Techniker im Bereitschaftsdienst jedes beliebige Endgerät für den Zugriff verwenden.



sematicon

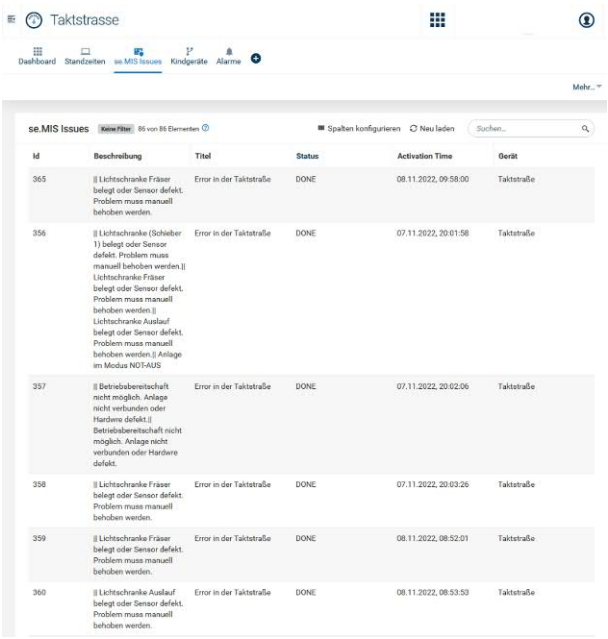
Integration in Drittlösungen
Unsere flexible REST-API

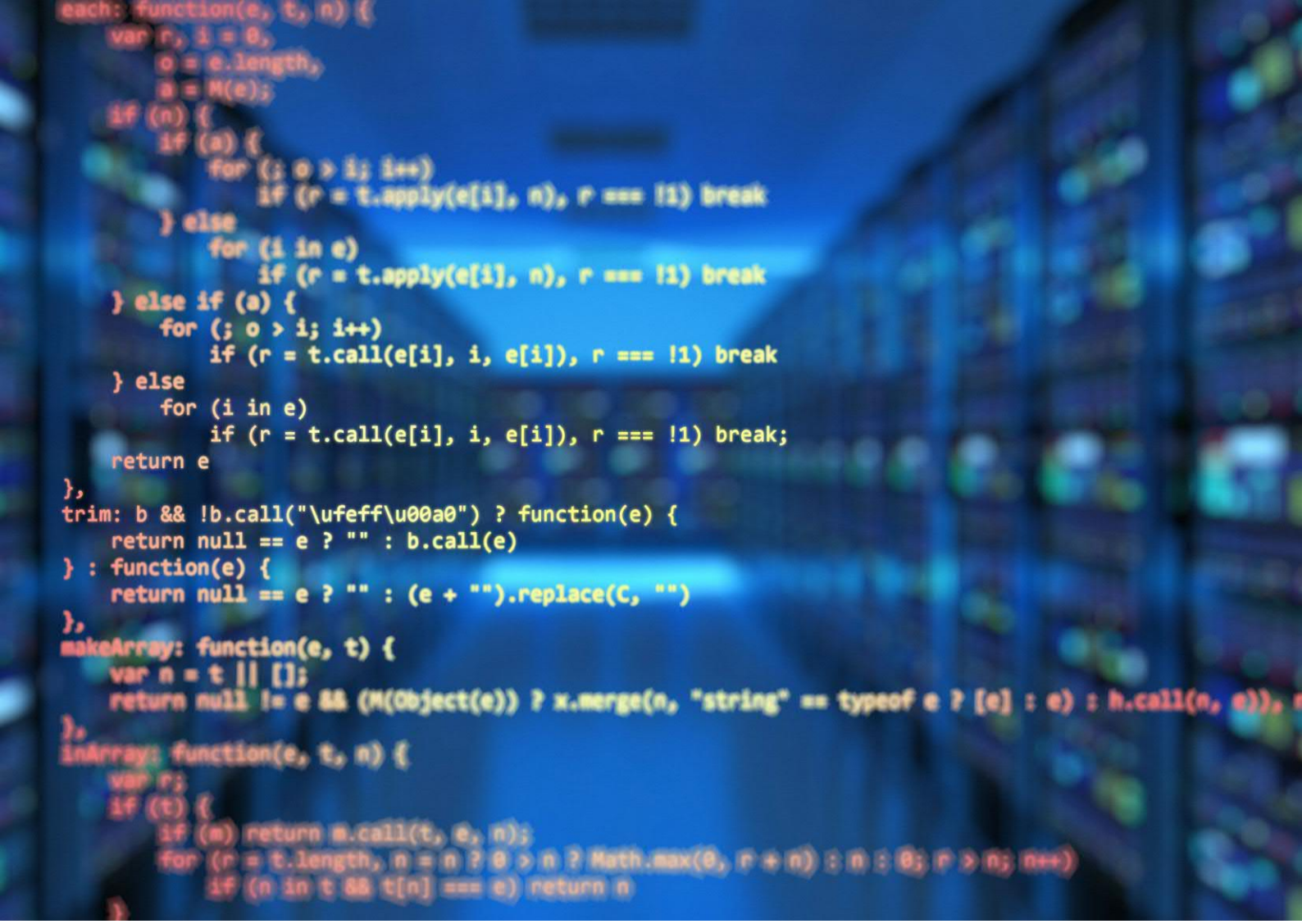
se.MIS™ als Plattform - Teil einer Gesamtlösung

