Vorstellung der Masterarbeit: IT-Sicherheit von Industriellen Kontrollsystemen

Gregor Bonney

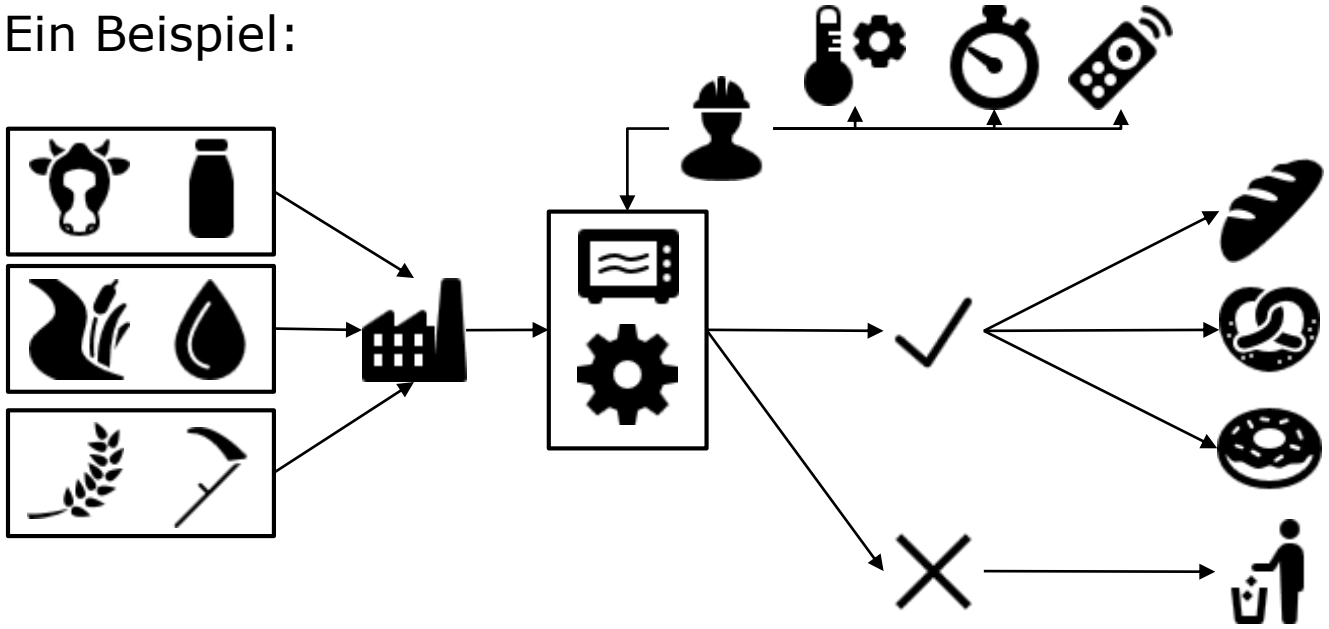
Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

Agenda

- Einführung
  - Industrielle Kontrollsysteme (ICS)
- Masterarbeit
  - Untersuchung eines Inline Controllers
  - Untersuchung des Steuerungsprotokolls

