

Vorstellung der Masterarbeit: IT-Sicherheit von Industriellen Kontrollsystemen

Gregor Bonney

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik

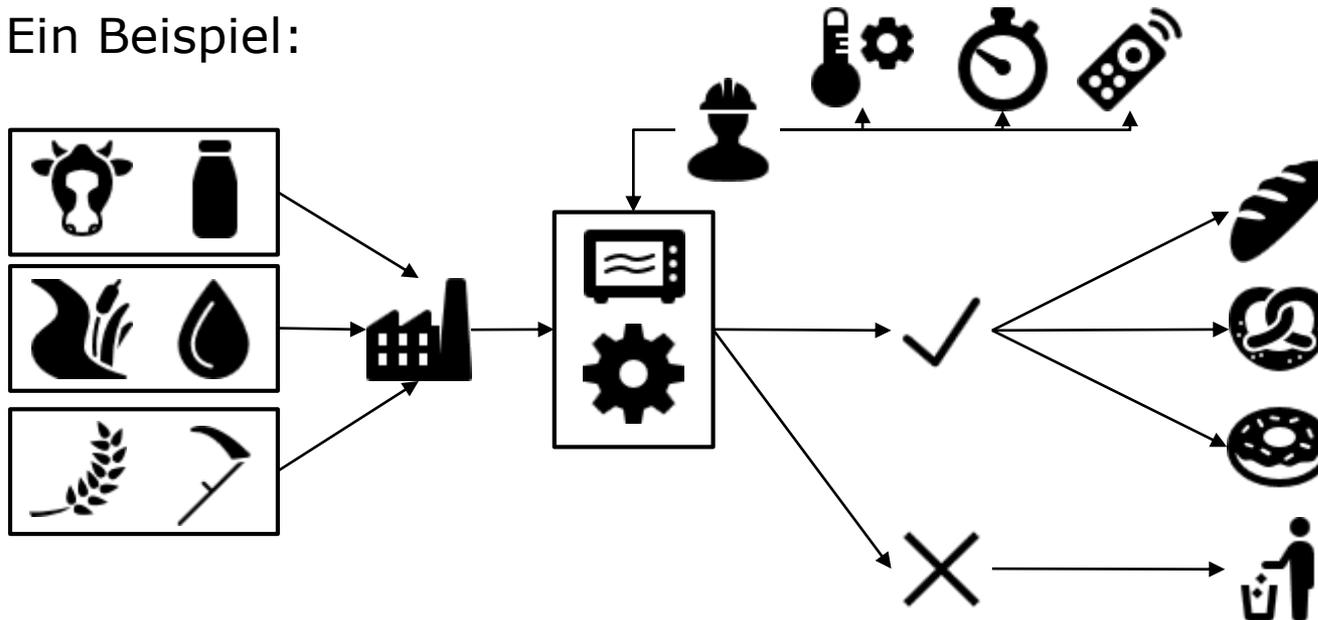


- Einführung
 - Industrielle Kontrollsysteme (ICS)

- Masterarbeit
 - Untersuchung eines Inline Controllers
 - Untersuchung des Steuerungsprotokolls

