Smashing PLCs for Fun and Profit

Einführung in ICS Security

Compass Security
Network Computing AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61

team@csnc.ch
www.csnc.ch

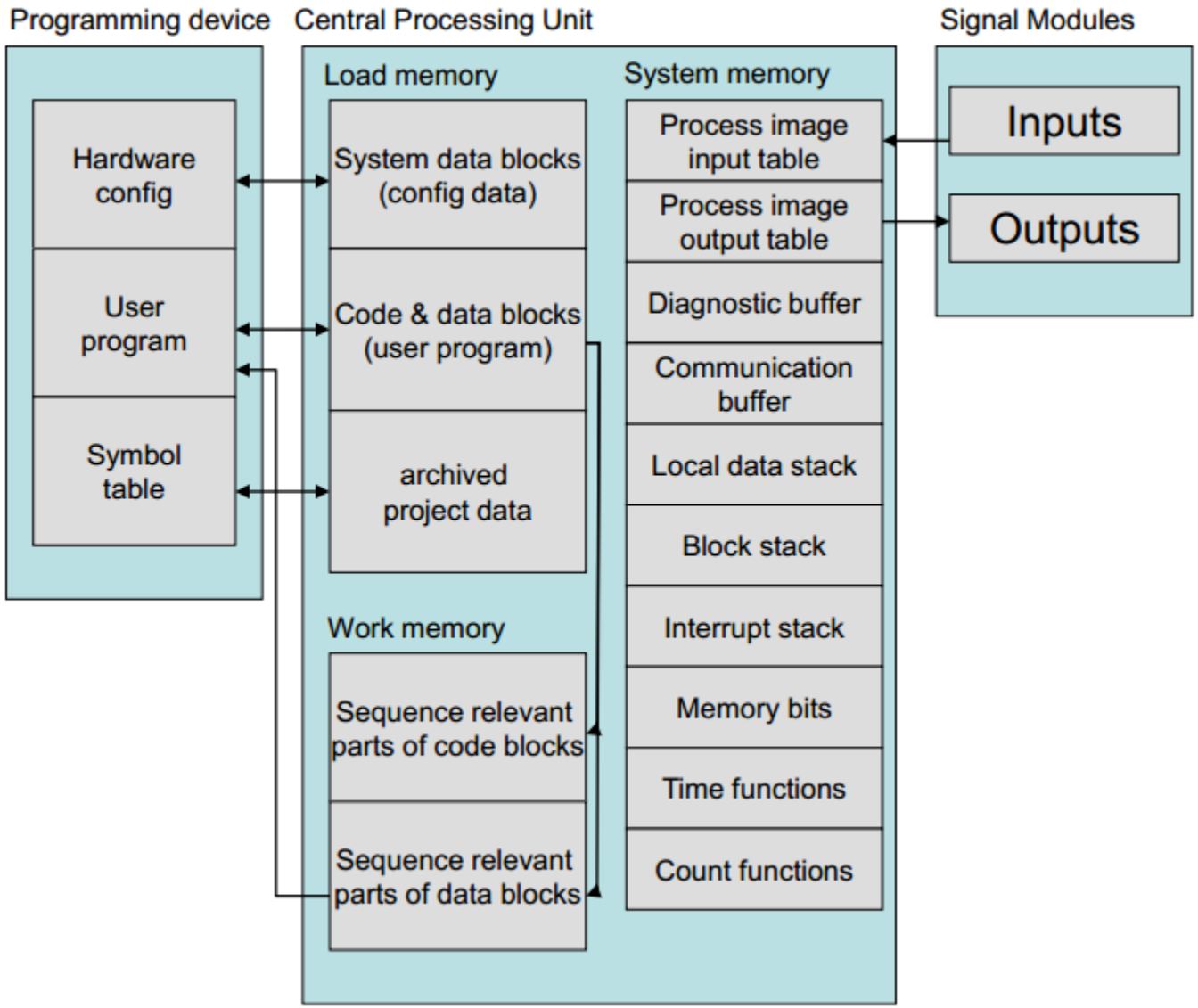
Gliederung

1. Einführung in Industriesysteme
2. Angriffe
3. Security Guidelines
4. Forschungsthemen
5. Checkliste

Einführung in Industriesysteme

Programmable Logic Controller (PLC)