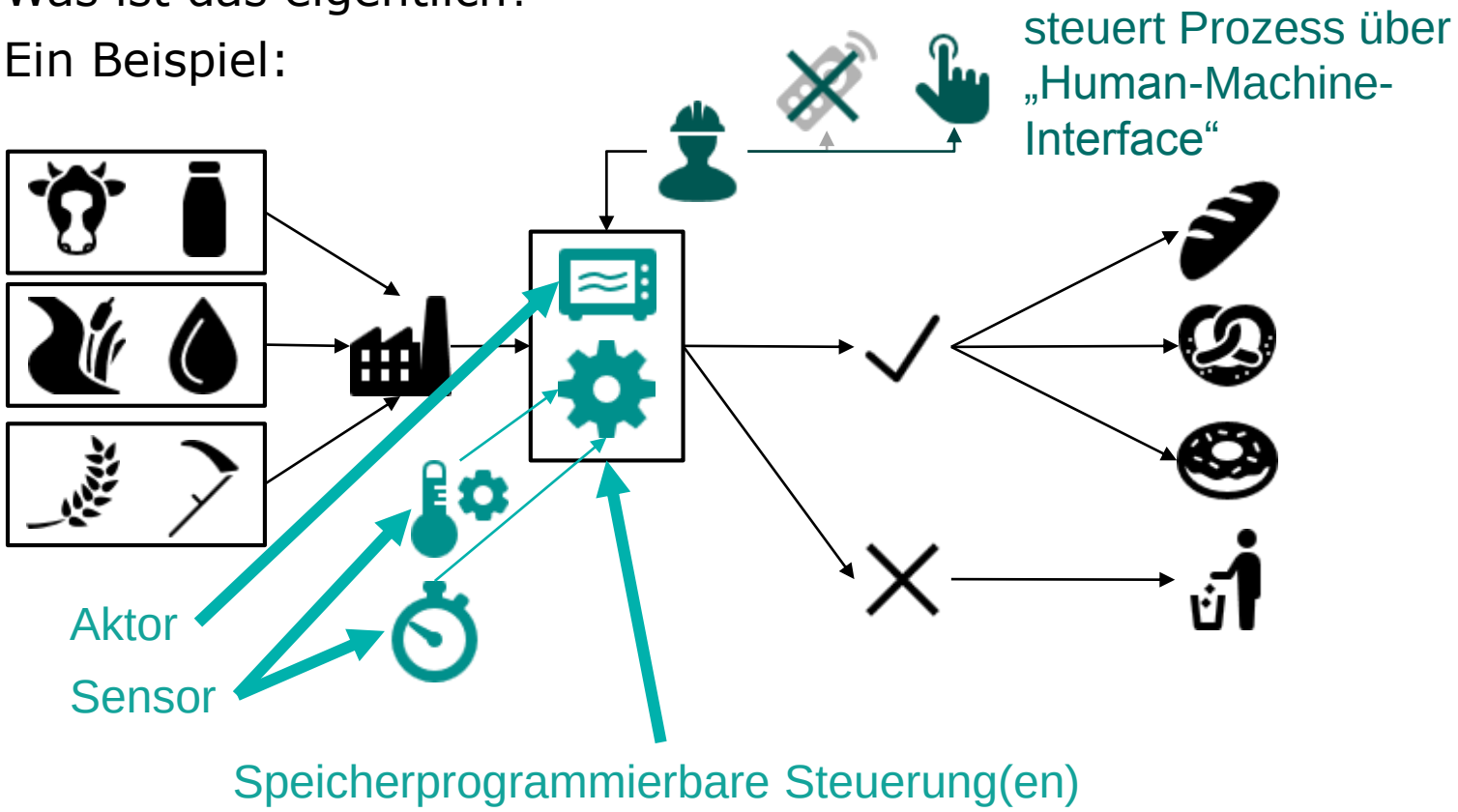
Einführung

- **Industrielle Kontrollsysteme (ICS)**
  - Was ist das eigentlich?
  - Ein Beispiel:



Einführung

- **Industrielle Kontrollsysteme (ICS)**
  - Was ist das eigentlich?
  - Ein Beispiel:



Masterarbeit

- IT-Sicherheit von Industriellen Kontrollsystemen
  - Untersuchung einer *Speicherprogrammierbaren Steuerung* eines Herstellers hinsichtlich der IT-Sicherheit.
    - Konfiguration im Werkszustand
    - Bereitgestellte Dienste
    - Firmware Analyse
  - Untersuchung des *Kommunikationsprotokolls.*
    - Analyse der übertragenen Pakete
    - Erstellung eines Paket-Parsers
    - Fuzzing von unbekannten Bytes

Masterarbeit

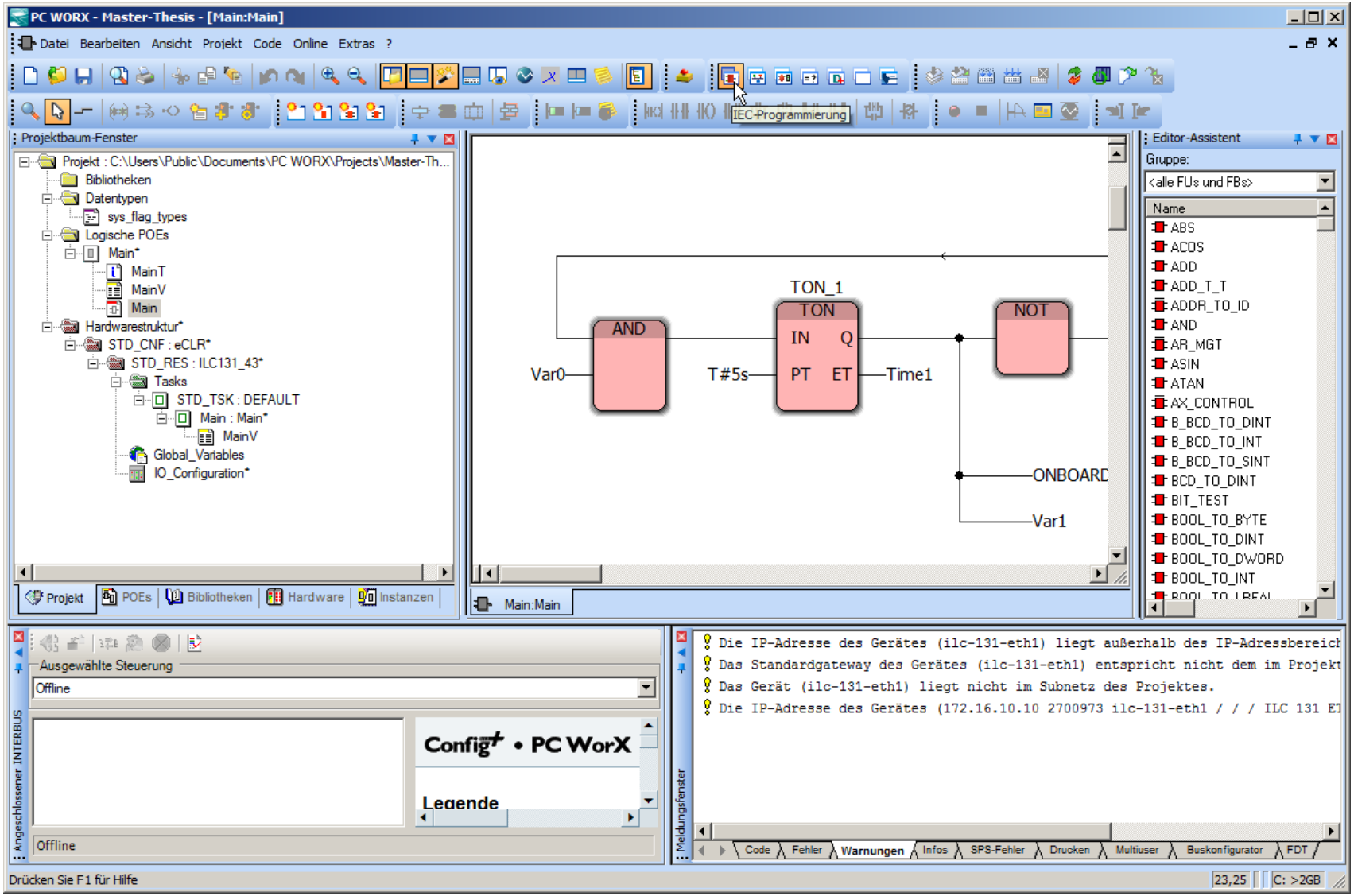
- Phoenix Contact
- Inline Controller 131

