Analyse des Stuxnet-Wurms

IT-SeCX 2010

FH-St. Pölten

12.11.2010

Georg Kremsner, MSc

Überblick

- Besonderheiten
- Verbreitung
- Aktionen des Wurms
- Anlageninfektion
- Schadenspotenzial
- Desinfektion
- Vorbeugung

Besonderheiten

- **Erster Angriff auf Industrie-Steuerungen**
  - Sicherheitskonzepte ausgehebelt
- **komplex und mehrere Komponenten**
- **Entwicklerteam**
- **kein kommerzieller Hintergrund erkennbar**
- **geheime Entwicklung**
- **„gestohlene“ Zertifikate (Windows-Treiber)**
  - Realtek, JMicron

Verbreitung - MS08-067

- bekannt von Conficker
- Dateifreigaben
- Lücke im RPC-Dienst
- Starten von Stuxnet
- Patch Oktober 2008

Verbreitung - MS10-046

- **LNK-Schwachstelle**
- **Beim Anzeigen einer Verknüpfung**
- **Auflösung von Symbolen (führt DLL aus)**
- **Erst in späteren Versionen von Stuxnet**
- **Frühe Versionen von Stuxnet**
  - autorun.inf (beim Anstecken von USB-Stick)
- **Patch August 2010**

Verbreitung - MS10-061

- **Druckerfreigabe**
- **„drucken“ von Dateien in %system%**
  - zeigt auf C:\Windows\system32
- **Starten von Stuxnet**
- **Patch September 2010**

Verbreitung - Step7

- **Projektdateien von SIMATIC Steuerungen**
- **Infektion der Projekte**
- **Öffnen eines infizierten Projekts**
  - Infektion des Rechners
    - Infektion weiterer Projektdateien
- **3 Generationen von Dateien**
  - Eindämmung der Verbreitung
  - Ausreichend für tiefe Infektion des Netzwerks

Verbreitung - WinCC

- **Datenbankdienst für Steueranlagen**
  - Standard-Passwort
- **Infektion des Datenbankservers durch Malformed SQL-Request**
  - Weiterverbreitung von dort aus
- **Einrichten von Stored Procedures**
  - Wertespeicherung
  - Verstecken von Stuxnet in der DB

Elevation of Privilege - MS10-073

- **Systemrechte erlangen**
- **manipulierte Konfigurationsdatei**
  - Keyboard Layout
- **ermöglicht tiefe Eingriffe ins System**
- **Patch Oktober 2010**

Elevation of Privilege - Task Scheduler

- Systemrechte erlangen
- umgeht UAC (User Account Control)
- ermöglicht tiefe Eingriffe ins System
- Patch nicht vorhanden

Aktionen des Wurms - PC

- **Einnisten im System**
  - Verstecken von Stuxnet (dig. Sig. Rootkit)
  - Methoden zur Abwehr von Virenscannern
  - Infektion von Siemens Programmiersoftware
  - Weiterverbreitung
  - Kommunikation mit anderen Stuxnet-Installationen und C&C-Server
- **Gegenseitige Updates im Netzwerk (P2P)**

Stuxnet Digitale Zertifikate

Verdächtigkeit der Zertifikate (Aus Sicht eines Virenschreibers)

- Adobe = PDF Viewer/Writer
- Microsoft = Windows, Office
- Nvidia = Grafikkarte
- Realtek = Soundkarten, NIC, USB, I/O Bausteine
- JMicron = USB, SATA
- Siemens ???