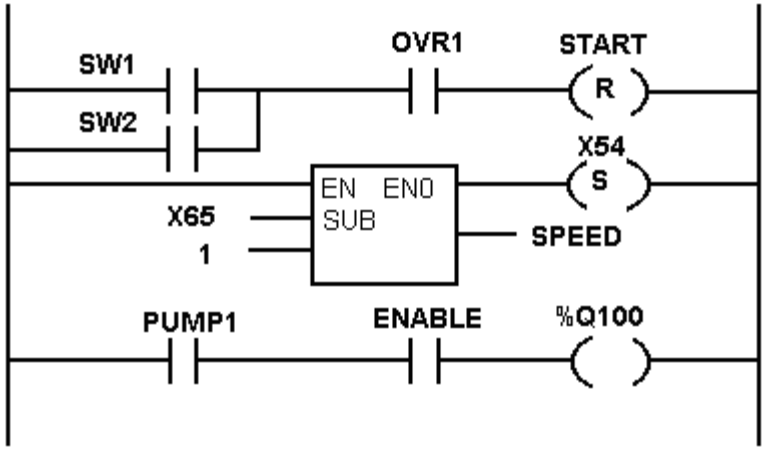
PLC

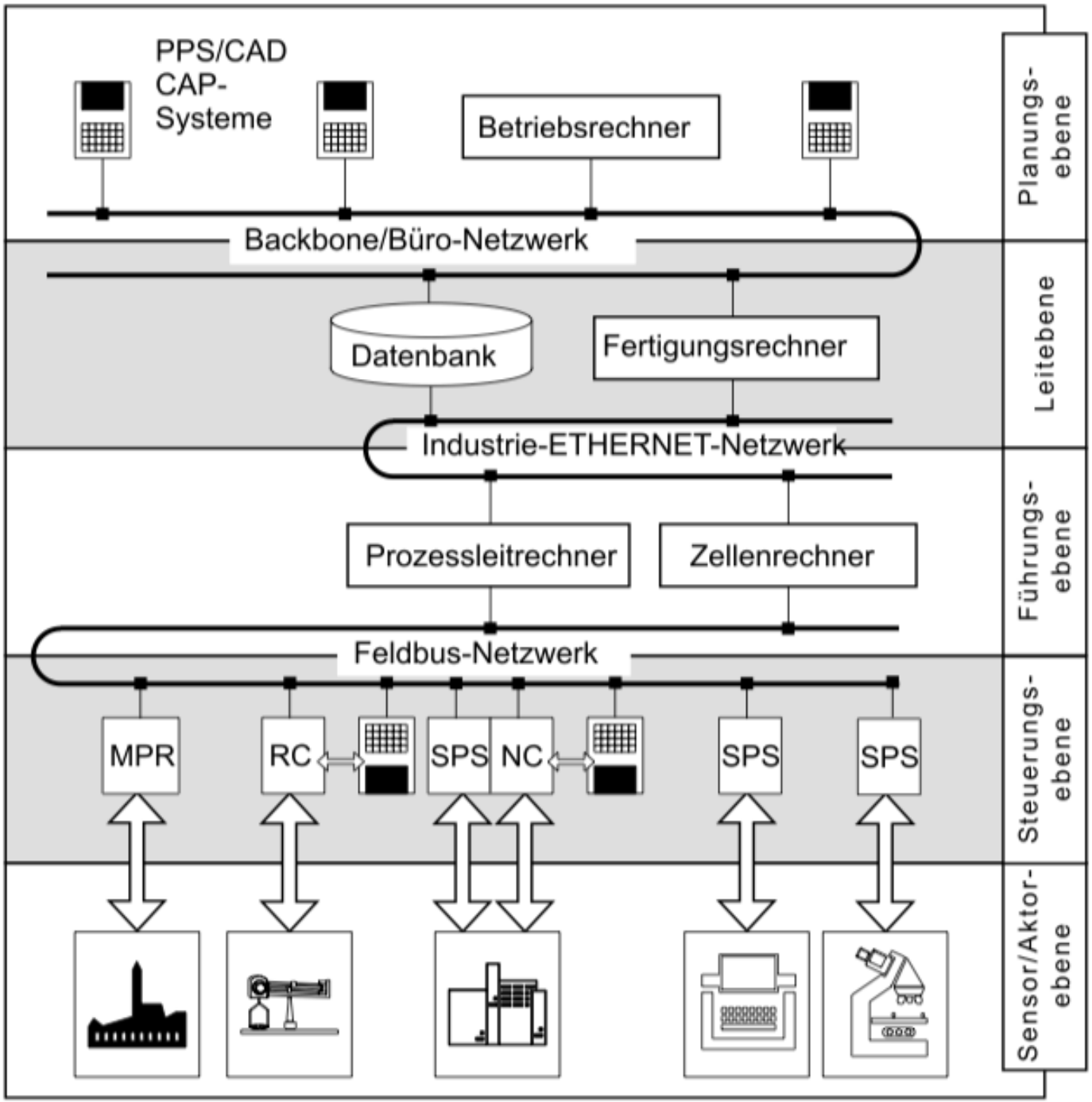

Programming device
Central Processing Unit
Signal Modules
Hardware config
User program
Symbol table
Load memory
System data blocks (config data)
Code & data blocks (user program)
archived project data
Work memory
Sequence relevant parts of code blocks