Artikeleigenschaften

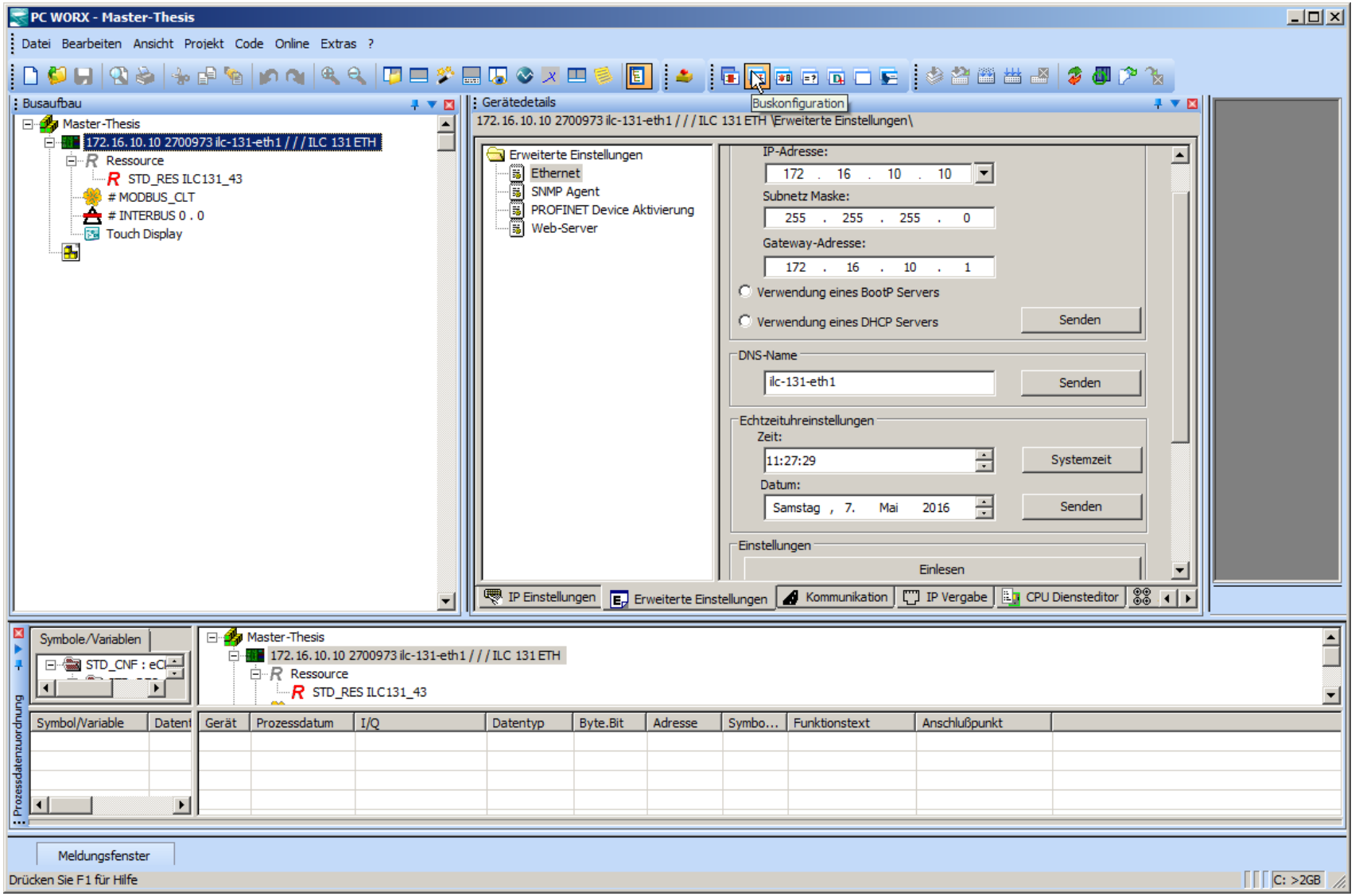
- PROFINET-Device
- Modbus/TCP-Client
- Unterstützung zahlreicher Protokolle wie: http, https, FTP, SNTP, SNMP, SMTP, SQL, MySQL, DCP uvm.
- Kostenfreies Engineering mit PC Worx Express (IEC 61131-3)
- Programm- und Datenspeicher (192kByte/192kByte)
- Modbus/TCP-Server-Server
- HTML 5
- Integrierter Web-Server zur Visualisierung mit WebVisit/atvise®
- Vollwertiger INTERBUS-Master (2048 I/O-Punkte)
- SD-Karte bis 2 GB als optional steckbaren Parametrierungsspeicher

Quelle: https://www.phoenixcontact.com/assets/images_pr/product_photos/large/52115_1000_int_04.jpg