Durch die flexible API und unseren „API-First“-Ansatz lässt sich se.MIS™ mühelos in andere Lösungen integrieren. So können Wartungsaufträge extern erteilt werden oder abgeschlossene Wartungs-aufträge extern weiterverarbeitetet werden.

Durch die intelligente Microservice Architektur von se.MIS™ kann sogar ganz auf unsere GUI verzichtet werden.

se.MIS™ kann aber auch dabei unterstützen, externe Systeme über eine anstehende Wartung zu informieren. Da se.MIS™ den Anwendungsfall „Mensch-Maschine“ abdeckt, ist es wahrscheinlich, dass ergänzende Lösungen eingesetzt werden müssen, die beispielsweise das Netzwerk ständig





auf Anomalien überwachen. Solche **Netzwerk-Monitoring-Lösungen** können über einen Wartungsfall informiert werden, um Alarme durch einen Techniker-Eingriff zu vermeiden.

In microsegmentierten Netzwerken kann **se.MIS™** mittels unterstützter **Firewalls** von Drittherstellern **temporäre Portfreischaltungen** erwirken - nach erfolgter Autorisierung und nur während eines offenen Wartungsauftrages. Dadurch lassen sich „Lücken“ in der Netzwerksegmentierung im Laufzeitbetrieb vermeiden.

Soll ein **vorhandenes Ticket-System** verwendet werden oder ist es notwendig, Informationen mit externen **ERP-Systemen** zur Verrechnung von Aufträgen durchzuführen, kann auf unsere in OpenAPI dokumentierte REST-API zurückgegriffen werden.

Sollen Änderungen am HMI - Display protokolliert werden, so kann auch die API verwendet werden.

Mit Unterstützung von unseren **se.MIS™ U200** USB-Hardware-Sicherheitsmodulen für den industriellen Einsatz lässt sich ein kryptographischer **Betriebsartenwahlschalter** realisieren. So haben mechanische Schlüssel ausgedient und es kann der handelnde Benutzer eindeutig identifiziert werden und seine Befähigung in Echtzeit überprüft werden.

se.MIS™ wird durch seine API zur Plattform und dient als Bindeglied für einen sicheren Maschinenzugriff.