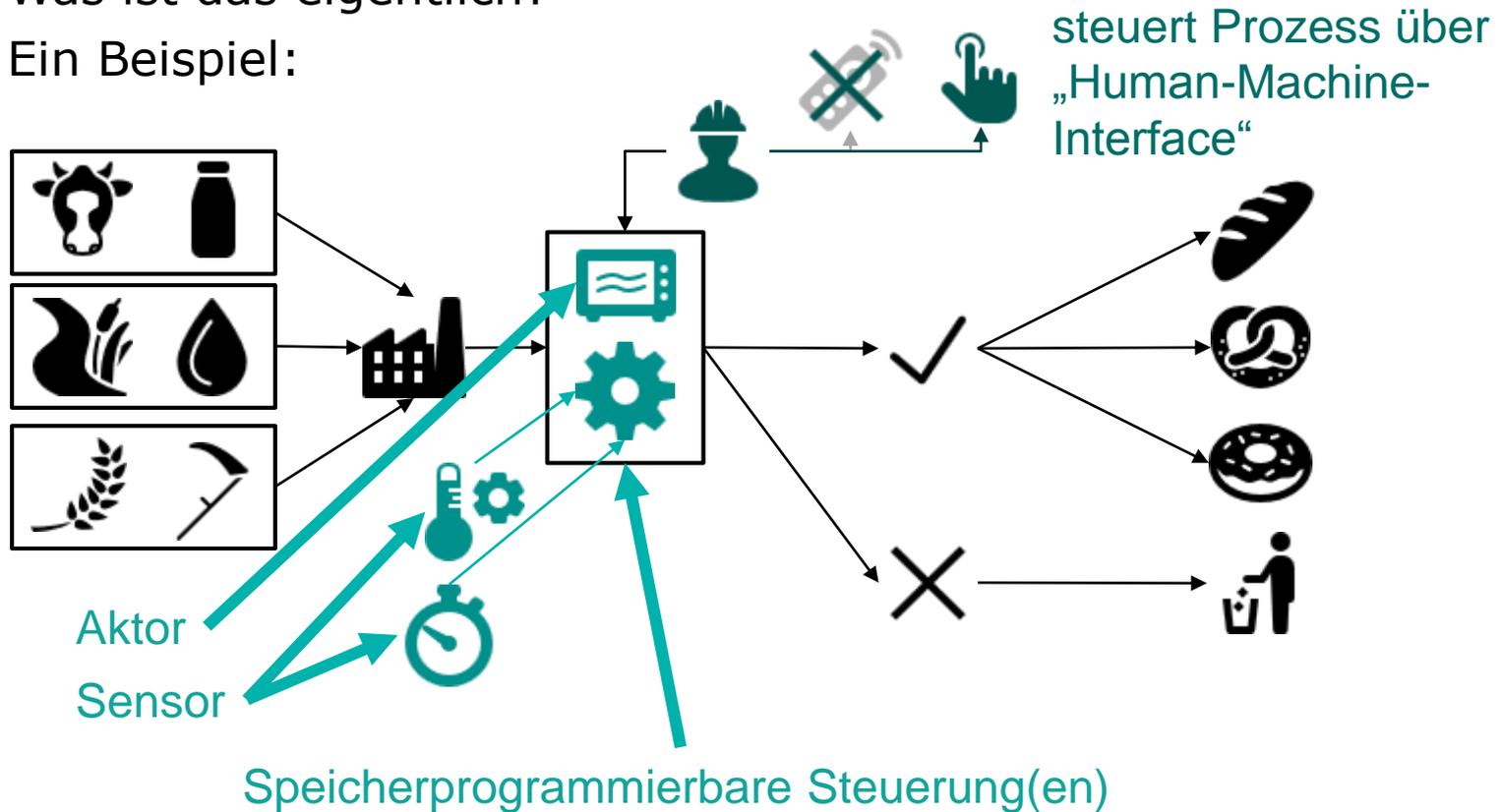
■ Industrielle Kontrollsysteme (ICS)

- Was ist das eigentlich?
- Ein Beispiel:



■ Industrielle Kontrollsysteme (ICS)

- Was ist das eigentlich?
- Ein Beispiel:



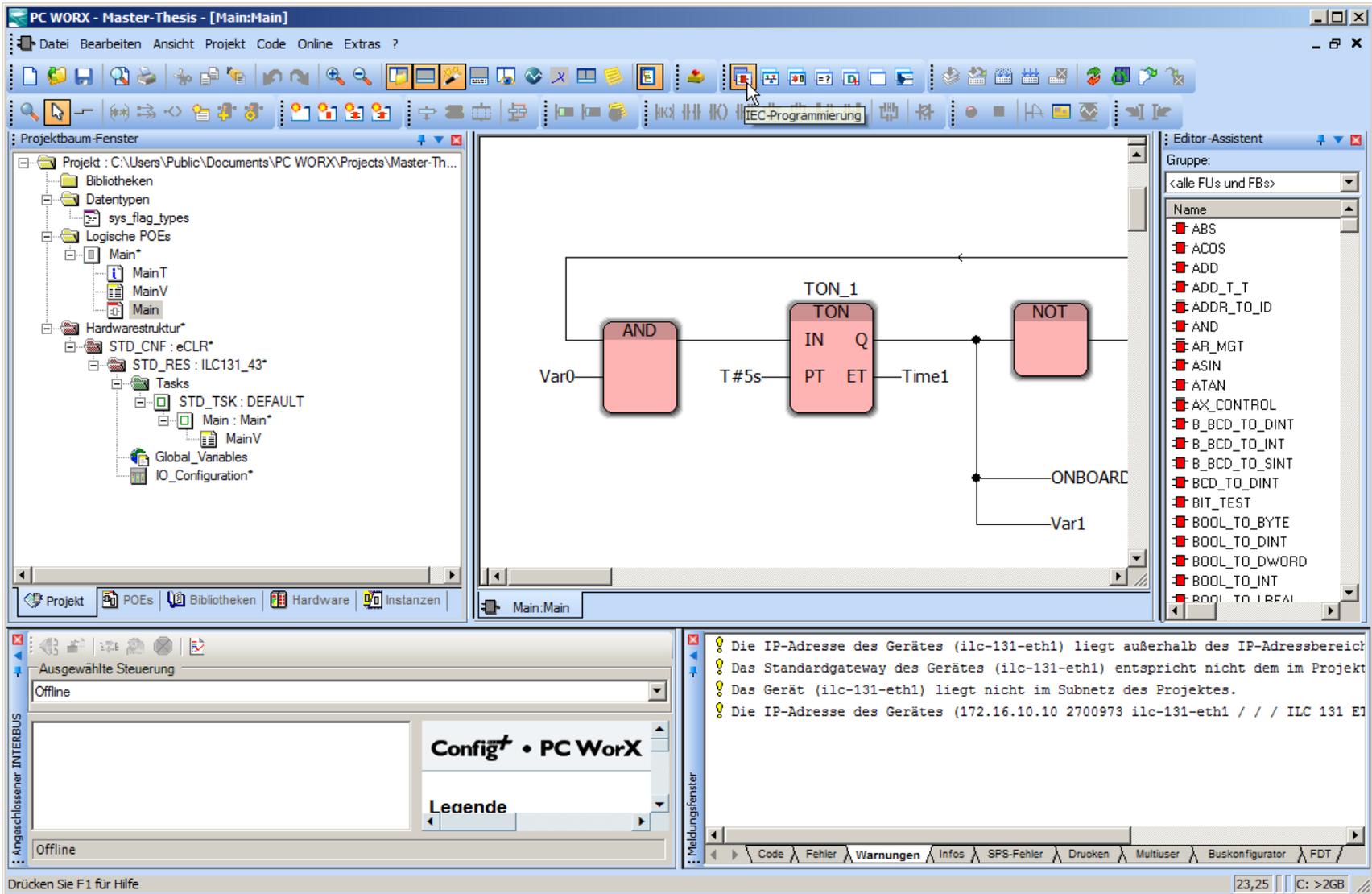
- IT-Sicherheit von Industriellen Kontrollsystemen
 - Untersuchung einer *Speicherprogrammierbaren Steuerung* eines Herstellers hinsichtlich der IT-Sicherheit.
 - Konfiguration im Werkszustand
 - Bereitgestellte Dienste
 - Firmware Analyse
 - Untersuchung des *Kommunikationsprotokolls*.
 - Analyse der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

- Phoenix Contact
- Inline Controller 131

Artikeleigenschaften

- PROFINET-Device
- Modbus/TCP-Client
- Unterstützung zahlreicher Protokolle wie: http, https, FTP, 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



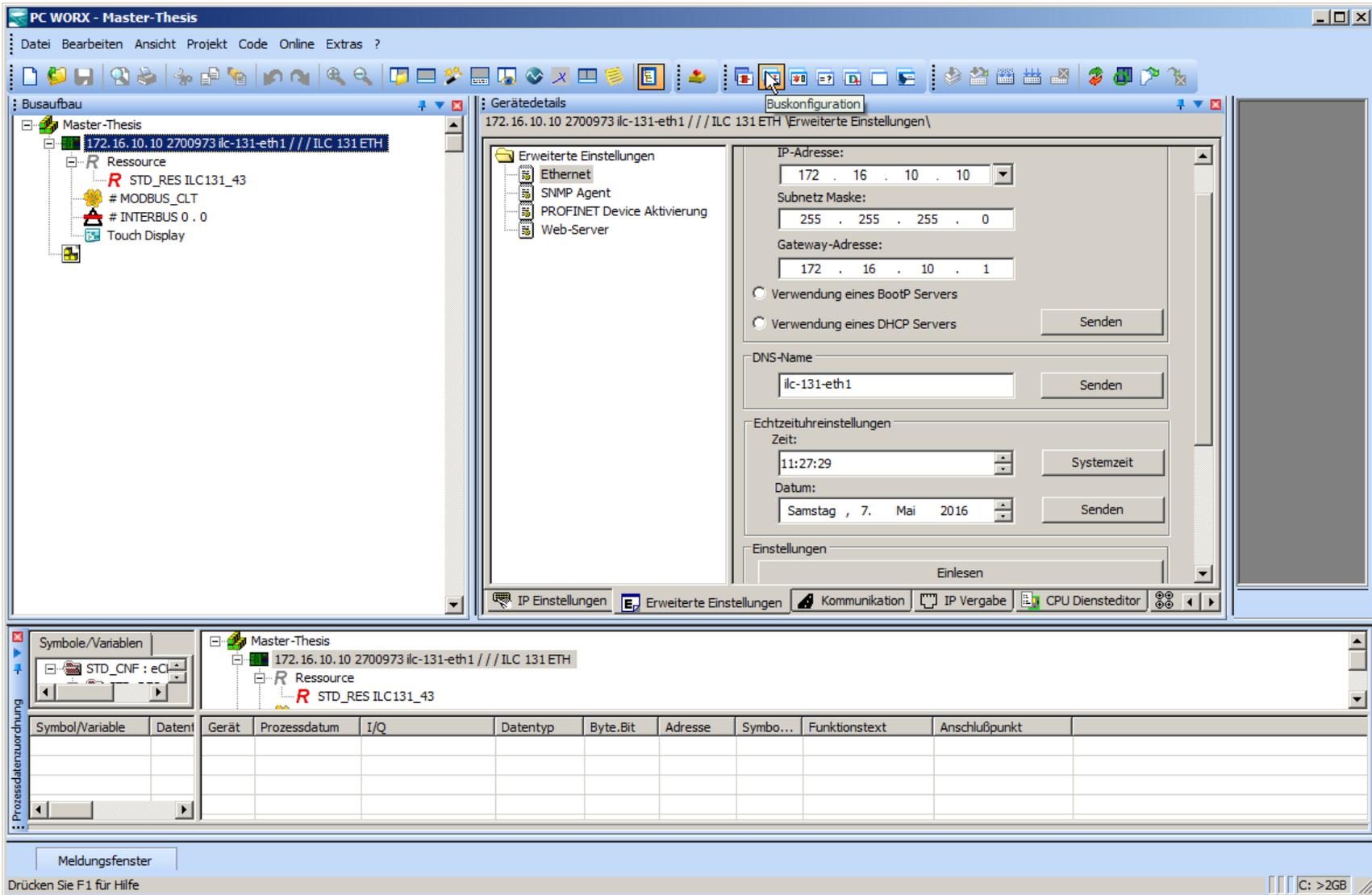
The screenshot displays the PC WORX software interface for IEC programming. The main window shows a ladder logic diagram with the following components:

- AND** (pink box) connected to **Var0**.
- TON_1** (pink box) with inputs **IN** and **PT**, and outputs **Q** and **ET**. It is set to **T#5s**.
- NOT** (pink box) connected to the output of the AND block.
- ONBOARD** and **Var1** are connected to the output of the NOT block.

The interface includes several panels:

- Projektbaum-Fenster** (Project Tree): Shows the project structure, including libraries, data types, logical POEs, and hardware configuration.
- Editor-Assistent** (Editor Assistant): A list of available functions and blocks, such as ABS, ACOS, ADD, AND, AR_MGT, ASIN, ATAN, AX_CONTROL, B_BCD_TO_DINT, B_BCD_TO_INT, B_BCD_TO_SINT, BCD_TO_DINT, BIT_TEST, BOOL_TO_BYTE, BOOL_TO_DINT, BOOL_TO_DWORD, BOOL_TO_INT, and BOOL_TO_REAL.
- Ausgewählte Steuerung** (Selected Control): Shows the current control state as "Offline".
- Meldungsfenster** (Message Window): Displays error messages, including IP address warnings for the device (ilc-131-eth1).

The status bar at the bottom indicates the current page is 23 of 25, and the system drive C: has more than 2GB of free space.



PC WORX - Master-Thesis

Datei Bearbeiten Ansicht Projekt Code Online Extras ?

Busaufbau

- Master-Thesis
 - 172.16.10.10 2700973 ilc-131-eth1 /// ILC 131 ETH
 - Ressource
 - STD_RES ILC131_43
 - # MODBUS_CLT
 - # INTERBUS 0 . 0
 - Touch Display

Gerätedetails Buskonfiguration

172.16.10.10 2700973 ilc-131-eth1 /// ILC 131 ETH [Erweiterte Einstellungen]

Erweiterte Einstellungen

- Ethernet
- SNMP Agent
- PROFINET Device Aktivierung
- Web-Server

IP-Adresse: 172 . 16 . 10 . 10

Subnetz Maske: 255 . 255 . 255 . 0

Gateway-Adresse: 172 . 16 . 10 . 1

Verwendung eines BootP Servers

Verwendung eines DHCP Servers Senden

DNS-Name: ilc-131-eth1 Senden

Echtzeithreinstellungen

Zeit: 11:27:29 Systemzeit

Datum: Samstag , 7. Mai 2016 Senden

Einstellungen Einlesen

IP Einstellungen | **Erweiterte Einstellungen** | Kommunikation | IP Vergabe | CPU Diensteditor