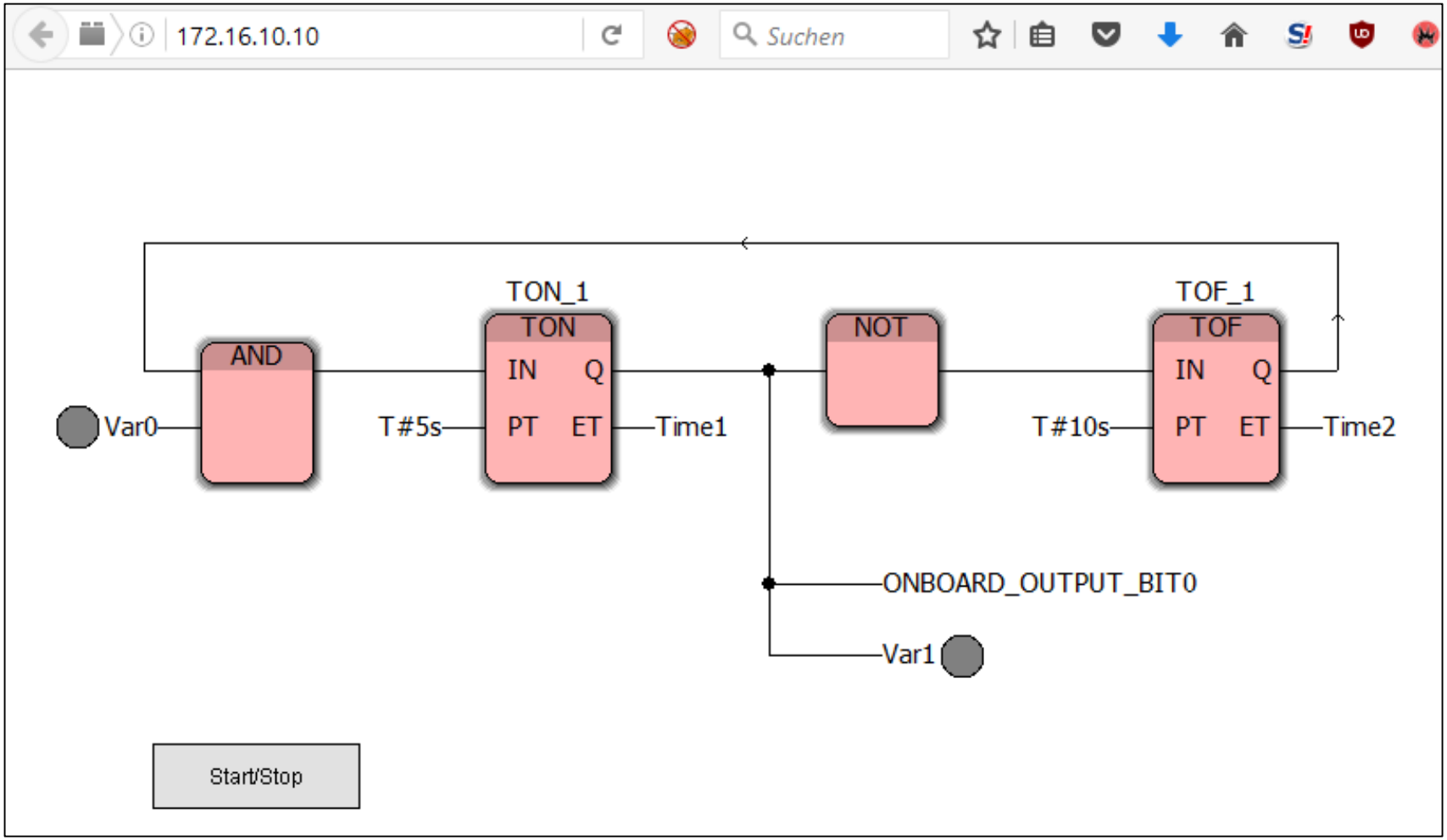
Masterarbeit



Masterarbeit



Masterarbeit

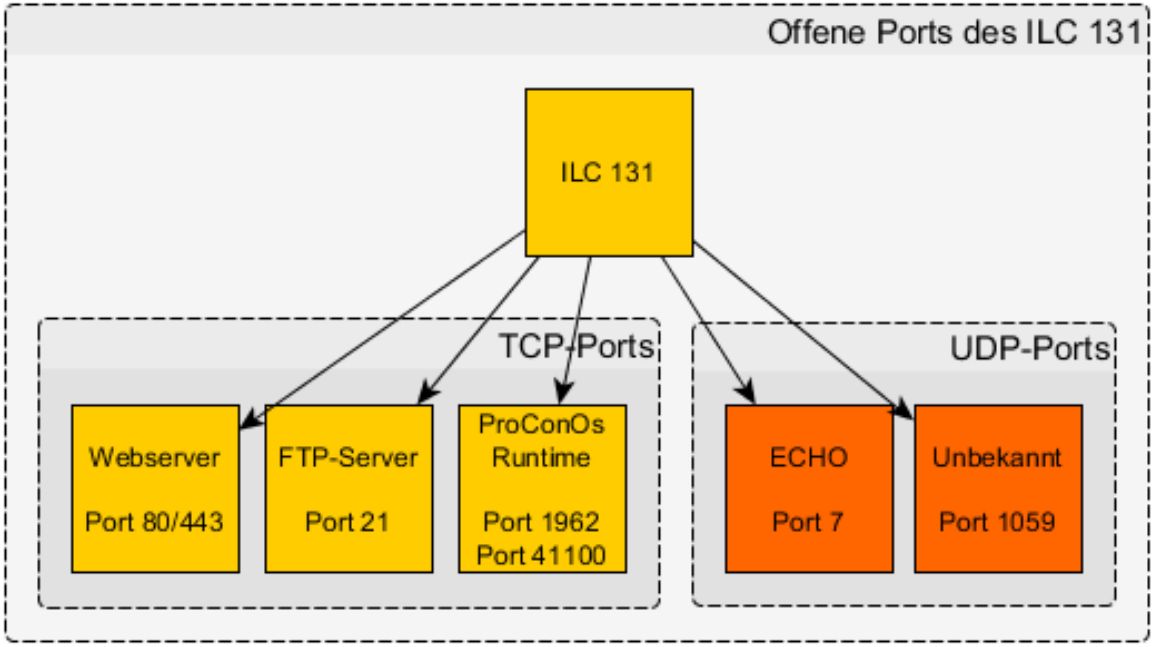


Masterarbeit

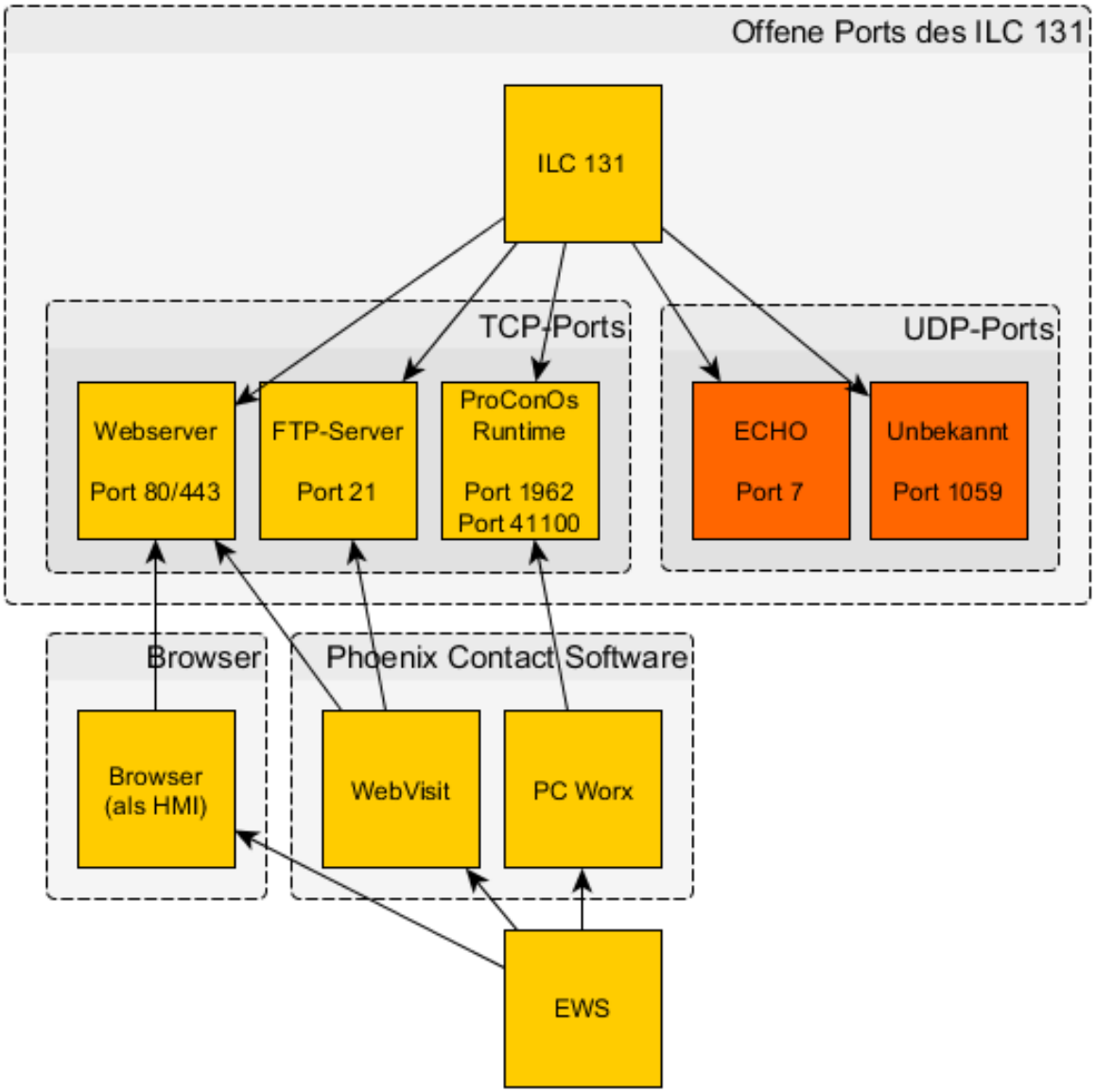
- Vorbereitende Tätigkeiten
  - Konfigurieren des ILC 131
  - Steuerungsprogramm entwickelt + übertragen
  - Visualisierung des Programms übertragen

