Secure Engineering Environment

Automatisierungslösungen cybersicher einbinden

Aktuelle Herausforderung von Automatisierungslösungen

Die Sichtweise auf die Sicherheit von Industrial Control Systems (ICS), welche Automatisierungslösungen zur Steuerung technischer Prozesse beinhalten, hat sich in der jüngeren Vergangenheit gewandelt. Diese Automatisierungslösungen waren lange Zeit abgeschottete Systeme basierend auf proprietären Technologien ohne eine Vernetzung zu Fremdsystemen. Eine Vernetzung mit dem Internet oder vorhandenen Kommunikationsnetzen wurde kaum in Betracht gezogen oder war aufgrund technologischer Barrieren nicht realisierbar.

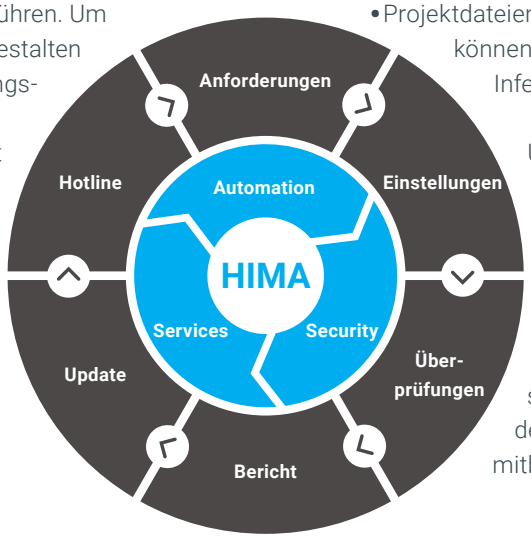
Neben organisatorischen Gefährdungen entstehen auch immer wieder menschliche Fehlhandlungen. Des Weiteren führen vorsätzliche Handlungen und gezielte Angriffe zu erhöhten Risiken von Schäden in Fertigungsprozessen.

Daher ist es besonders wichtig die zur Datenverarbeitung eingesetzten IT Systeme robust auszuführen. Um die Engineering Umgebung secure zu gestalten ist darauf zu achten, dass die Verbindungskontrolle, der Datentransfer und das Monitoring auf hohem Niveau gesichert sind. Aber auch die Härtung (Eingeschränkte Funktionalität des Windows Betriebssystems sowie Malware und Virenschutz) und die Kapselung, bei der Kontrolle aller PC Komponenten welche eine Verbindung zum äußern Umfeld zulassen, das höchste Sicherheitsniveau aufweisen.

Das Herzstück im Engineering Umfeld ist die Engineering Workstation (EWS). Diese gilt es im besonderen Maße abzusichern, da diese die Prozessführung positiv aber auch negativ beeinflussen kann. Diese gilt ins besondere im Bereich der Sicherheitssysteme (Safety Systems, SIL). Mögliche Bedrohungsszenarien, welche sich negativ auf die Produktionsprozess auswirken können, sehen wie folgt aus:

- Infizierte USB Sticks (z.B. im Office-Netz/privaten Umfeld) können durch Schadsoftware ihren Weg direkt in die ICS-Netze finden.
- Wartungsnotebooks können durch Internet-Zugriff, in Office-Netzen oder in der Infrastruktur eines externen Dienstleisters infiziert werden. Werden diese dann im ICS-Netz betrieben, erfolgt die Infektion der dortigen Systeme und Komponenten mit Schadcode.
- Projektdateien oder ausführbare Anwendungen können Schadcode enthalten, der zu einer Infektion oder einem Datenabfluss führt.

Um den Bedrohungen vorzubeugen sind verschiedene technische und organisatorische Maßnahmen erforderlich. Nur so lassen gravierende negative Auswirkungen auf die Anlagenstruktur verhindern. Mit der HIMA Secure EWS erhalten sie ein Produkt, welches nachstehende Eigenschaften zur Erhöhung der Robustheit und Sicherheit bereits mitbringt.



Ganzheitliche Lösung für Automation Security Services

Based on Windows IOT Enterprise LTSC (Long Term Version)

Verbindungskontrolle:
Einschränkung der Netzwerk – Konnektivität auf Verbindungen zur HIMA Steuerungstechnik, HIMA OPC Komponenten bzw. sicheres Portal für den Austausch von Daten und Updates.

Datentransfer:
Sicheres Ein- und Ausschleusen von Daten (Datenschleuse), Verschlüsselung, Authentifizierung usw.

Monitoring:
Aufzeichnung / Logging von Systemereignissen, Anmeldevorgängen sowie administrativen eingriffen.

Härtung:
Eingeschränkte Funktionalität des Windows Betriebssystems sowie Mailware und Virenschutz.

Kapselung:
Kontrolle aller PC Komponenten welche eine Verbindung zum äußern Umfeld zulassen wie z.B. USB Ports, CD/DVD/ Blue Ray, SD Cards, Ethernet Ports, Wifi usw.

