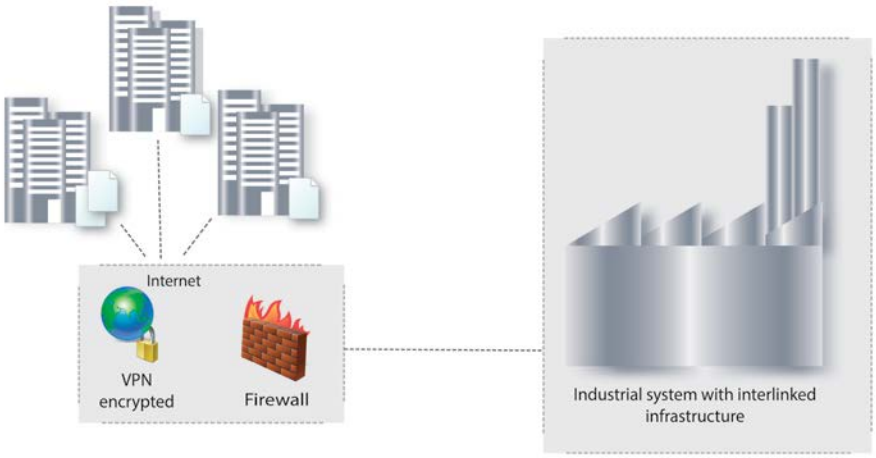
ICS / IPS-Lock

Threats

Stuxnet, Duqu, Flame, Mahdi, Gauss, Shamoon - their various versions and modern variants bring production systems to a stillstand. System security reached the most hurtful points: money, the availability of production.

A rising number of security incidents in Industrial Control Systems (ICS), SCADA and IPS areas has been recorded heavily influencing availability, quality or product liability – thereby also negatively influencing costs and profit. VDMA and BSI point out the high risks. Although successful, these devious attacks often lie dormant until the right moment arises. Component based attacks bringing damage after combining them and using different attack vectors also rise in numbers.



Current IT security situation: VPN and Firewall are the only defensive structures, helping malware to spread out encrypted. Furthermore there is no protection against internal data transfer via USB stick.

The Challenge

Communication between systems has always been a necessity. Integrity and security of processes were controlled through organizational policies by involved persons in authority. Lowering of costs can be achieved by replacing manual data transport with interlinking. Direct interlinks such as USB sticks contradict all concepts of security (monitoring, data integrity, authenticity …). Operators however consider costs from different points of view:

- Productive systems must not be changed, because liability or service levels would be lost.
- Remote maintenance enables fast reactions in critical situations and improves productivity. VPN and Firewalls are insufficient nevertheless, because attacks then will be transferred encrypted via allowed standard ports.
- Collecting quality and further production data through remote access endangers the security of all systems and violates the confidence of data, which in many branches becomes more important in times of industrial and economic espionage.
- The cost reduction through interlinking must be accompanied by invests in security systems

Implementation of efficient security mechanisms in industrial surroundings is a complex challenge. ICS facilities (automation, process control and guidance systems) consist of multi-layered systems for example automation devices like SPS systems and human machine interfaces (HMI) as well as industrial PCs (IPC). The different subsystems have different requirements:

- Heterogeneity of surroundings (i.e. very old operating systems)
- Partially crosslinked systems
- Susceptibility to errors
- Maintenance services
- Availability and integrity

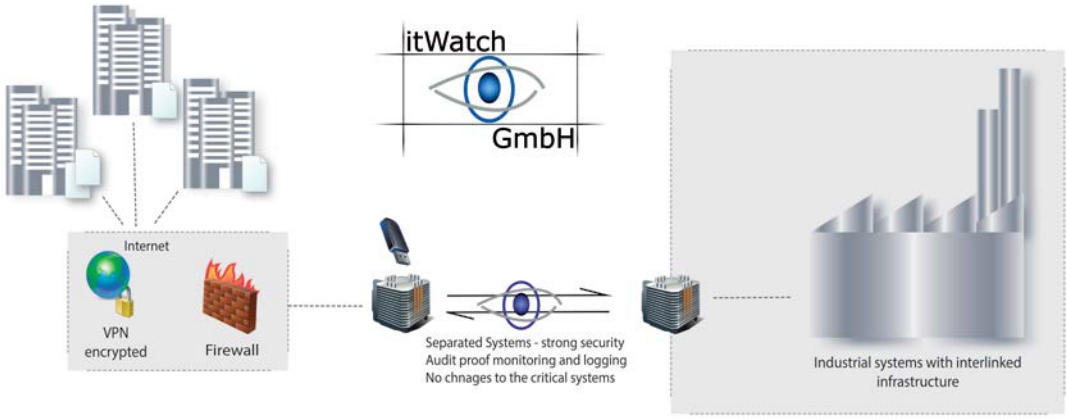
Instead of using conventional IT security mechanisms like authentication, access control etc. that are high in administrational costs, a fully automated process control is more effective. The patented solution of itWatch uses the many advantages of controlled processes in a securized workflow. Every single access as well as data manipulation are recognized and allowed or restricted according to the acting process. Audit proof logging is included. Encryption of confidential results with a company key ensures the security of your data.

The Solution

The proven technology of itWatch utilizes different product components and expertise to create a sophisticated product for the protections of industrial systems.

- Any file can be checked depending on specific regulations. Without changing the product these regulations (pattern definitions) can be customized easily according to the customer's needs.
- All ports and connected devices of a system are identified, authenticated, monitored and depending on the data content approved or blocked.
- Without implementing code into the data control system, remote systems can be integrated.
- Well-matched to specific needs confidentiality is guaranteed by encryption with user defined keys or company keys.
- Logging of complex system conditions, changes to systems, data transfer and data leakage are key points of this product. Audit proof evidence of all activities is recorded.
- Automatic execution within a securized workflow and monitoring of actions are accompanied by applying the necessary privileges in the right moment (event triggered). The right parameters are identified automatically or defined directly within secured user dialogues.

The system works on standard systems or as appliance integrated in the network. In special cases the complete bundle including the decoupled systems is offered as a mobile device.



Data and application lock divides the networks logically and transparent for the user.

Use Case

Untrustworthy employees abroad have to collect quality data from measuring stations using a portable storage device. Instead of authorizing the employee to log in, connect the device and read the data, itWatch's ICS/IPS lock offers the following solution scenarios:

Solution 1 with code on the measuring computer:
A specific encrypted device which can be authenticated is used to transfer the measuring data directly after connecting it to the station. The process runs fully automated without interaction between machine and employee. A Login is not needed.

Solution 2 without code on the measuring computer:
The measuring systems are linked to the Decoupled Systems (Remote Controlled Application System). The double lock systems and automation component control the data transfer automatically and if needed encrypt it. This system can be linked fixed or be integrated as a mobile device.

About itWatch

The products of itWatch follow a more than 15 years lasting tradition. Their stability and reliability is documented in millions of systems active every day. The products were approved for usage in highly secure environments labelled with a military 'Secure' classification in 2003. Since then they show their sturdiness and dependability in cases of aggressive attacks on a daily basis.