- Durchführung
  - Portscan
  - Mitschneiden des Datenverkehrs
  - …

Masterarbeit



Masterarbeit

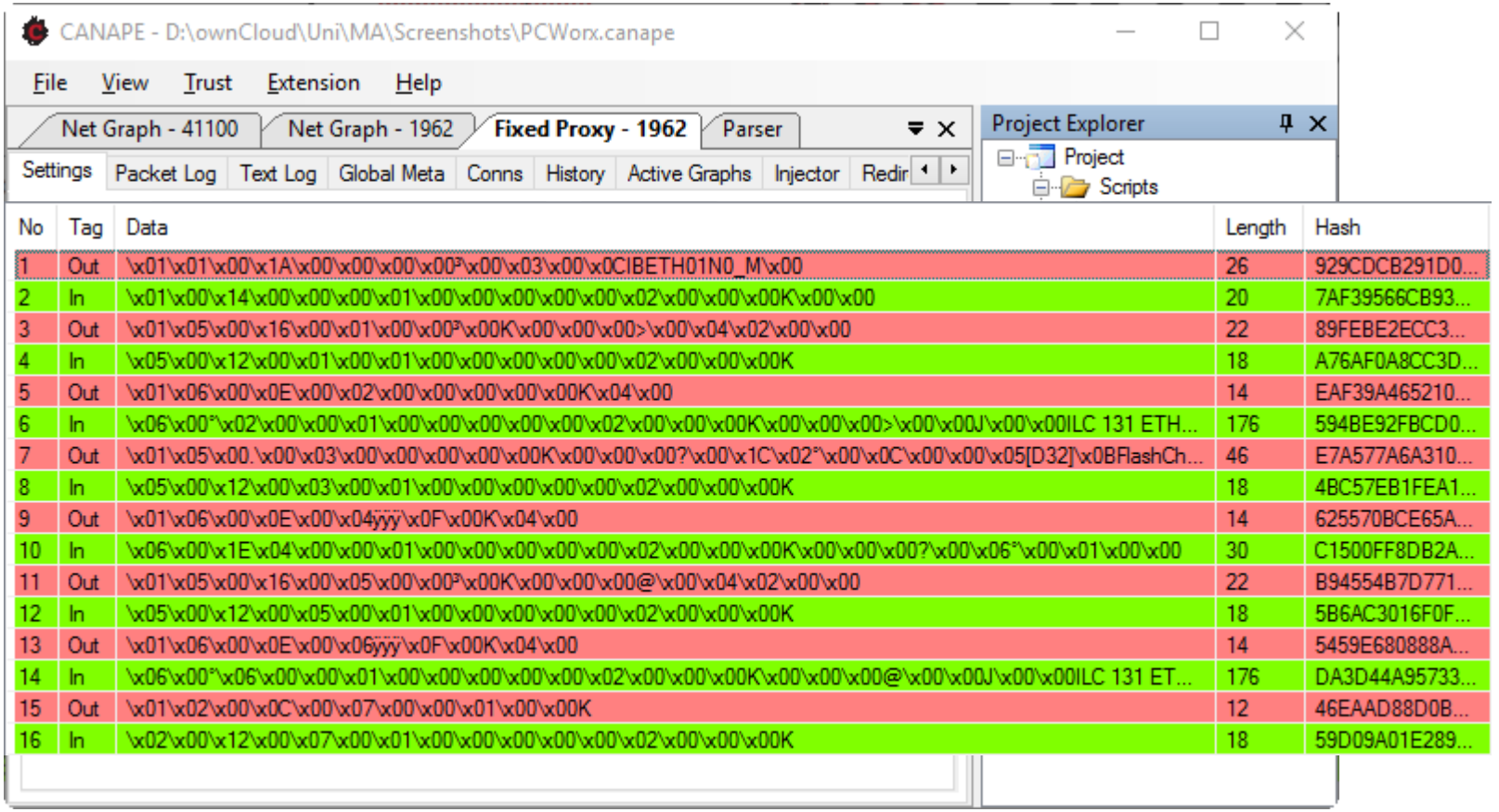


Masterarbeit

- Binär-Proxy: Canape

Canape

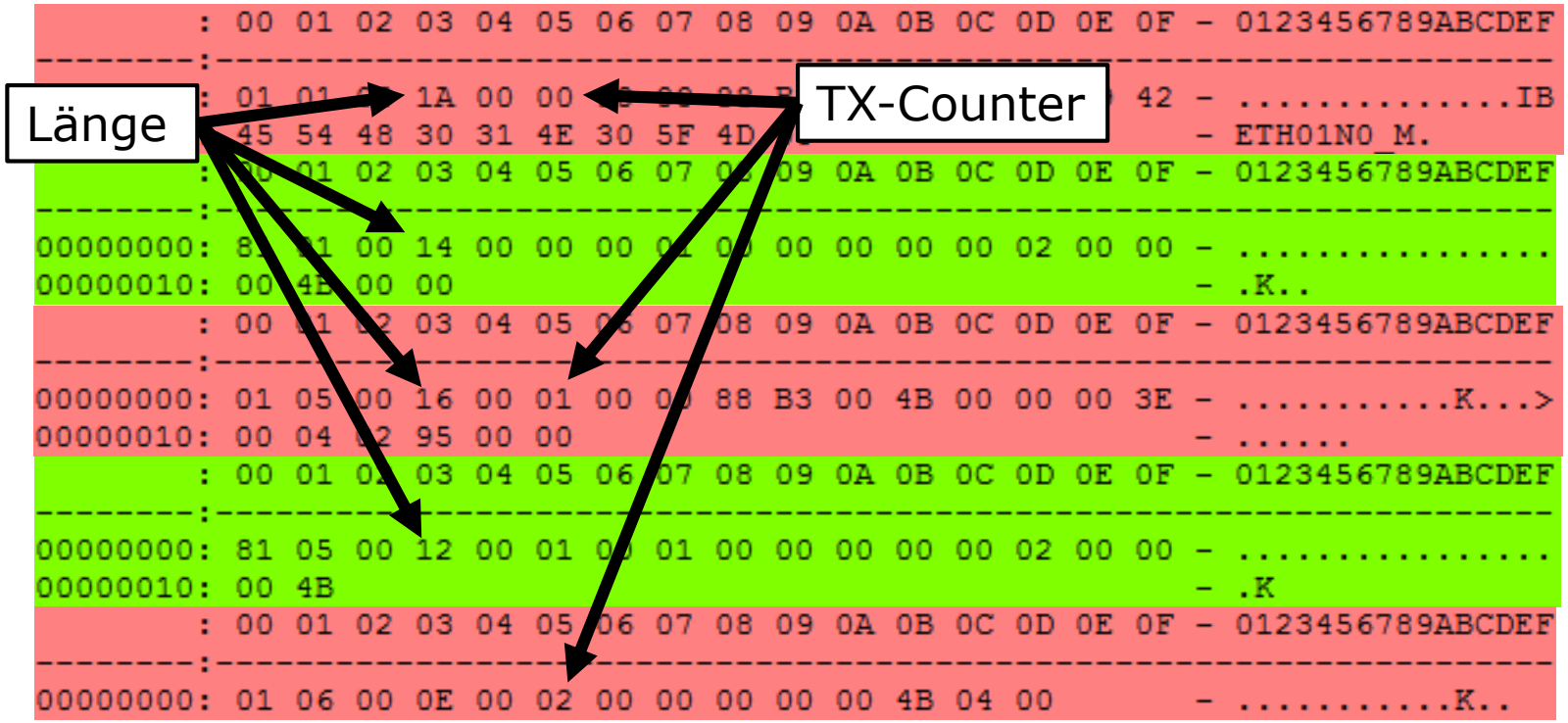
01100011011000001011011100110000010111 00000110010 1