Symbole/Variablen

Master-Thesis

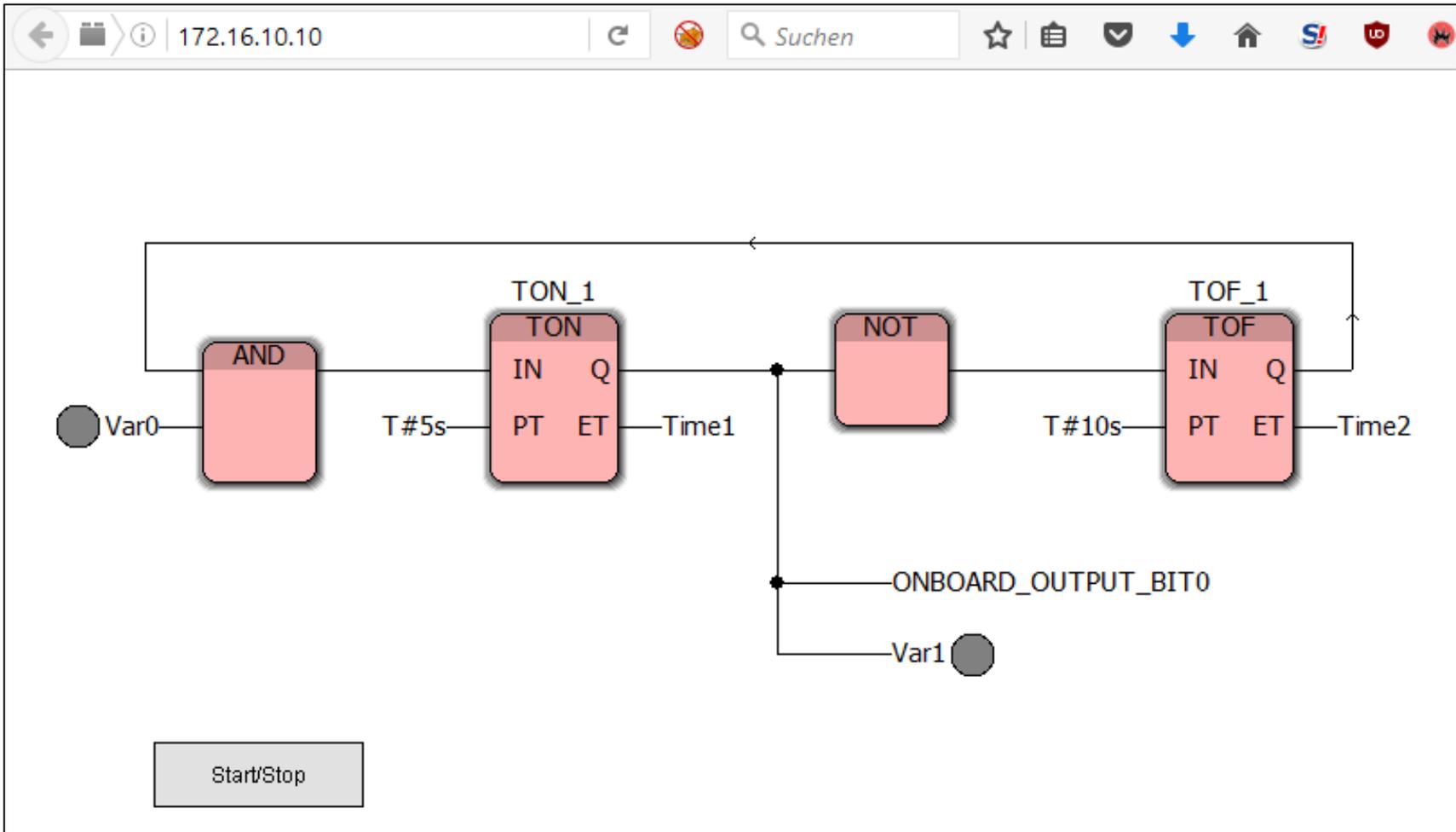
- 172.16.10.10 2700973 ilc-131-eth1 /// ILC 131 ETH
 - Ressource
 - STD_RES ILC131_43

| Symbol/Variable | Datentyp | Gerät | Prozessdatum | I/Q | Datentyp | Byte, Bit | Adresse | Symbo... | Funktionstext | Anschlußpunkt |
|-----------------|----------|-------|--------------|-----|----------|-----------|---------|----------|---------------|---------------|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Meldungsfenster