Auswahl war: Realtek, dann JMicron

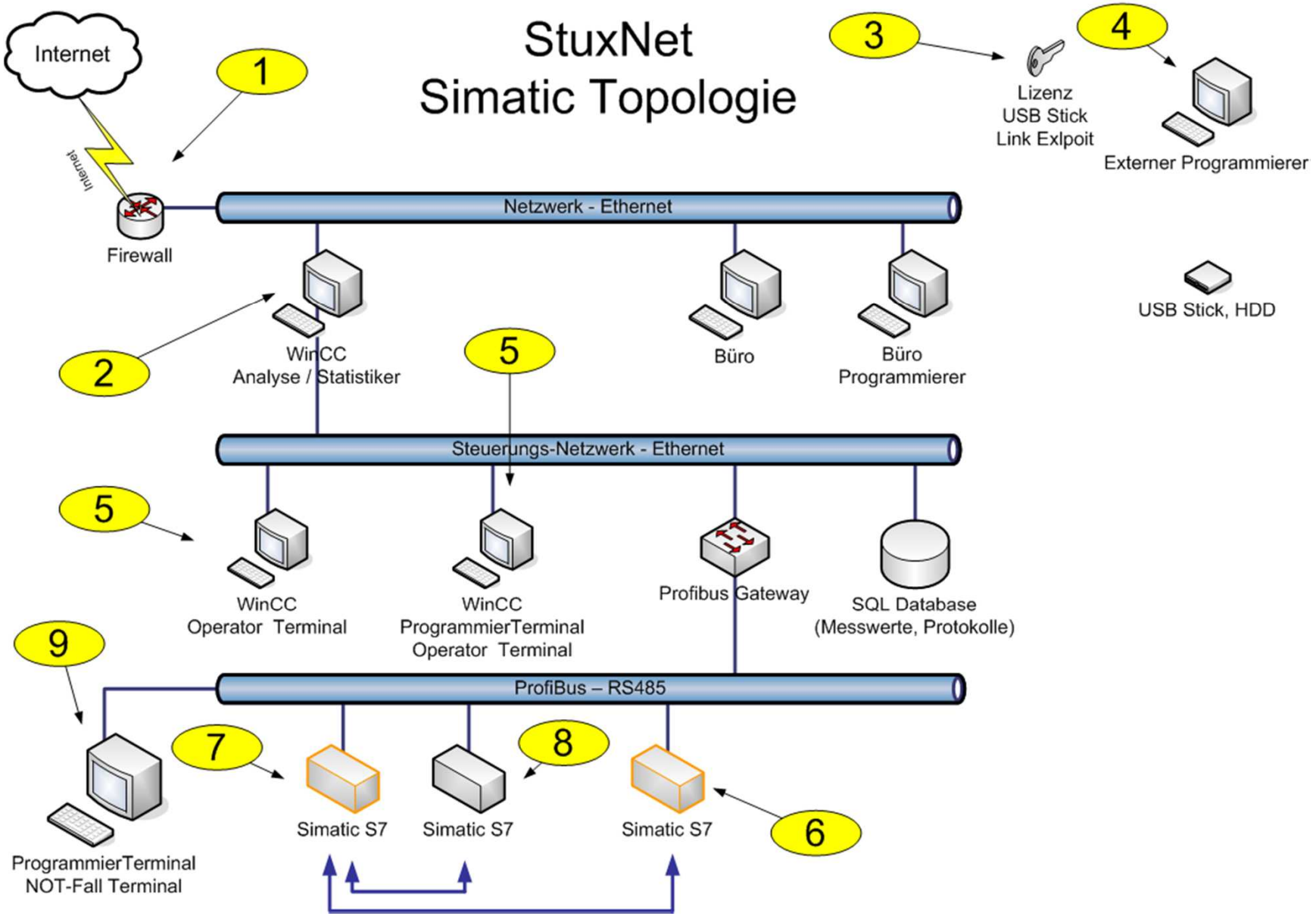
Aktionen des Wurms - S7

- **Modifikation von Step7 / WinCC**
  - Verstecken von Stuxnet
  - Schutz von Stuxnet
- **Infektion von Steueranlagen (SIMATIC S7)**
  - Ersetzen/Modifizieren von Codeblöcken
  - Spionage?
  - Sabotage?