No	Tag	Data	Length	Hash
1	Out	\x01\x01\x00\x1A\x00\x00\x00\x00³\x00\x03\x00\x0CIBETH01N0_M\x00	26	929CDCB291D0...
2	In	\x01\x00\x14\x00\x00\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K\x00\x00	20	7AF39566CB93...
3	Out	\x01\x05\x00\x16\x00\x01\x00\x00³\x00K\x00\x00\x00>\x00\x04\x02\x00\x00	22	89FEBE2ECC3...
4	In	\x05\x00\x12\x00\x01\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K	18	A76AF0A8CC3D...
5	Out	\x01\x06\x00\x0E\x00\x02\x00\x00\x00\x00\x00K\x04\x00	14	EAF39A465210...
6	In	\x06\x00"\x02\x00\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K\x00\x00\x00>\x00\x00J\x00\x00ILC 131 ETH...	176	594BE92FBCD0...
7	Out	\x01\x05\x00.\x00\x03\x00\x00\x00\x00\x00K\x00\x00\x00?\x00\x1C\x02"\x00\x0C\x00\x00\x05[D32]\x0BFlashCh...	46	E7A577A6A310...
8	In	\x05\x00\x12\x00\x03\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K	18	4BC57EB1FEA1...
9	Out	\x01\x06\x00\x0E\x00\x04ÿÿÿ\x0F\x00K\x04\x00	14	625570BCE65A...
10	In	\x06\x00\x1E\x04\x00\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K\x00\x00\x00?\x00\x06"\x00\x01\x00\x00	30	C1500FF8DB2A...
11	Out	\x01\x05\x00\x16\x00\x05\x00\x00³\x00K\x00\x00\x00@\x00\x04\x02\x00\x00	22	B94554B7D771...
12	In	\x05\x00\x12\x00\x05\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K	18	5B6AC3016F0F...
13	Out	\x01\x06\x00\x0E\x00\x06ÿÿÿ\x0F\x00K\x04\x00	14	5459E680888A...
14	In	\x06\x00"\x06\x00\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K\x00\x00\x00@\x00\x00J\x00\x00ILC 131 ET...	176	DA3D44A95733...
15	Out	\x01\x02\x00\x0C\x00\x07\x00\x00\x01\x00\x00K	12	46EAAD88D0B...
16	In	\x02\x00\x12\x00\x07\x00\x01\x00\x00\x00\x00\x00\x02\x00\x00\x00K	18	59D09A01E289...

Masterarbeit

- Paket-Detailansicht

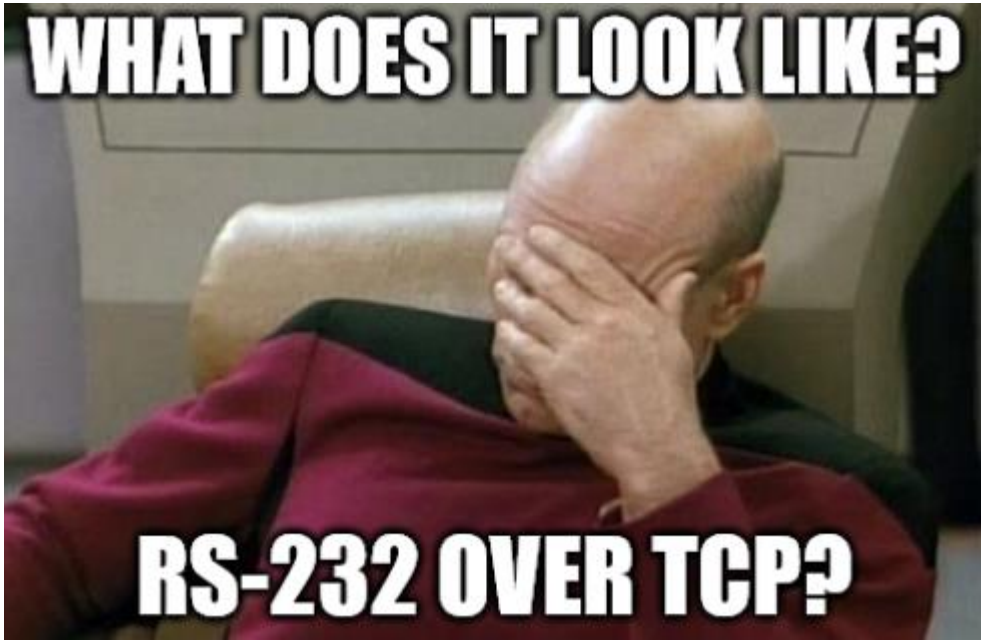


Masterarbeit

Wie bitte?

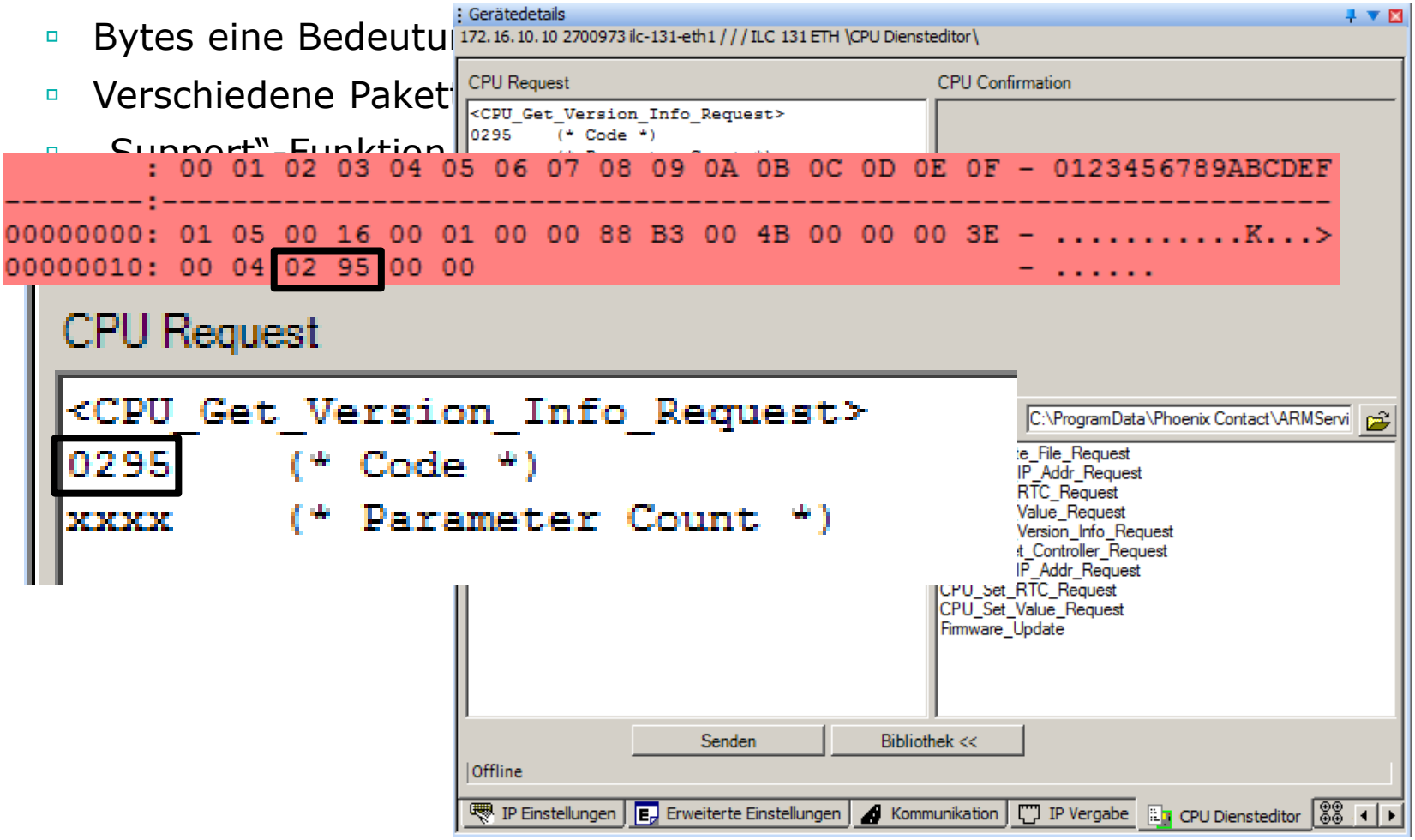
- *Länge* und *TX-Counter* im TCP-*Daten*segment?
- TCP-Header enthält doch schon die Länge!
- TCP macht doch die Flusskontrolle!