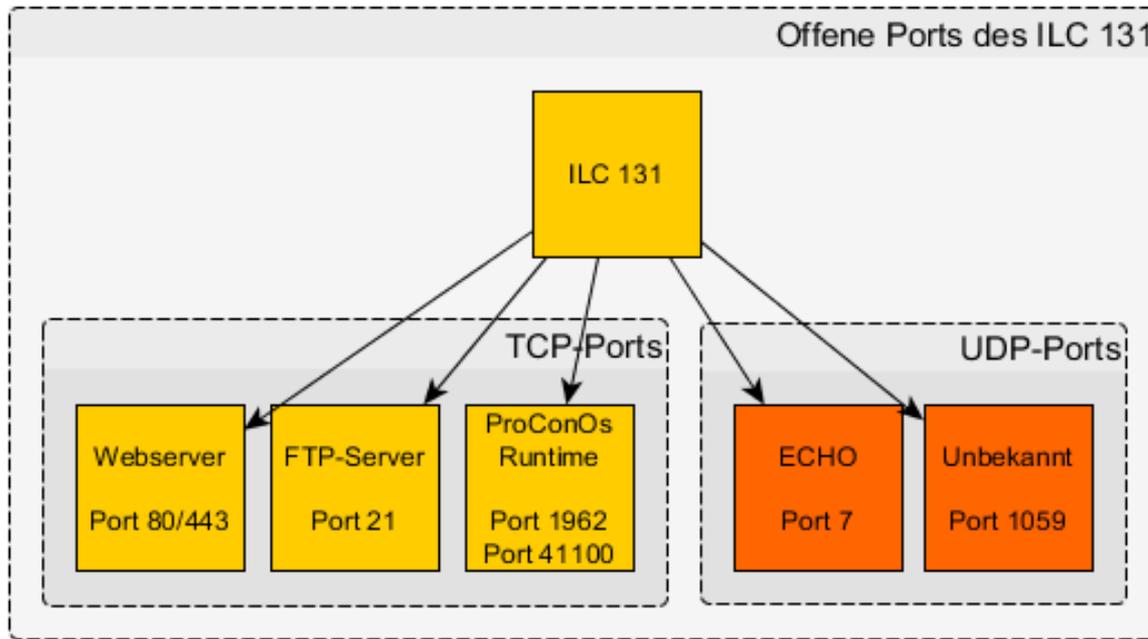
Drücken Sie F1 für Hilfe

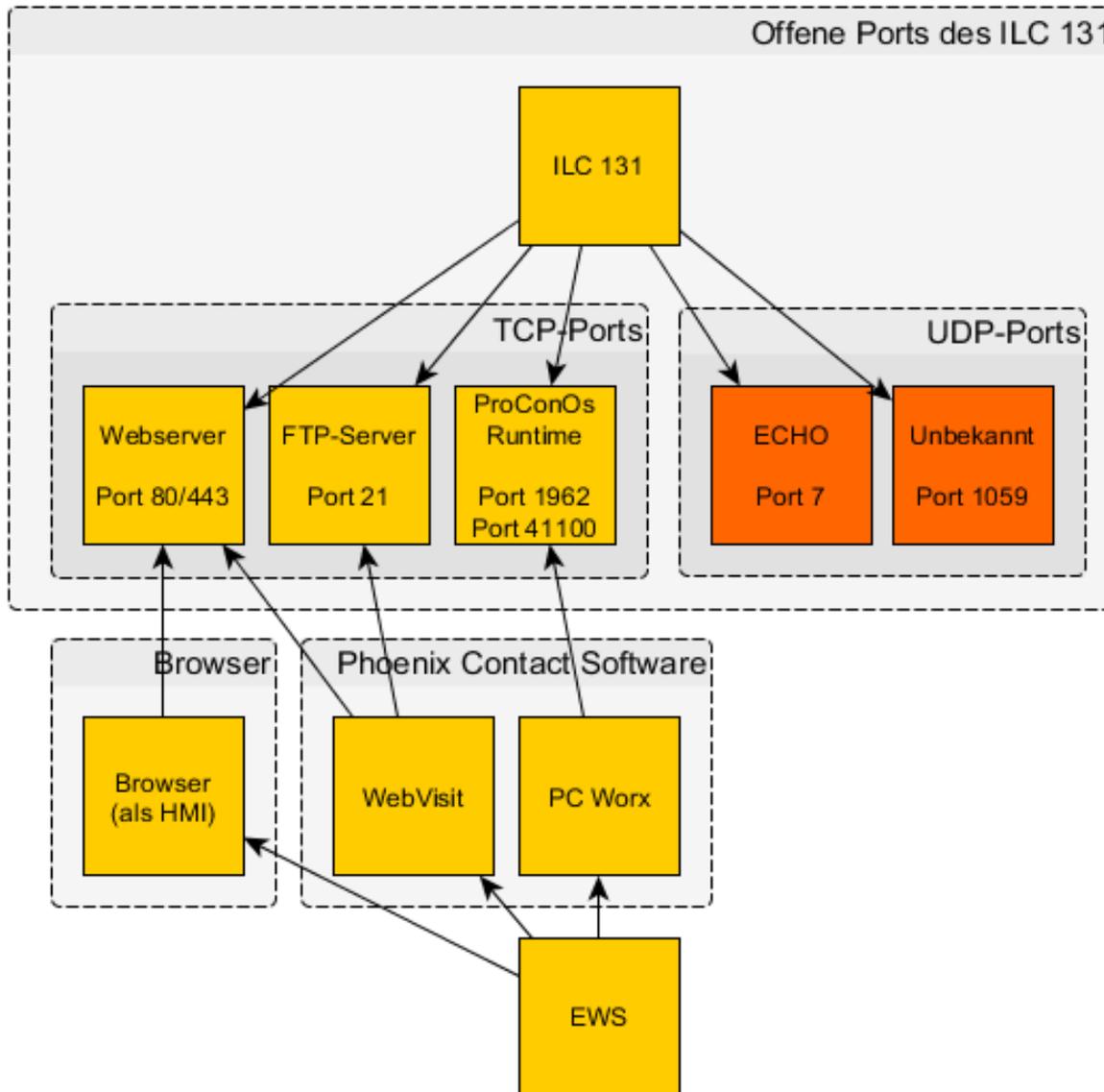
C: >2GB



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

- Durchführung
 - Portscan
 - Mitschneiden des Datenverkehrs
 - ...





- Binär-Proxy: Canape



