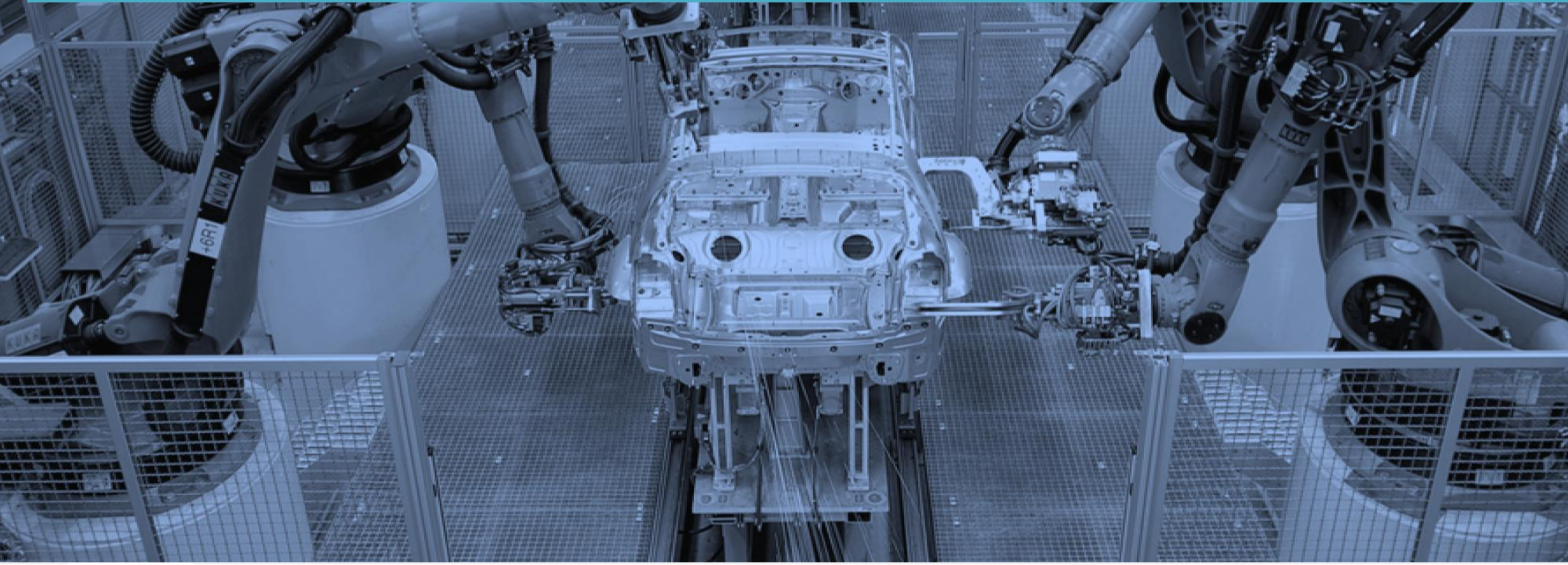
Stuxnet zum Frühstück
Industrielle Netzwerksicherheit 2.0

Stuttgart und München



TÜV SÜD

HIRSCHMANN
A BELDEN BRAND

secXTREME
Information Security

YELLO NETCOM

Choose certainty.
Add value.

TÜV SÜD Embedded Systems

Sicherheitsthemen für Ethernet basierte Systeme in der Industriellen Automatisierung

TÜV SÜD AG
Munich, June 30st, 2011

TÜV SÜD HIRSCHMANN A BELDEN BRAND secXTREME Information Security YELLO NETCOM

AGENDA

1 The Industrial Systems in the past

2 Ethernet as Communication Interface opened the door ...

3 Aspects of Attacks

4 The challenge for Industrial IT-Security

Encapsulated Embedded Systems as Stand-alone Systems

Industrial Systems in the past

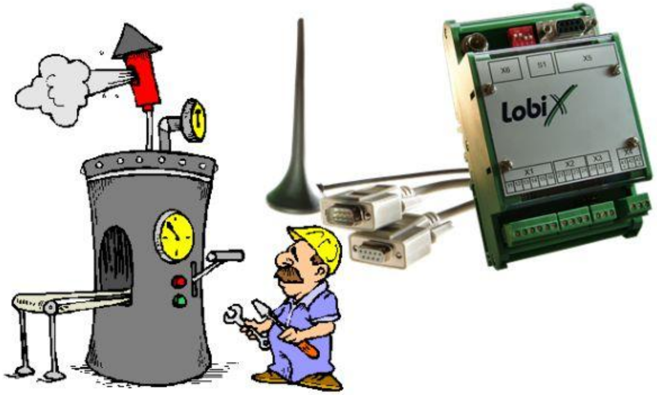
- Stand-alone systems, no access from the out-side

- Access only for trained employees

Added Communication Capabilities

Industrial Systems were extended with communication interfaces

- Connected Systems over field-busses (RS-232/-422/-485, CAN, …)
- Encapsulated control networks over Ethernet
- Proprietary Applications



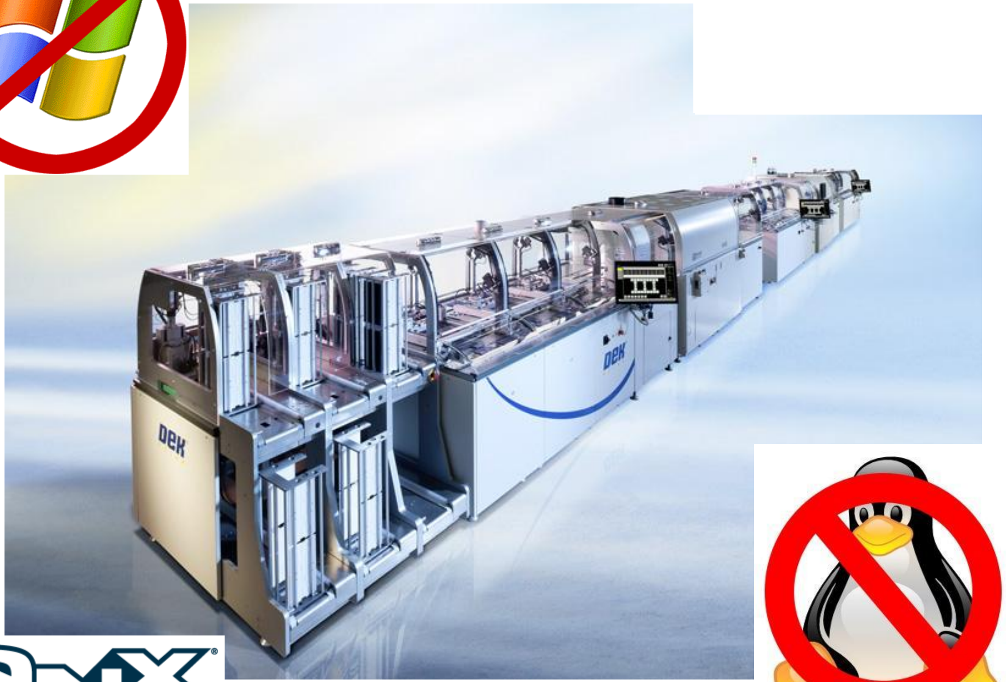
Special Embedded Systems

Industrial Systems were based on special designs

- Application runs directly on the Hardware without an Operating System

- Special, not common Operating Systems like VxWorks or QNX were used

VxWorks



QNX

AGENDA

1 The Industrial Systems in the past

2 Ethernet as Communication Interface opened the door ...

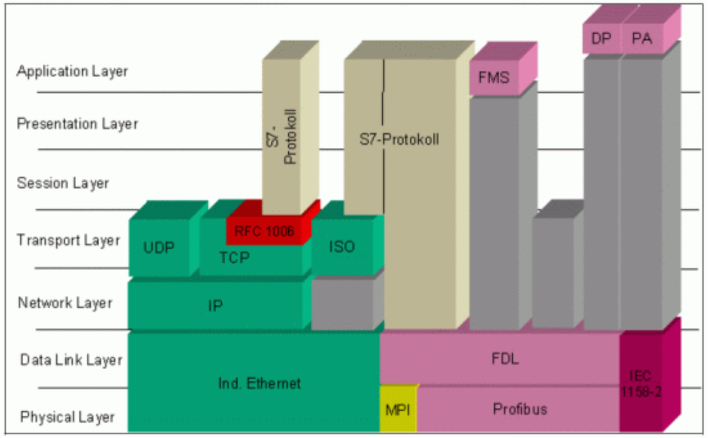
3 Aspects of Attacks

4 The challenge for Industrial IT-Security

Ethernet – A standardized Communication Interface

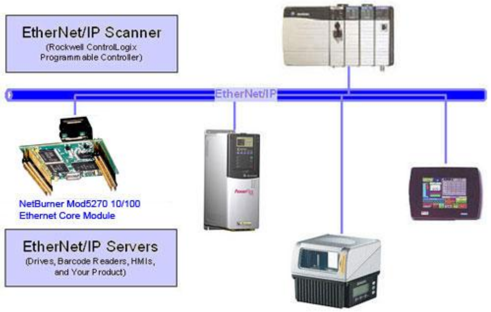
Ethernet is an open standard

- Ethernet is an open defined standard to connect several systems together
- The data is usually transferred over the network in clear text mode without any security
- Data is snoop-able during the transfer over the Ethernet