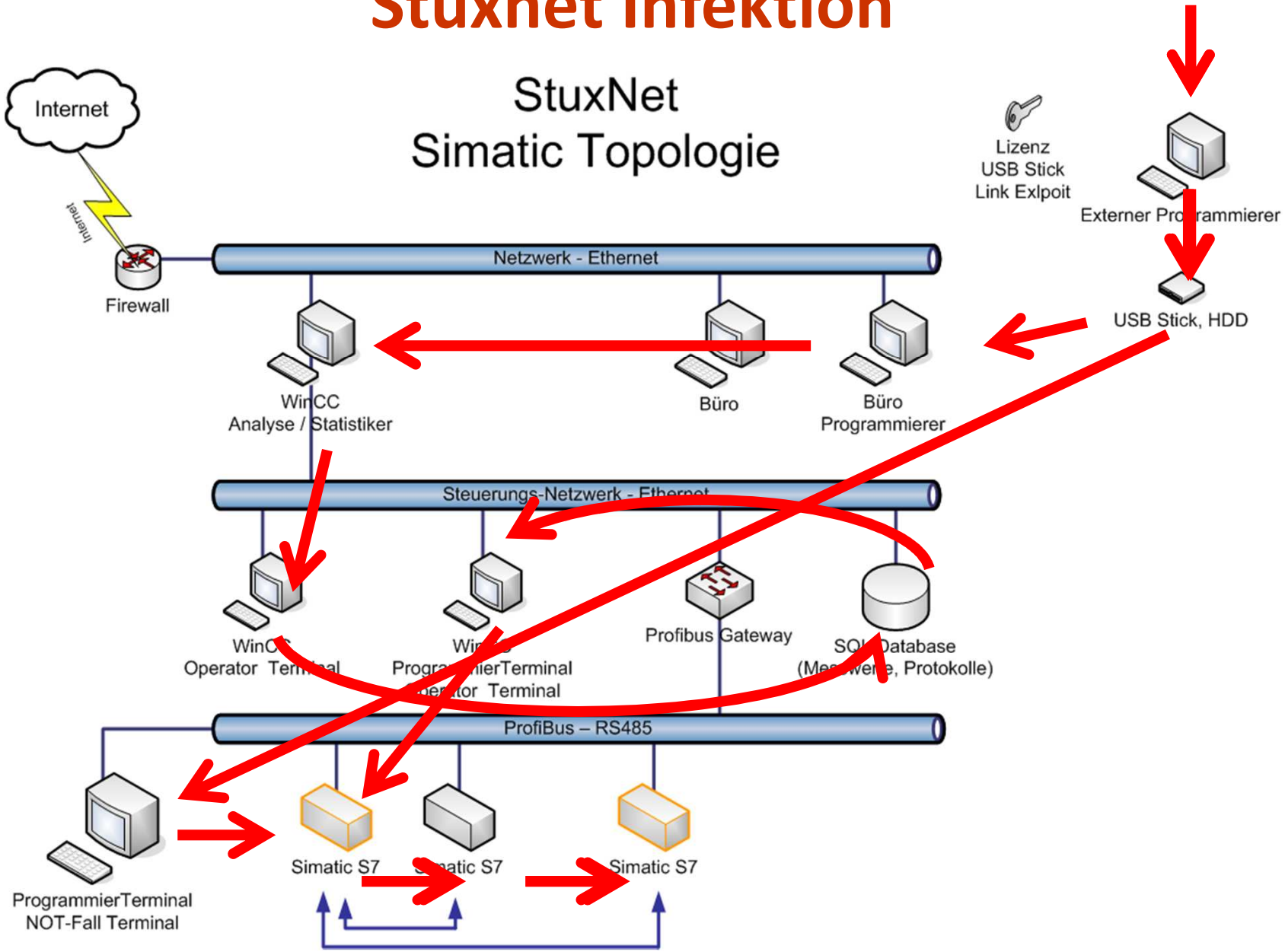
Schadenspotenzial

- **Abhängig von der Anlage**
  - Auswirkungen auf S7 nicht vorhersehbar
  - Sabotage möglich
  - Störung möglich
  - keine öffentlich bekannten Vorfälle
- **„normale“ PCs unerheblich**
  - nur Weiterverbreitung
  - durch Architektur alles möglich
  - C&C Server bereits down