CANAPE - D:\ownCloud\Uni\MA\Screenshots\PCWorx.canape

File View Trust Extension Help

Net Graph - 41100 Net Graph - 1962 **Fixed Proxy - 1962** Parser

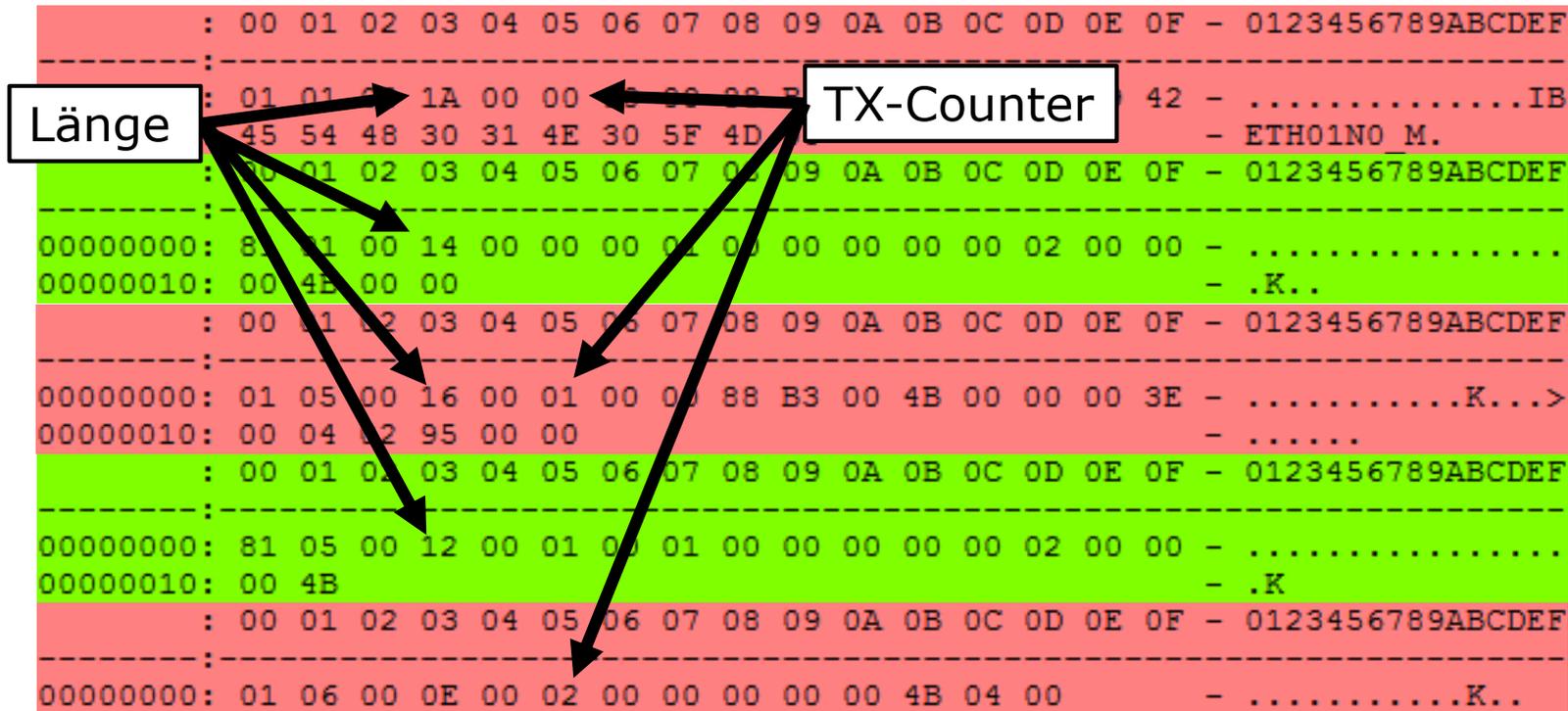
Settings Packet Log Text Log Global Meta Conns History Active Graphs Injector Redir

