Secure Engineering Environment

Cyber-secure integration of automation solutions

Today‘s automation solution challenge

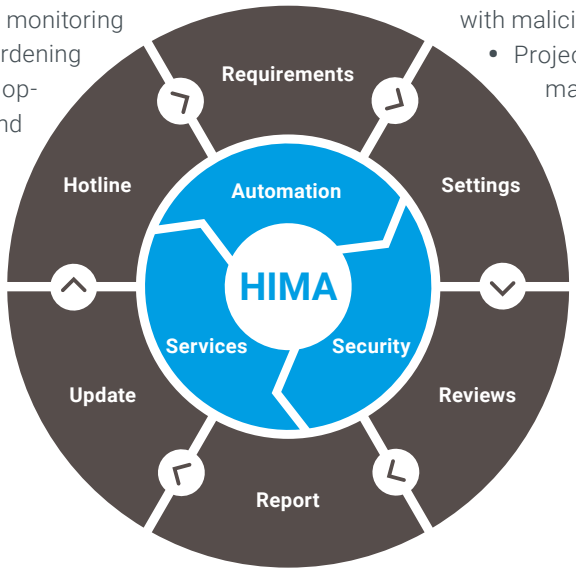
Recently, a change has taken place in the approach to security in Industrial Control Systems (ICS), which include automation solutions for the control of technical processes. For a long time, these automation solutions were isolated systems based on proprietary technologies, without networking to third-party systems. Networking with the Internet or existing communication networks was either not considered or not feasible due to technological barriers. In addition to organizational hazards, human error is a recurring factor. The risk of damage in production processes is increased even further through deliberate actions and targeted attacks.

It is therefore key for IT systems used for data processing to be robust. To make the engineering environment secure, connection control, data transfer and monitoring have to be secured at a high level. Hardening (limited functionality of the Windows operating system, as well as malware and virus protection) and encapsulation when controlling PC components, which allow a connection to the external environment, must also have the highest security level.

The core of the engineering environment is the Engineering Workstation (EWS). Safeguarding the EWS is vital, as it can have a positive or negative impact on process control. This applies in particular to the area of safety systems (SIL). Possible threat scenarios, which could have a negative impact on the production process, are as follows:

- Infected USB sticks (e.g., in the office network/private environment) can directly enter the ICS networks through malware.
- Maintenance notebooks can be infected through Internet access, office networks or the infrastructure of an external service provider. If these are then operated in the ICS network, the systems and components there are infected with malicious code.
- Project files or executable applications may contain malicious code that leads to infection or data leakage. Various technical and organizational measures are required to prevent these threats. This is the only way to prevent serious negative effects on the plant structure.

The HIMA Secure EWS is a product with the following features to increase robustness and safety.



Integral Solution for Automation Security Services

Based on Windows IOT Enterprise LTSC (Long Term Version)

Connection control:
Limiting network connectivity to connections to HIMA control technology, HIMA OPC components or secure portal to exchange data and updates.

Data transfer:
Secure inflow and outflow of data (data gateway), encryption, authentication, etc.

Monitoring:
Recording/logging of system events, login processes and administrative interventions.

Hardening:
Limited functionality of Windows operating system, as well as malware and virus protection.

Encapsulation:
Control of all PC components that allow connection to an external environment, such as USB ports, CD/DVD/Blue Ray, SD cards, Ethernet ports, Wi-Fi, etc.

If your engineering station is properly secured, how is your data transferred to and from the engineering station?

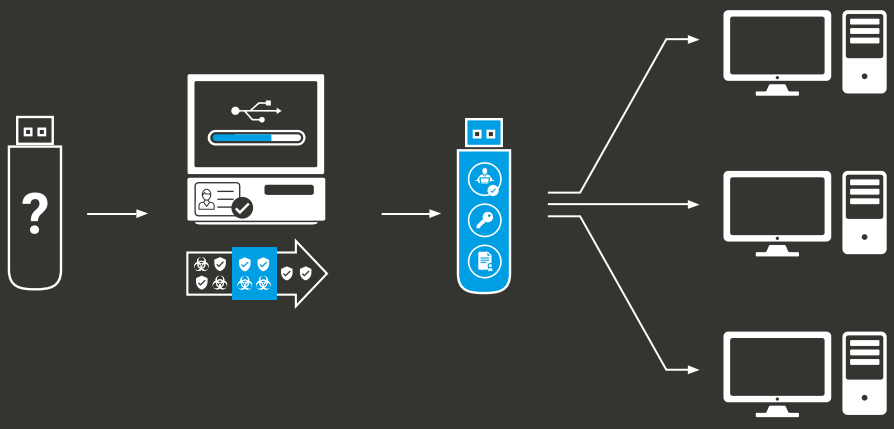
Simple and effective solution: data security gateway

For particularly critical environments, it is advisable to isolate the automation environment. Nevertheless, project and diagnostic data must be exchanged and transferred from and to the isolated system. In many cases, this is done using removable media. To protect yourself from the risks mentioned above, use of a data security gateway is a suitable option.

The data security gateway scans connected removable media with several virus scanners, thus ensuring that only data and media classified as secure are admitted to the automation network. The data security gateway works independently of existing systems and requires little maintenance due to the associated services.

STRONG DUO:

Data security gateway and engineering workstation go hand in hand



Features of the data security gateway:

- Malware scanning of mobile media
- Up to three virus scanners
- Copy of secure data to mobile media or a network drive
- Logging of executed processes
- Notification on detection of viruses or abnormalities
- Maintenance and monitoring
- Remote maintenance for efficient troubleshooting
- Patch management
- DriveLock support
- Full integration in your overall security concept

About HIMA

The HIMA Group is the world's leading independent provider of smart safety solutions for industrial applications. With more than 35,000 installed TÜV-certified safety systems worldwide, HIMA qualifies as the technology leader in this sector. Its expert engineers develop customized solutions that help increase safety, cyber security, and profitability of plants and factories in the digital age. For over 45 years, HIMA has been a trusted partner to the world's largest oil, gas, chemical, and energy-producing companies. These rely on HIMA solutions, services and consultancy for uninterrupted plant operation and protection of assets, people, and the environment. HIMA's offering includes smart safety solutions that help increase safety and uptime by turning data into business relevant information. HIMA also provides comprehensive solutions for the efficient control and monitoring of turbomachinery (TMC), burners and boilers (BMC), and pipelines (PMC). In the global rail industry, HIMA's CENELEC-certified SIL 4 COTS safety controllers are leading the way to increased safety, security, and profitability. Founded in 1908, the family-owned company operates from over 50 locations worldwide with its headquarters in Brühl, Germany with a workforce of approximately 800 employees.

For more information please visit: *www.hima.com*

For further information, please contact us:

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

Or visit us online:
https://www.hima.com/en/about-hima/cybersecurity

HIMA SMART SAFETY.

www.hima.com