Sequence relevant parts of data blocks
System memory
Process image input table
Process image output table
Diagnostic buffer
Communication buffer
Local data stack
Block stack
Interrupt stack
Memory bits
Time functions
Count functions
Inputs
Outputs

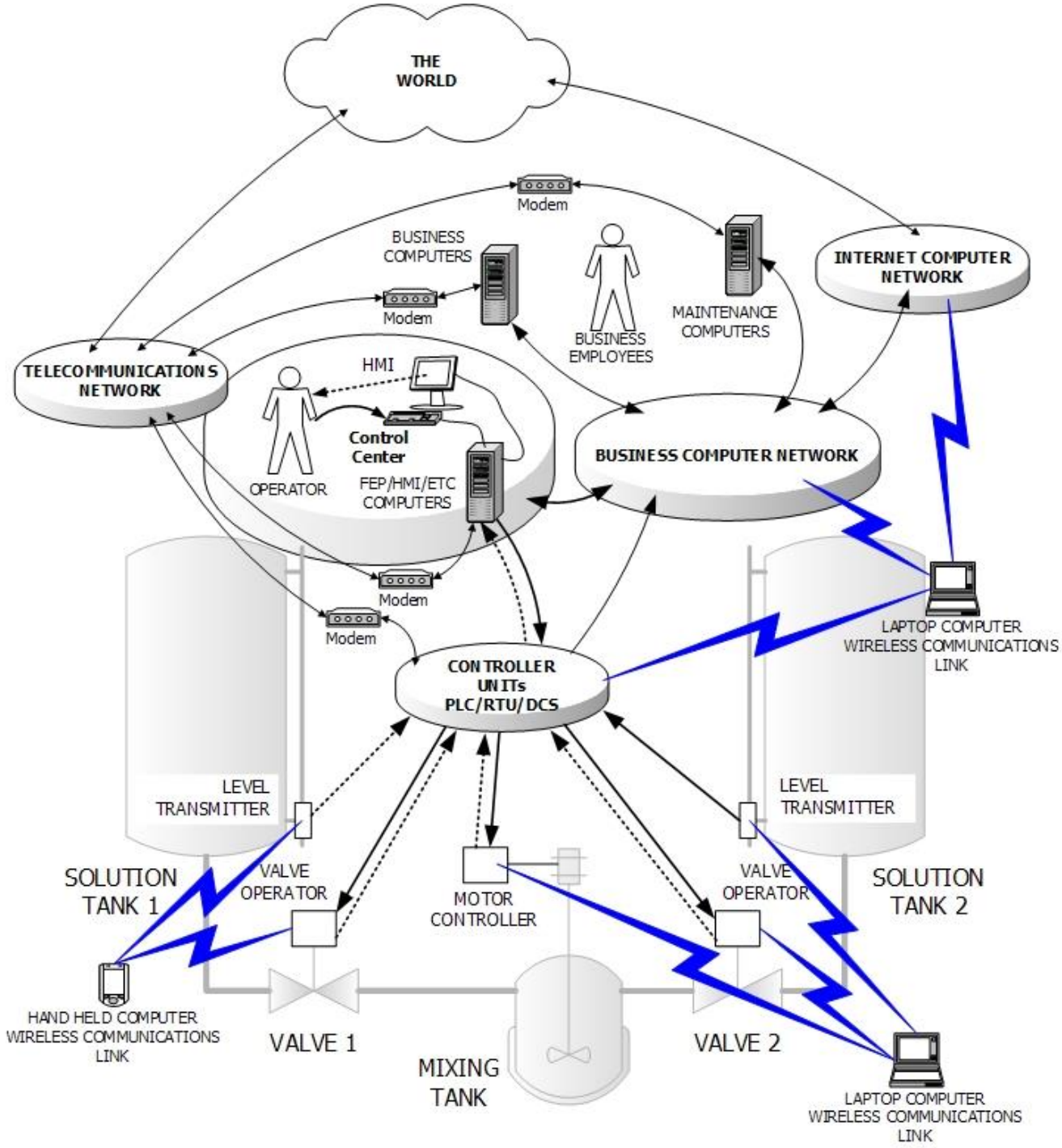
PLC Programmierung

Programmierung ist standardisiert nach ISO/IEC 61131-3:

- IL (Instruction List)
- ST (Structured Text)
- LD (Ladder Diagram)
- FBD (Function Block Diagram)
- SFC (Sequential Flow Chart)




PPS/CAD
CAP-
Systeme
Betriebsrechner
Backbone/Büro-Netzwerk
Datenbank
Fertigungsrechner
Industrie-ETHERNET-Netzwerk
Prozessleitrechner
Zellenrechner
Feldbus-Netzwerk
MPR
RC
SPS
NC
SPS
SPS
Planungs-ebene
Leitebene
Führungs-ebene
Steuerungs-ebene
Sensor/Aktor-ebene

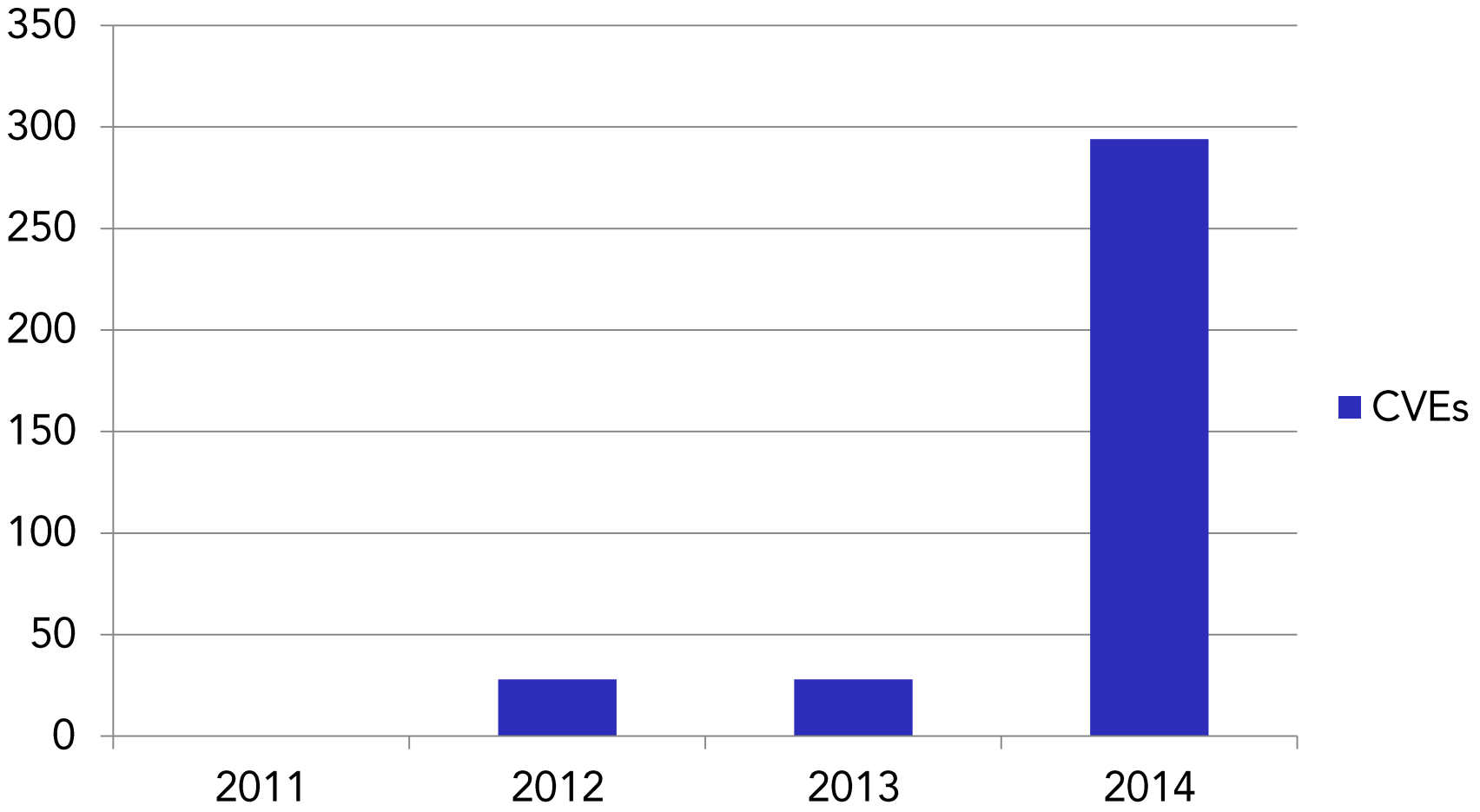

THE WORLD
Modem
BUSINESS COMPUTERS
Modem
BUSINESS EMPLOYEES
MAINTENANCE COMPUTERS
INTERNET COMPUTER NETWORK
TELECOMMUNICATIONS NETWORK
HMI
Control Center
OPERATOR
FEP/HMI/ETC COMPUTERS