- RS-232 over TCP?



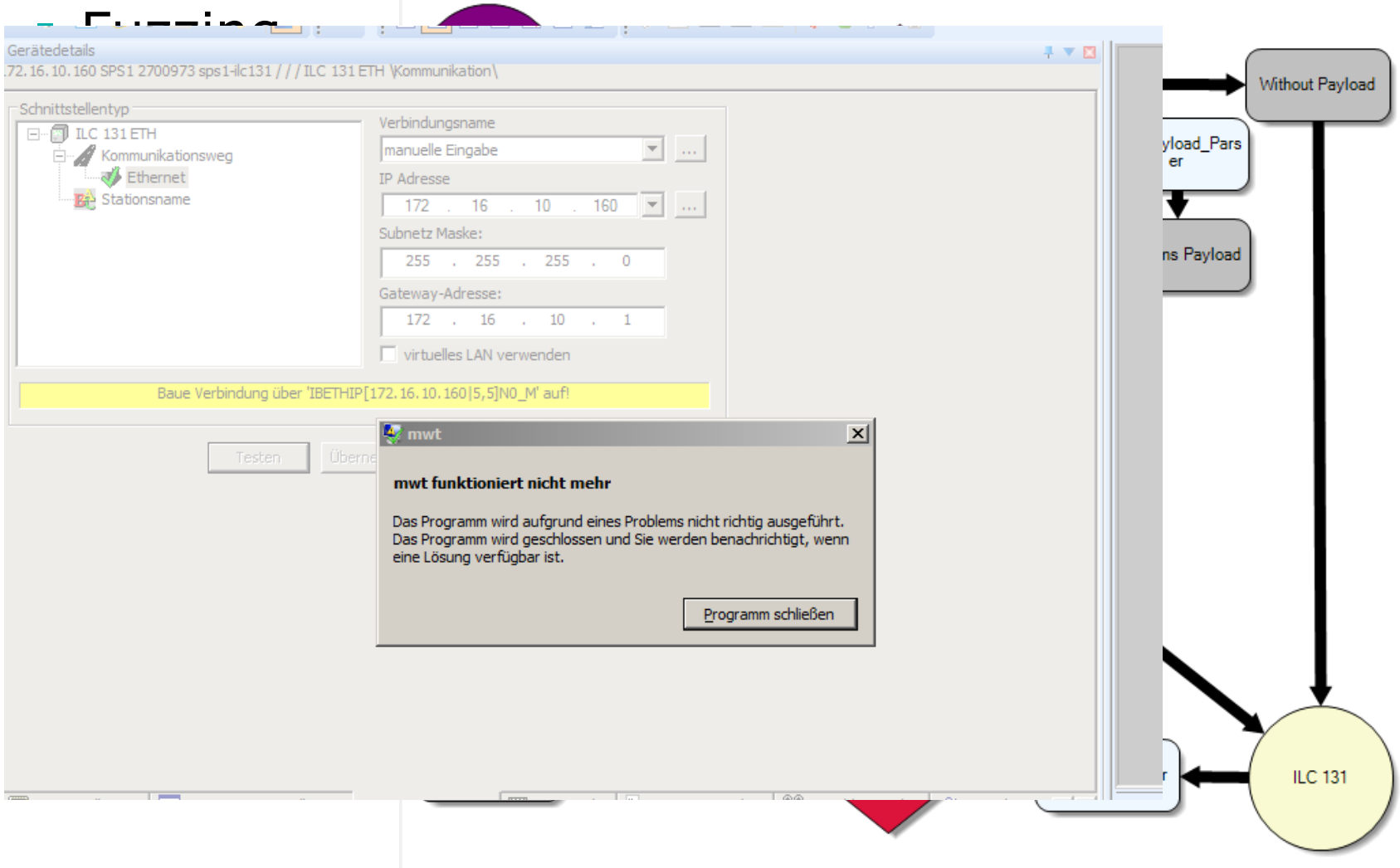
Masterarbeit

- Entwicklung von Paket-Parser
  - Bytes eine Bedeutu
  - Verschiedene Paket
  - „Support“-Funktion



Masterarbeit

- Fuzzing



Master-Thesis

- Der Stand bisher
  - Masterarbeit läuft noch
  - mehrere Schwachstellen gefunden
  - darunter: „Denial of Service“ identifiziert
  - Responsible Disclosure

Vielen Dank für Ihre Aufmerksamkeit

Gibt es Fragen?

Kontaktmöglichkeit:
gregor.bonney@alumni.fh-aachen.de

Einführung

- **Industrielle Kontrollsysteme (ICS)**
  - Was ist das eigentlich?
  - Ein weiteres Beispiel: