framatome

Software OPANASec

Access Protection for Critical Infrastructures

Protect your automation systems against cyber-attacks and espionage

Challenge

The increased interconnectivity of digital systems with numerous, often lowcost industrial devices as well as emerging new security threat vectors require the design and deployment of new security measures. Program code or configuration data of a programmable logic controller (PLC) can be read out or manipulated through interfaces that lack sufficient protection. IT security laws mandate the protection of process and automation systems against cyber-attacks. Any intrusion of unauthorized personnel into automation systems can cause damage to or misuse of critical infrastructures. If systems are compromised, the modifications are often records hard to trace or go undetected. This makes countermeasures even more difficult and thus contributes to further endangering the safety of critical infrastructure.

Solution

The Software OPANASec secures and monitors the integrity of your SIMATIC automation systems. OPANASec Integrity Protection ensures that the software of PLCs is not penetrated and tampered with. OPANASec Integrity Monitoring continuously records any changes to SIMATIC S7-300, S7-400 and S7-1500* controllers facilitating forensic troubleshooting. OPANASec can be quickly configured and is easy to use.

OPANASec protects:

- Critical power supply
- Transport and traffic control
- Drinking water plants
- Nutrition processes
- Medicine and health processes
- Chemicals and pharmaceutical processes.

*in development

Customer benefits

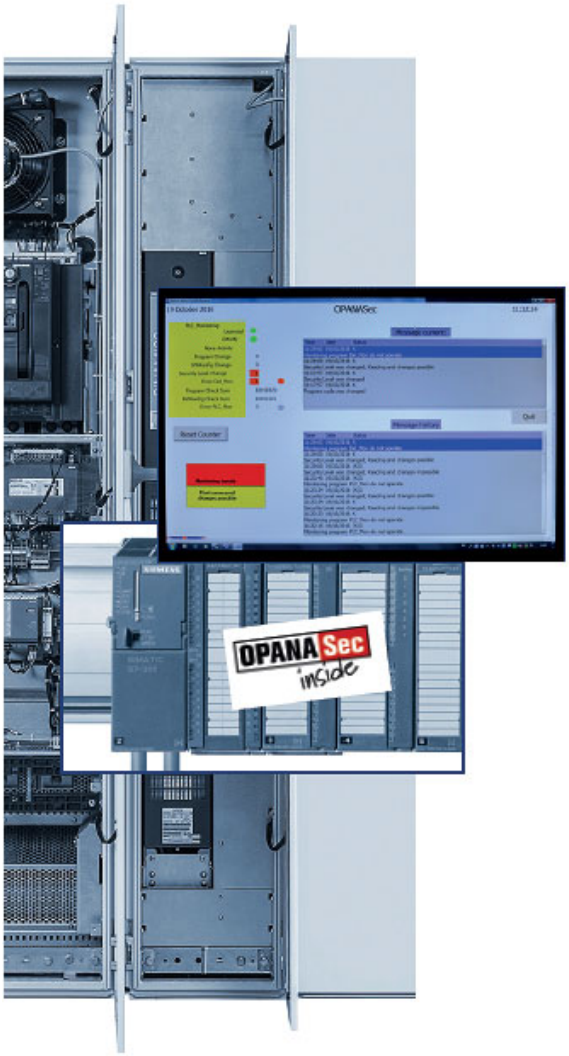
- Ensuring availability of equipment
- Securely blocking the access to systems
- Protection against intellectual property theft, espionage and manipulation of program and configuration data
- Avoid costs through cyber-attacks and liability claims
- Effective threat protection and regulatory compliance

Your performance
is **our** everyday **commitment**

Technical information

OPANASec protects by requiring external approval as well as providing monitoring, log and notification features:

- Any manipulation is detected immediately
- For example, a key switch blocks changes to the program code or the configuration data of the PLC
- Changes in the PLC are recorded in different ways (log file)
- The status and alarm messages can be evaluated as required. In addition, the software includes a built-in self-monitoring function to protect against manipulation of the monitor itself.



Features

- Internal security: built-in access protection and integrity monitoring features
- Easy configuration with popular tools (CFC, LAD, STL, FBD)
- Suitable as a standard solution for S7-300, S7-400 and S7-1500 including F/H/FH systems
- Post attack investigations and evidence (digital forensics support)
- Unrestricted usage of the output signals (HMI, SCADA, SMS, lights, etc.)

HMI = Humane Machine Interface
SCADA = Supervisory Control and Data Acquisition
SMS = Short Message Service

Contact: ic@framatome.com
www.framatome.com

framatome