BUSINESS COMPUTER NETWORK
Modem
Modem
LAPTOP COMPUTER WIRELESS COMMUNICATIONS LINK
CONTROLLER UNITs PLC/RTU/DCS
LEVEL TRANSMITTER
LEVEL TRANSMITTER
SOLUTION TANK 1
VALVE OPERATOR
MOTOR CONTROLLER
VALVE OPERATOR
SOLUTION TANK 2
HAND HELD COMPUTER WIRELESS COMMUNICATIONS LINK
VALVE 1
MIXING TANK
VALVE 2
LAPTOP COMPUTER WIRELESS COMMUNICATIONS LINK

Herausforderungen

- Zunehmende Vernetzung
- Standardisierung der Industrieprotokolle
- Protokolle sind unzureichend gesichert
- Patching kaum vorhanden
- Lange Lebenszeit der Systeme

CVE Entwicklung

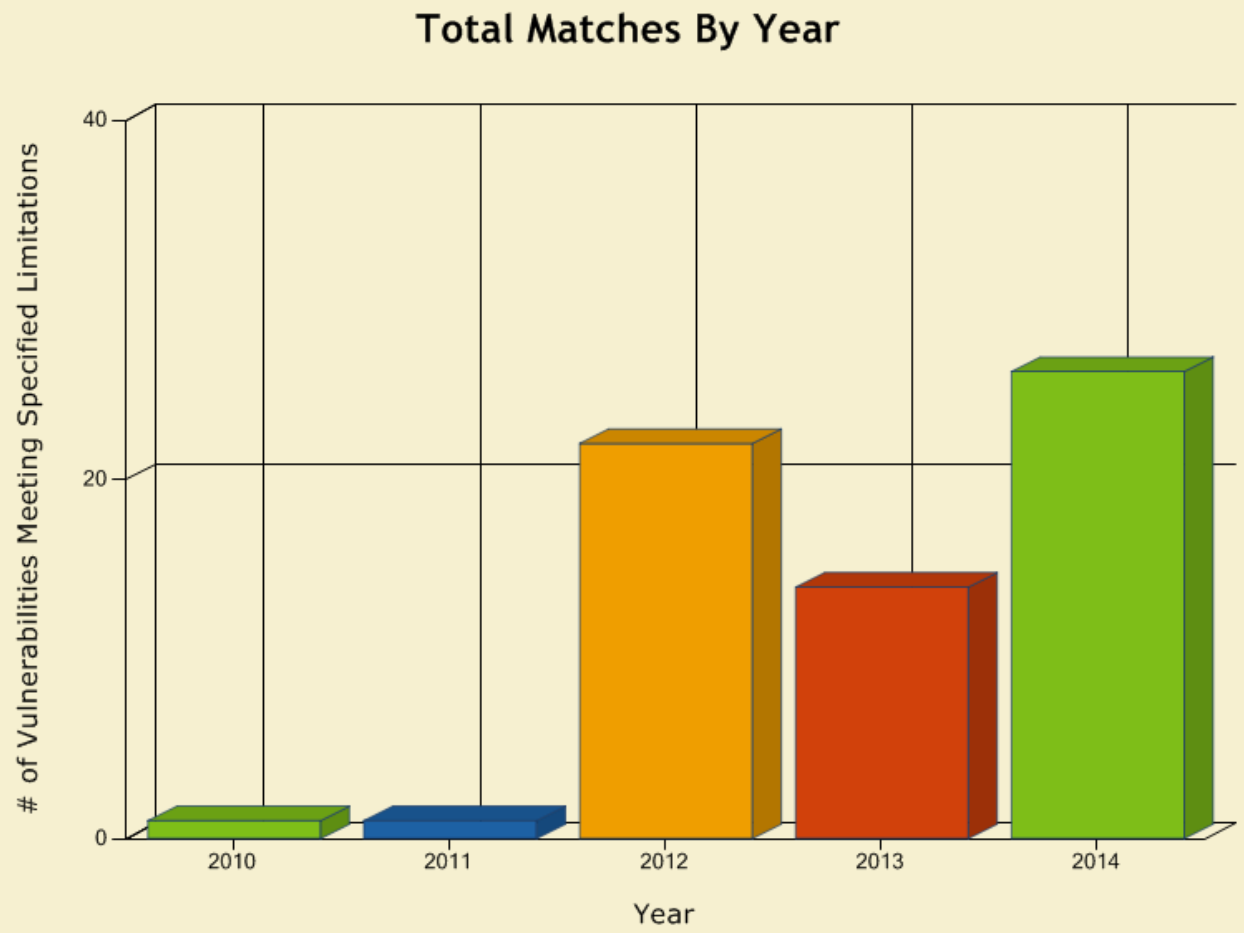
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