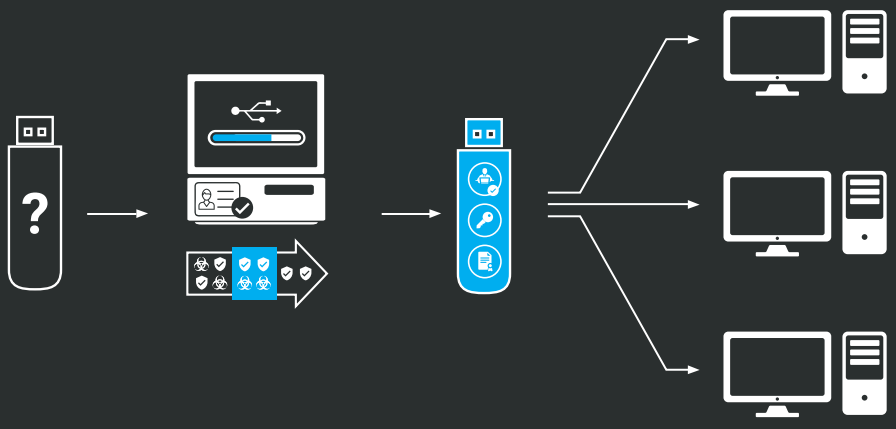
Wenn Ihre Engineering Station entsprechend geschützt ist, wie gelangen dann Ihre Daten sicher von und zur Engineering Station?

Einfache und effektive Lösung: Datenschleuse

Für besonders kritische Umgebungen ist es angeraten das Automatisierungsumfeld zu isolieren. Trotzdem müssen Projekt- und Diagnosedaten von und zu mit dem isolierten System ausgetauscht werden. In vielen Fällen erfolgt dieses durch den Einsatz von Wechseldatenträgern. Um sich dabei vor den oben genannten Risiken zu schützen, bietet sich der Einsatz einer Datenschleuse an.

Die Datenschleuse scannt angeschlossene Wechseldatenträger mit mehreren Virenscannern, so dass nur als sicher eingestufte Daten und Datenträger für das Automatisierungsnetzwerk zugelassen werden. Dabei arbeitet die Datenschleuse unabhängig von vorhandenen Systemen und kann aufgrund von entsprechenden Services wartungsarm betrieben werden.

STARKES DUO: Datenschleuse und Engineering Workstation greifen Hand in Hand



Merkmale der Datenschleuse:

- Durchsuchen von mobilen Datenträgern auf Schadsoftware
- Bis zu drei Virenscanner
- Kopieren sicherer Daten auf einen mobilen Datenträger oder Netzwerklaufwerk
- Protokollierung durchgeführter Vorgänge
- Benachrichtigung bei Virenfund und Auffälligkeiten
- Maintenance und Monitoring
- Fernwartung zur effizienten Problembehandlung
- Patchmanagement
- DriveLock-Unterstützung
- Volle Integration in Ihr Gesamtsicherheitskonzept

Über HIMA

Die HIMA Gruppe ist der weltweit führende unabhängige Anbieter smarter Safety-Lösungen für die Industrie. Mit global mehr als 35.000 Installationen TÜV-zertifizierter Sicherheitssysteme gilt HIMA als Technologieführer der Branche. Die spezialisierten Ingenieure des Unternehmens entwickeln individuelle Lösungen, mit denen Kunden im digitalen Zeitalter die Funktionale Sicherheit erhöhen, Cybersecurity stärken und die Rentabilität ihrer Anlagen und Fabriken steigern. Seit mehr als 45 Jahren gilt HIMA als verlässlicher Partner der weltgrößten Unternehmen der Öl-, Gas-, Chemie- und energieerzeugenden Industrie. Sie alle vertrauen auf Lösungen, Services und Beratungsleistungen von HIMA, stellen so einen unterbrechungsfreien Betrieb ihrer Anlagen sicher und schützen ihre Wirtschaftsgüter, ihre Mitarbeiter und die Umwelt. Zum HIMA-Portfolio gehören smarte Safety-Lösungen, die Daten in geschäftsrelevante Informationen umwandeln und damit zu höherer Sicherheit und Anlagenverfügbarkeit beitragen. Darüber hinaus bietet HIMA umfassende Lösungen für die effiziente Kontrolle und das Monitoring von Turbomaschinen (TMC), Brennern und Kesseln (BMC) und Pipelines (PMC). In der globalen Bahnindustrie sind die CENELEC-zertifizierten SIL 4-Safety-Controller auf COTS-Basis von HIMA führend in puncto Funktionaler und IT-Sicherheit sowie bei der Rentabilität. Das 1908 gegründete Familienunternehmen mit Hauptsitz in Brühl in Deutschland ist heute an mehr als 50 Standorten weltweit vertreten und beschäftigt rund 800 Mitarbeiter weltweit.

Erfahren Sie mehr unter: *www.hima.com*

Sie möchten mehr erfahren? Kontaktieren Sie uns:

Klaus Wagner & Heiko Schween
Abteilung Automation Security
Telefon: +49 (0) 6202 709-128 / -599
E-mail: k.wagner@hima.com / h.schween@hima.com

Oder besuchen Sie uns online auf:
https://www.hima.com/de/unternehmen/cybersecurity

HIMA SMART SAFETY.

www.hima.com