sematicon

Schutz von SPS-Anlagen mit dem PLC-Guard

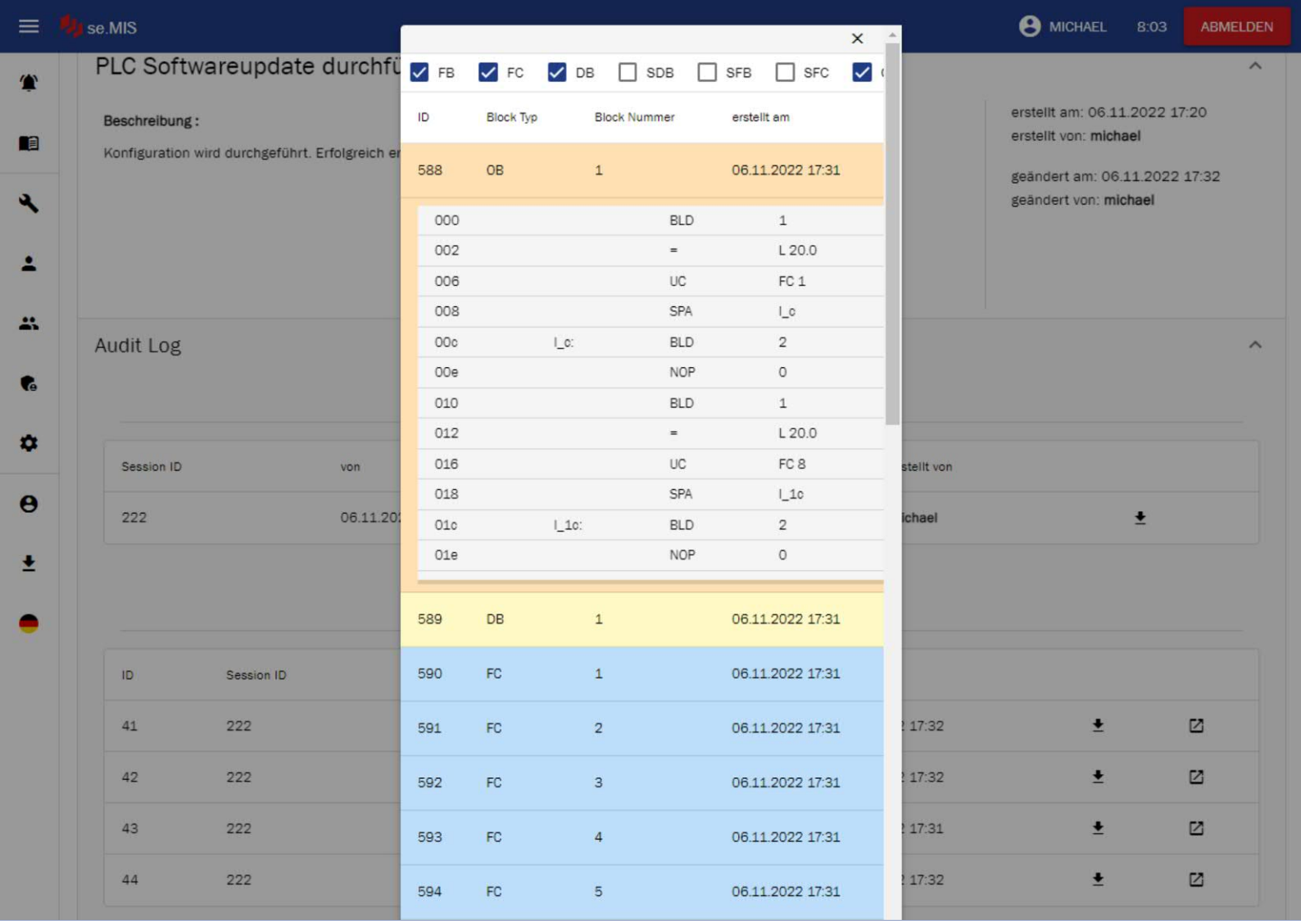
se.MIS™ und der isolierte Zugriff auf SPS Steuerungen

SPS Anlagen sind aufgrund ihres Designs besonders anfällig für Angriffe von außen. Oftmals reicht eine Netzwerkverbindung, um die SPS anzuhalten oder Programmteile zu verändern.