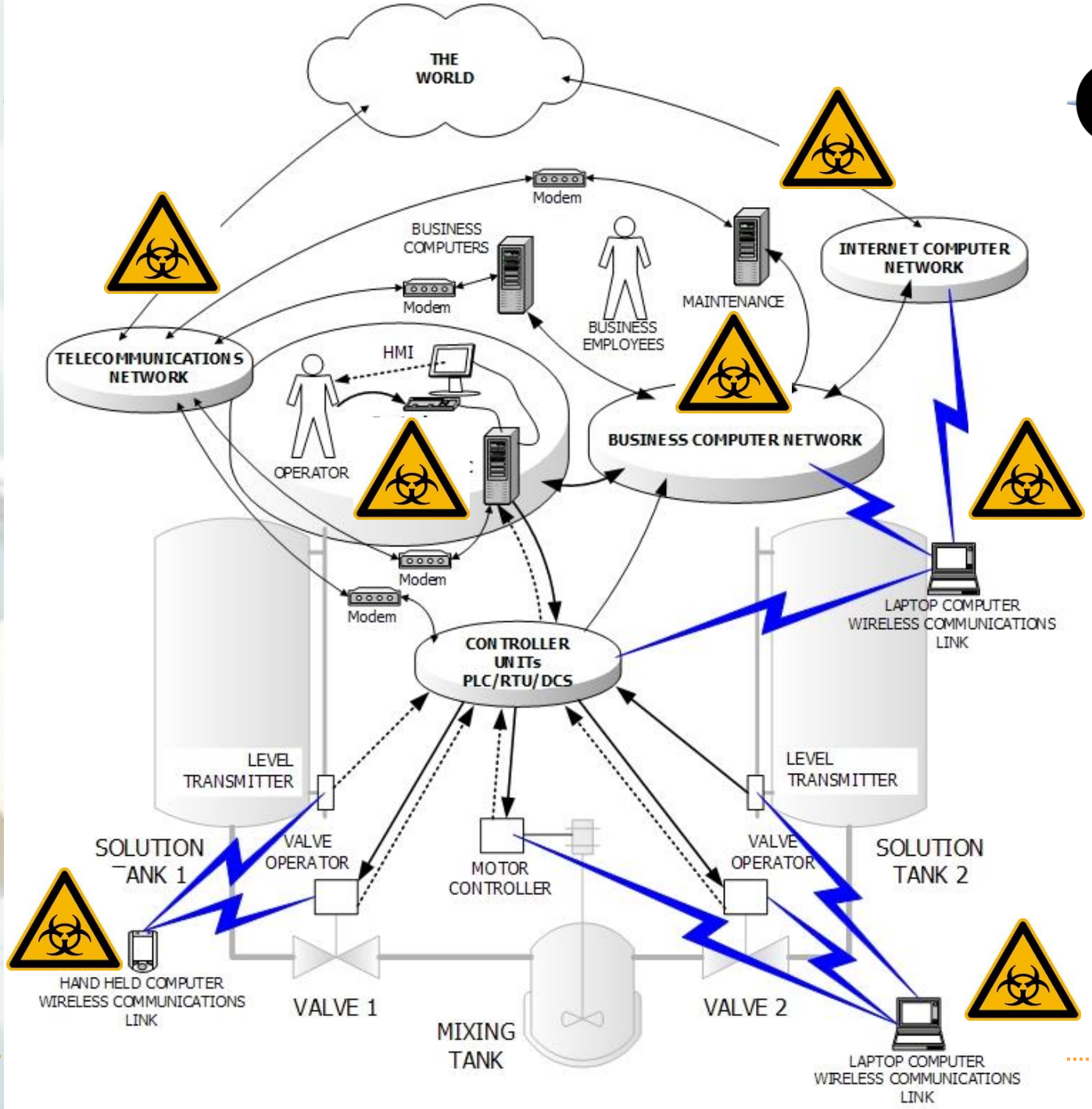


CVE Entwicklung

Search Parameters:

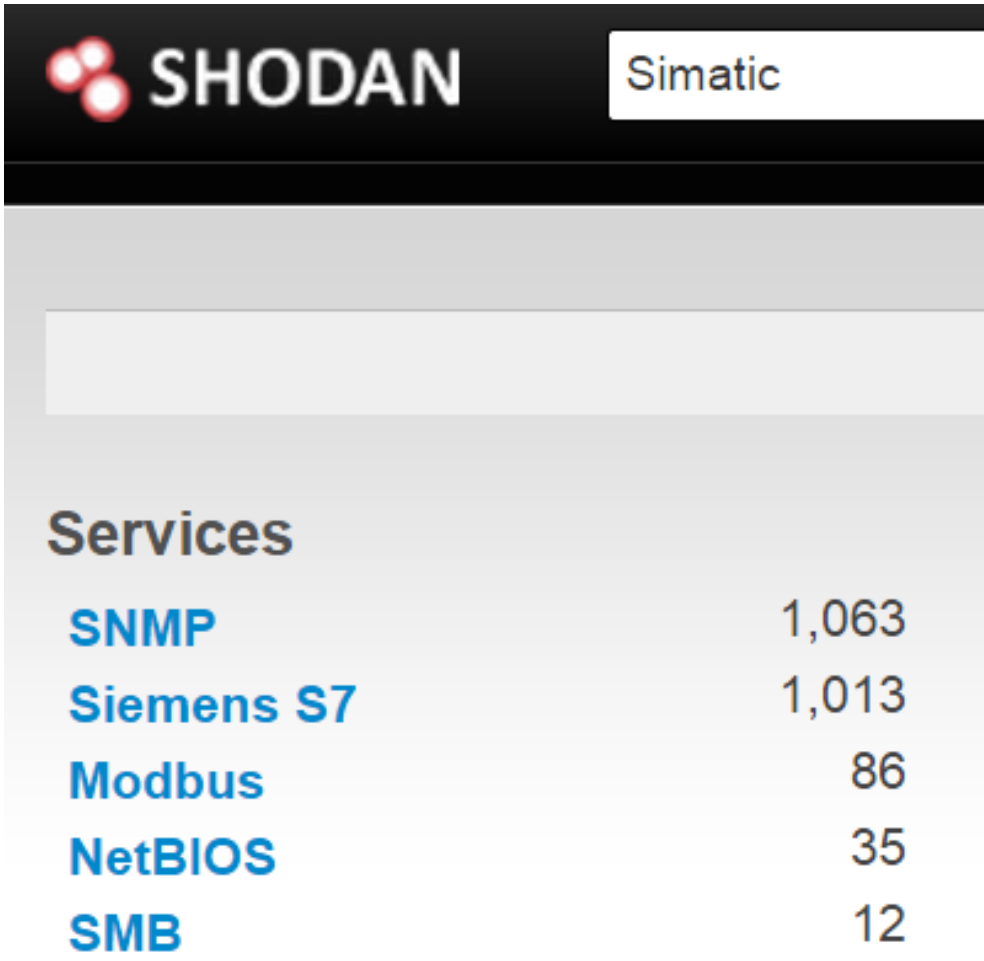
- **Contains Software Flaws (CVE)**
- **Keyword (text search):** Simatic




THE WORLD
Modem
BUSINESS COMPUTERS
Modem
BUSINESS EMPLOYEES
MAINTENANCE
INTERNET COMPUTER NETWORK
TELECOMMUNICATIONS NETWORK
HMI
OPERATOR
BUSINESS COMPUTER NETWORK
Modem
Modem
LAPTOP COMPUTER WIRELESS COMMUNICATIONS LINK
CONTROLLER UNITs PLC/RTU/DCS
LEVEL TRANSMITTER
LEVEL TRANSMITTER
SOLUTION TANK 1
VALVE OPERATOR
MOTOR CONTROLLER
VALVE OPERATOR
SOLUTION TANK 2
HAND HELD COMPUTER WIRELESS COMMUNICATIONS LINK
VALVE 1
MIXING TANK
VALVE 2
LAPTOP COMPUTER WIRELESS COMMUNICATIONS LINK