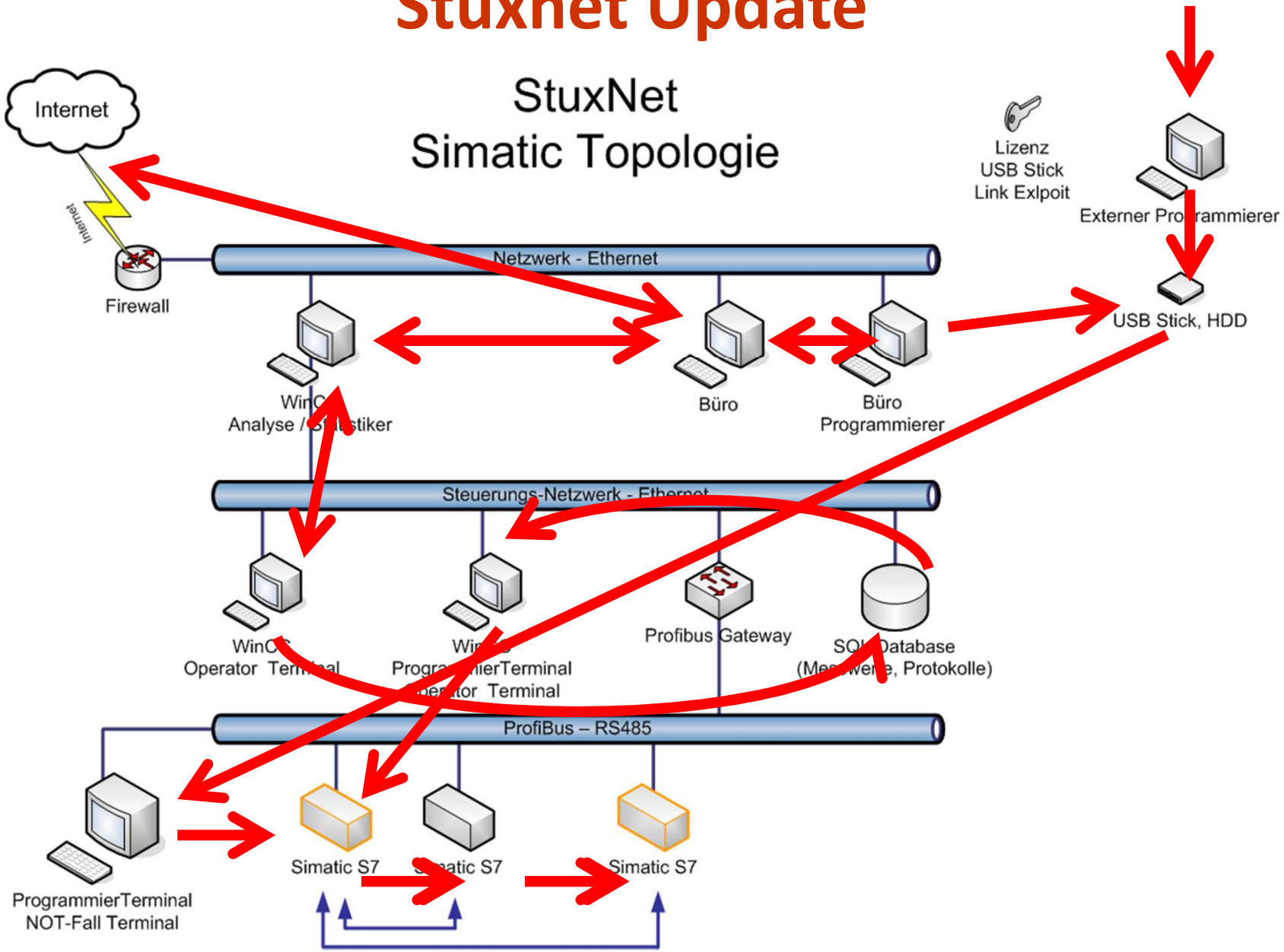
Schema einer Industrieanlage



Stuxnet Infektion



Stuxnet Update



Desinfektion

- **PC / Netzwerk**
  - Infizierte PCs vom Netzwerk trennen
  - Einzel-Desinfektion
  - Entfernen aller Komponenten (SYSCLEAN)
  - Neustart
  - Patches & Virenscanner
  - Neustart (zurück ans Netzwerk)
- **SIMATIC S7**
  - Projekt-Backups mit sauberem PC einspielen

Vorbeugung

- **PC / Netzwerk**
  - Patches
  - Virenscanner
  - Sicherheitskonzept
- **SIMATIC S7**
  - Sicherheitskonzept

Probleme industrieller Anlagensteuerung

- System ist offline/abgeschottet
- „Never touch a running system“
- Programmiergeräte und Software steinalt
- Steuerung ist Rand-Problem von Produktionsanlagen (Untergeordnetes Mittel zum Zweck)
- „Steuerungs-Einheitsbrei“

Fragen