Für den Betrieb wichtige Funktionen wie etwa Softwareänderungen im Betrieb oder das „Device-Discovery“ können aber auch missbräuchlich dazu verwendet werden, um dem System zu schaden. Mittels des „Device-Discovery“-Features lässt sich etwa die SPS eindeutig identifizieren. Sind das Modell und die angeschlossenen Baugruppen bekannt, kann ein Angreifer in den laufenden Code eingreifen. So lassen sich etwa mit einem Befehl alle Ausgänge der SPS aktivieren. Die Zerstörung der Anlage ist dann sehr wahrscheinlich.

Der Aufwand, eine solche Software zu schreiben, ist sehr gering. Außerdem ist der technische Fußabdruck sehr klein und schwer zu erkennen.

Stuxnet war noch viel einfallsreicher bei der Kompromittierung der SPS. Durch eine Manipulation des Netzwerktreibers wurde beim Programmieren der SPS vor dem Verlassen der Netzwerkschnittstelle ein Programmteil angehängt. Eben dieser Teil wurde beim Prüfen des Programms vor Erreichen der Entwicklungsumgebung abgeschnitten. Die Entdeckung war somit schwer bis unmöglich.



se.MIS™ unterstützt durch seine IP-Funktionalität jede Art von SPS-Steuerung, sofern diese über das Netzwerk konfiguriert und programmiert werden kann.

Das Audit-Log speichert in diesem Fall aber lediglich den Netzwerk-Verkehr zur späteren Analyse ab. Der optional lizenzierbare **PLC-Guard** setzt hier völlig neue Maßstäbe. Er erlaubt den Eingriff in die SPS-Kommunikation und die Überprüfung des Quellcodes bevor dieser die SPS erreicht.

Die Prüfung erfolgt dabei unabhängig vom Techniker-PC direkt im **se.MIS™ Manager**. Gemäß dem Zero-Trust-Prinzip ist der Techniker-PC definitionsgemäß eine Gefahr. War dieser einmal mit dem Internet verbunden, besteht die Gefahr einer Kompromittierung durch Schadsoftware.

se.MIS™ isoliert den Zugang des Technikers, der lediglich eine Verbindung zu einer **virtuellen SPS** aufbaut, die innerhalb von **se.MIS™** emuliert wird.

Im Falle eines Programm-Downloads auf die SPS wird der Maschinencode abgefangen und von **se.MIS™** disassembliert. Alle Blöcke sowie der Inhalt in Form der Anweisungsliste (AWL) werden wieder sichtbar gemacht.

Ungeplante Änderungen lassen sich somit auf der „letzten Meile“ vor der SPS identifizieren und es ist sichergestellt, dass nur beabsichtigter Code die Anlage erreicht.

Neben der reinen Protokollierung der Downloads hat der Anlagenbetreiber zusätzlich die Möglichkeit, den Code zurückzuhalten und manuell freizugeben.

Durch die definierbaren Workflows lassen sich Veränderungen zur Vorversion identifizieren und gezielt Backups vergangener Stände direkt aus dem Wartungsbuch auf die SPS laden.

Derzeit unterstützt PLC-Guard den Marktführer SIEMENS S7 - weitere Modelle folgen nach Bedarf.

sematicon

Einbindung alter Anlagen ohne Netzwerkzugriff

se.MIS™ und der Zugriff auf alte Rechner und Systeme

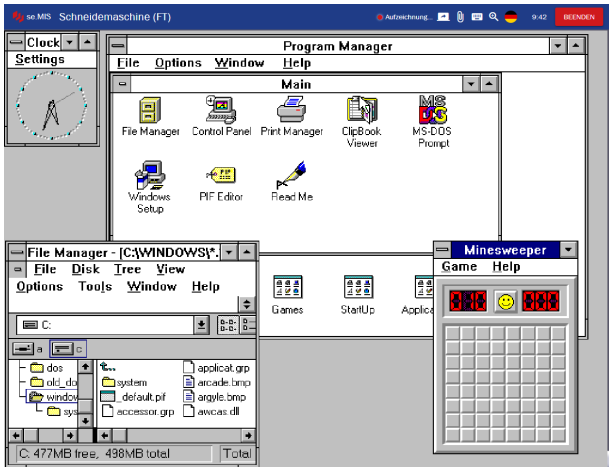
Um möglichst alle Anlagen und Systeme abzudecken bietet **se.MIS™** mit den optional erhältlichen **KVM-Extendern** die Möglichkeit, auch Systeme ohne Netzwerkanbindung ins System einzubinden.