1. Information Gathering

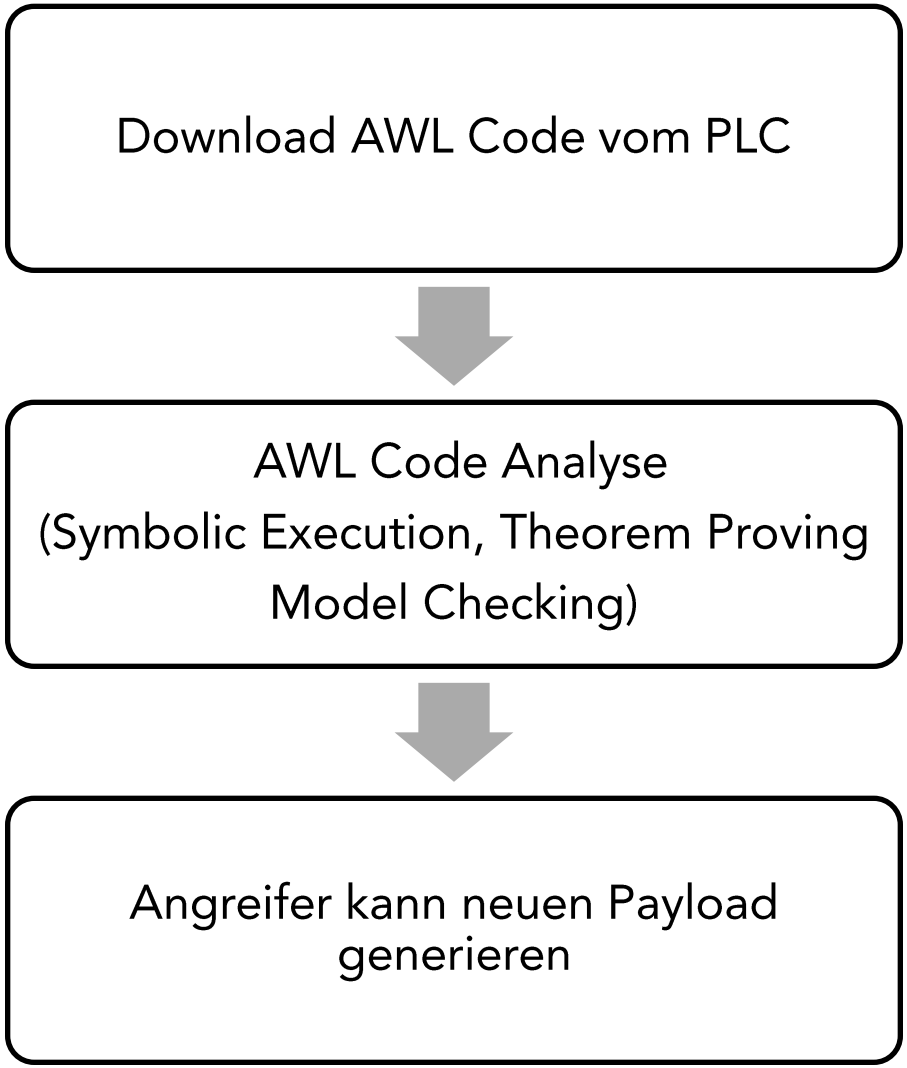
- Shodan
- plcscan
- ZMap



2. Compass Security ICS Tool

- Stop Flooding
- Replay Attacken
- Code Upload
- Analyse von PLC Code

Analyse von PLC Code



Security Guidelines

- Keine unnötige Exponierung von ICS Geräten ins Internet
- Einführung einer ICS Sicherheitszone
- Fernwartung ausschliesslich über VPN
- Security Audits von internen und externen Komponenten
- Risikomanagement und Self-Assessment
- Schulung von Mitarbeitern

Security Guidelines

- NIST (Guide to Industrial Control Systems Security)
- BSI (ICS-Security-Kompendium)
- US Energy Department (21 Steps to Improve Cyber Security of SCADA Networks)

Forschung

Programmverifikation

- SABOT [2012]
- PLC Code Vulnerabilities Through SCADA Systems [2013]
- A Trusted Safety Verifier [2014]

Anomaly-Detection

- Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol [2012]
- Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems [2013]

Checkliste

1. Sind Komponenten meines ICS auf Shodan gelistet?
2. Welche Komponenten setze ich ein und wann wurden sie gepatcht?
3. Sind meine Systeme von einer Vulnerabilität betroffen?
4. Welche Verbindungen zum SCADA Netzwerk werden aufgebaut?
5. Sind diese Komponenten gehärtet?
6. Sind sich die Mitarbeiter über die Gefahren und Auswirkungen eines Angriffs bewusst?