Ethernet used for Communication

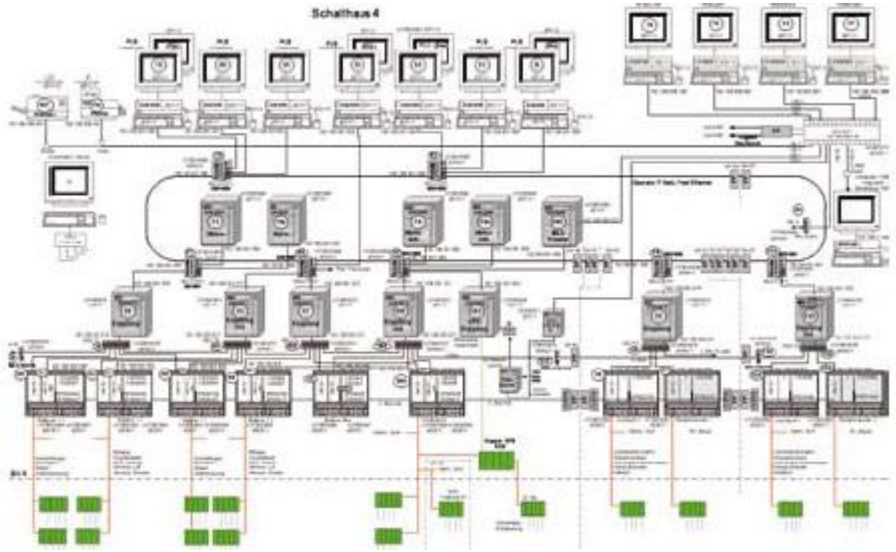
Ethernet for data, command and control



EtherNet/IP Scanner
(Rockwell ControlLogix Programmable Controller)

NetBurner Mod5270 10/100 Ethernet Core Module

EtherNet/IP Servers
(Drives, Barcode Readers, HMIs, and Your Product)

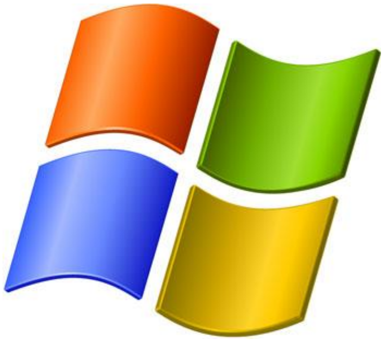


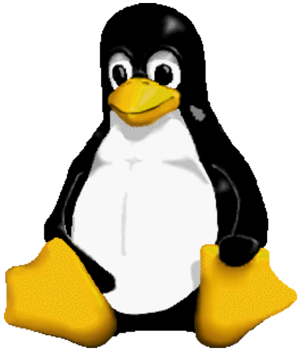
Ethernet is used for:

- Encapsulated networks
- Local networks
- World Wide Web

Common used Operating Systems and Ethernet Security Issues

Ethernet is not secure by itself





- Ethernet provides no security by itself
- Every Operating System have Security Lacks at the Ethernet Interface
- Common used Operating Systems have well known Security Holes and therefore easier targets for Security Attacks

AGENDA

1 The Industrial Systems in the past

2 Ethernet as Communication Interface opened the door …

3 Aspects of Attacks

4 The challenge for Industrial IT-Security

Differences between Office and Industrial IT Security Attacks

What are the intentions for IT Security Attacks

- Security Attacks on Office networks are usually target on knowledge
- Same applies for Industrial Systems, but …
- … espionage is not the only aspect
- Sabotage of Industrial Systems over the Ethernet can happen

Type of Industrial IT Security Attacks

How to get into a Industrial System

- Industrial Systems connected directly or indirectly to the World Wide Web can be a target of Attacks
- There are different kinds of attacks:
  - ➢ Security Lacks in Ethernet Services (like Telnet, FTP, DNS)
  - ➢ Viruses and Trojans can be implemented over emails or by infected USB Sticks
- The basis for an attack might have a commercial, but also a political background.

AGENDA

1 The Industrial Systems in the past

2 Ethernet as Communication Interface opened the door …

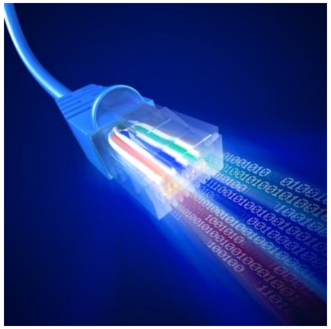
3 Aspects of Attacks

4 The challenge for Industrial IT-Security

Requirements of Industrial Systems

Limits and limitations for Ethernet communication between Industrial Systems

- Industrial Systems communication requirements:
  - Performance requirements
  - Real Time requirements
  - Tested and Proven – no further changes are allowed
- These requirements are the limitations of Intrusion Prevention Systems and Firewalls



Solutions for Industrial Systems Security

Possibilities to protect Industrial Systems

- Usage of network topologies to prevent Industrial Systems from access or data exchange over the web
- Usage of encryption like TSL for all access and data transfer to the web if this is necessary
- Usage of special security enhancing tools like HoneyBox

Thank you for listening

Questions

Suggestions