So lassen sich auch Maschinen unabhängig von ihrem Alter und Betriebssystem einbinden. Notwendig ist ausschließlich ein PS/2 und VGA-Port oder ein DVI-Anschluss mit USB.

Der KVM-Extender digitalisiert die analogen Bildschirmsignale, Tastatur und Mauseingaben.

Auch moderne Systeme lassen sich mit dem KVM-Extender anbinden.

Dies ist z.B. bei Systemen nötig, bei denen ein Netzwerkzugriff technisch verhindert werden muss. Über den Extender ist sichergestellt, dass nur Zugriff mit Bildschirm, Tastatur und Maus möglich ist.



Die **se.MIS™ KVM-Extender** Serie

Die **se.MIS™ KVM-Analog-Erweiterung** erlaubt die direkte Verbindung von Tastatur-, Maus- und Bildschirmanschluss eines Steuerungs-PCs. Egal ob MS-DOS, Windows CE oder ein anderes System - mit diesem Extender lassen sich alle Arten von Geräten mit VGA und PS/2 fernsteuern.

Auflösungen bis zu 1600 x 1200 Pixel können problemlos digitalisiert und übertragen werden. Die Stromversorgung erfolgt wahlweise über den PS/2 Anschluss oder über ein optionales Netzteil (5 V DC) und ist somit unabhängig von anderen Stromquellen.

Die **se.MIS™ KVM-Analog-Duo-Erweiterung** bietet gegenüber der Analog-Variante den Vorteil, dass noch ein lokaler Bildschirm oder ein lokales HMI-Panel verbunden werden kann. Der Steuerungs-PC wird mit dem Eingang verbunden und der lokale Bildschirm mit dem Ausgang.

Auflösungen bis zu 1600 x 1200 Pixel können problemlos digitalisiert und übertragen werden. Die Stromversorgung erfolgt wahlweise über den PS/2 Anschluss oder über ein optionales Netzteil (5 V DC) und ist somit unabhängig von anderen Stromquellen.

Die **se.MIS™ KVM-Digital-Erweiterung** kann mit digitalen Systemen über DVI bzw. HDMI verbunden werden. Beim Anschluss über einen USB-Anschluss verhält sich das Gerät wie eine USB-Tastatur bzw. eine USB-Maus. USB-Virtual-Media-Unterstützung kann mittels Lizenz nachgerüstet werden.*

Auflösungen bis zu 1920 x 1200 Pixel sind möglich. Die Stromversorgung erfolgt mittels USB-Anschluss oder über ein optionales Netzteil. Der USB-Anschluss ist ein USB 2.0 Type B.

*Nicht in allen Versionen von **se.MIS™** verfügbar. Bitte gesondert anfragen.

Wir sind das Münchner Unternehmen mit dem Fokus auf IT-Sicherheit und Kryptographie im industriellen Umfeld.

Wir bieten Unterstützung an zu den Themen:

Sicheres Management von Industrieanlagen

Verschlüsselte, nachvollziehbare und sichere Verbindung auf kritischen Mikroprozessor-, Industrie- und Steuerungsanlagen

Kryptographie für IoT, IIoT und Embedded Systeme

Konzeption, Unterstützung und Begleitung bei der Entwicklung sicherer IIoT, IoT und Embedded Systeme

Training und Consulting

Dienstleistungen rund um das Thema Zertifikate (PKI), Kryptographie, Verschlüsselung und sichere Schlüssel-Aufbewahrung (HSM)

sematicon AG
Schatzbogen 56
81829 München
Deutschland

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

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

sematicon
INDUSTRIAL IT SECURITY

DE 2022