

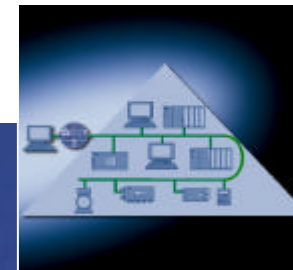
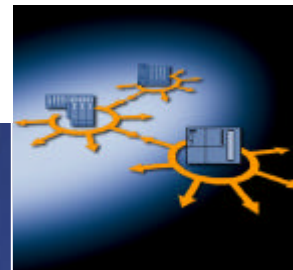


Industrial Security Automation Systems vendor's point of view

Axel Gruner SIEMENS AG A&D PT2 M

You want to utilize current technological trends in automation

- Trend away from centralized control structures towards distributed local units
- Use of Ethernet at all levels of automation
- Increased use of open IT standards in automation
- IT and automation world are growing closer together





Sources of danger from increased networking

Networking with Industrial Ethernet also at the field level. Implicit protection from fieldbus protocols is lost

Greater potential danger

Automation islands "grow" together on the shared cable

**Mutual influence
Addressing errors**

Automation network is connected with office network

**Mutual influence
Addressing errors
Unauthorized access**

Remote client accesses from insecure networks (Internet, WAN, wireless LAN)

**Danger of attacks (DoS, ..)
Danger of espionage
Danger of manipulation**

Sites are networked together

**Danger of attacks (DoS, ..)
Danger of espionage
Danger of manipulation**



Objectives of IT Security

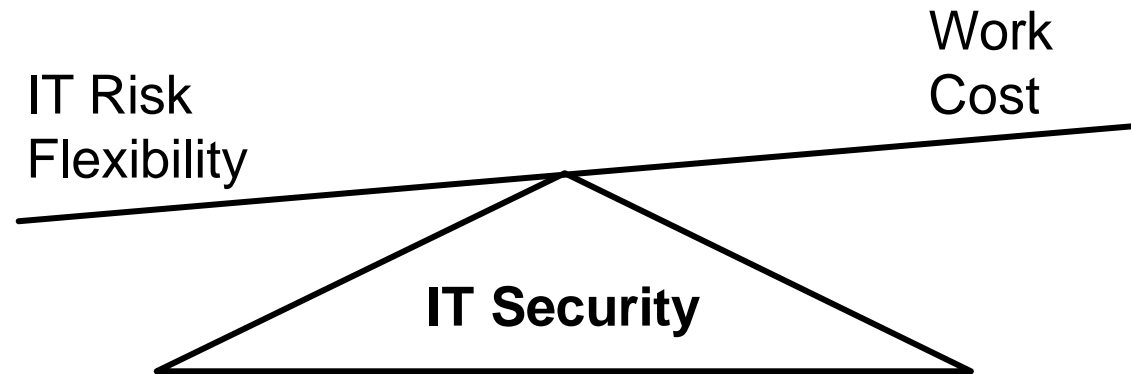
In general, IT Security must ensure:

- Data availability
- Data confidentiality
- Data integrity (uncorrupted data)

Most important objective in production:

- Permanent availability of the control systems
- No production downtimes
 - **due to IT security problems**
 - **due to IT security measures**

IT Security – a Compromise



IT security costs money and requires work

Flexible systems with comprehensive functions always involve a high IT risk

IT security problems also involve costs, e.g. caused by production loss

Security is always a compromise



General security requirements in automation

- Protection of programmable controllers against unauthorized access
 - access control and filtering of data traffic
- Protection of data transmissions against espionage and manipulation → data encryption
- Secure identification of communication partner
 - secure authentication mechanisms
- Protection against malicious software (viruses, worms & Trojan horses)
 - Even without virus scanners, since they cannot always be used due to performance requirements, system incompatibilities or high overhead
- Transparent interventions with ability to initiate countermeasures in the case of access violation
 - Logging of security-relevant events

Special demands on industrial security in automation

Ease of use

- Expert knowledge in security can not normally be anticipated
- Commissioning and maintenance must require as little overhead as possible

Reaction-free and transparent

- No changes to existing network topology
- No reconfiguration of existing network nodes
- Protocol-independent data traffic security

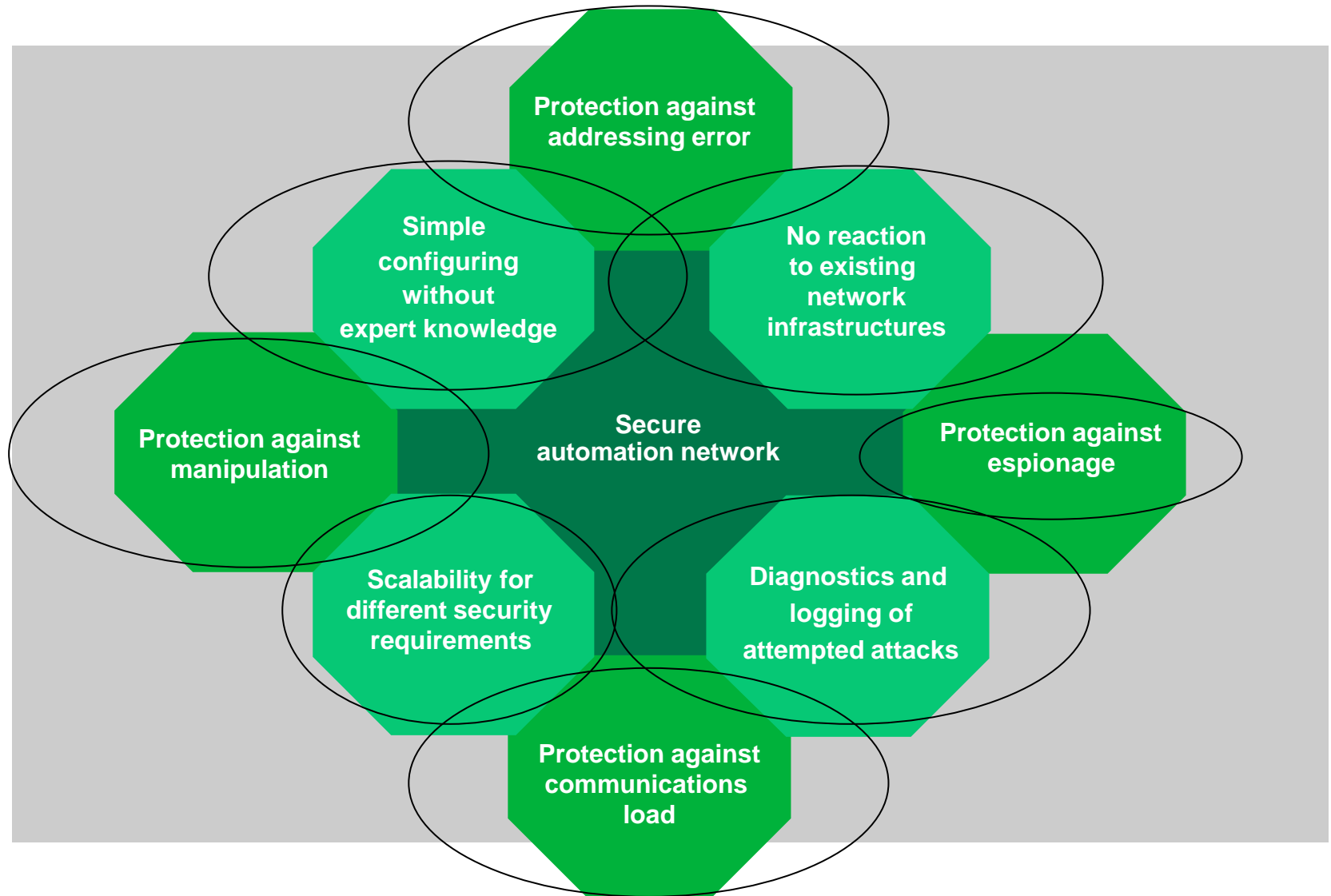
Real-time capability and security must not be mutually exclusive!

Minimize risk of viruses, worms and Trojan horses even without burdensome virus scanners

→ These special demands are not fulfilled by office security solutions!



Security requirements in automation networks





Thank you.