Project Explorer

- Project
- Scripts

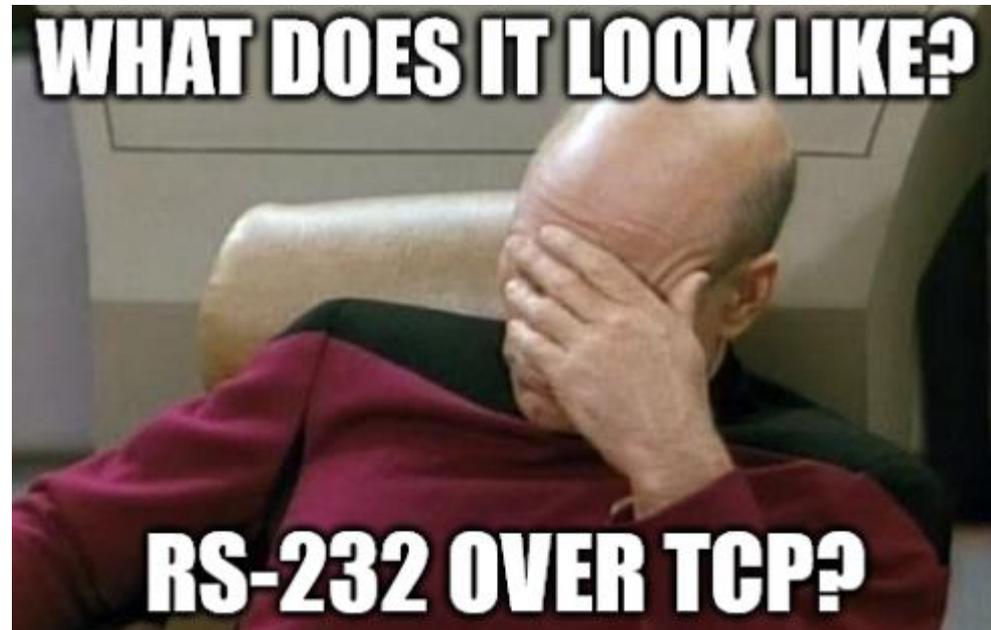
| No | Tag | Data | Length | Hash |
|----|-----|---|--------|-----------------|
| 1 | Out | \x01\x01\x00\x1A\x00\x00\x00\x00\x03\x00\x0CIBETH01NO_M\x00 | 26 | 929CDCB291D0... |
| 2 | In | \x01\x00\x14\x00\x00\x00\x01\x00\x00\x00\x00\x02\x00\x00\x00\x00\x00 | 20 | 7AF39566CB93... |
| 3 | Out | \x01\x05\x00\x16\x00\x01\x00\x00\x00\x00\x00\x00>\x00\x04\x02\x00\x00 | 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\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\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\x04jyy\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\x06*\x00\x01\x00\x00 | 30 | C1500FF8DB2A... |
| 11 | Out | \x01\x05\x00\x16\x00\x05\x00\x00\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\x06jyy\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... |

■ Paket-Detailansicht



Wie bitte?

- *Länge* und *TX-Counter* im TCP-Datensegment?
- TCP-Header enthält doch schon die Länge!
- TCP macht doch die Flusskontrolle!
- RS-232 over TCP?



Entwicklung von Paket-Parser

- Bytes eine Bedeutung
- Verschiedene Paket
- Support" Funktion

The screenshot shows a network packet capture tool interface. The main window displays a list of packets, with the selected packet highlighted in red. The packet data is shown in hexadecimal and ASCII format. Below the main window, a detailed view of the CPU Request packet structure is shown, including fields for code and parameter count.

Packet Data (Hex/ASCII):

```

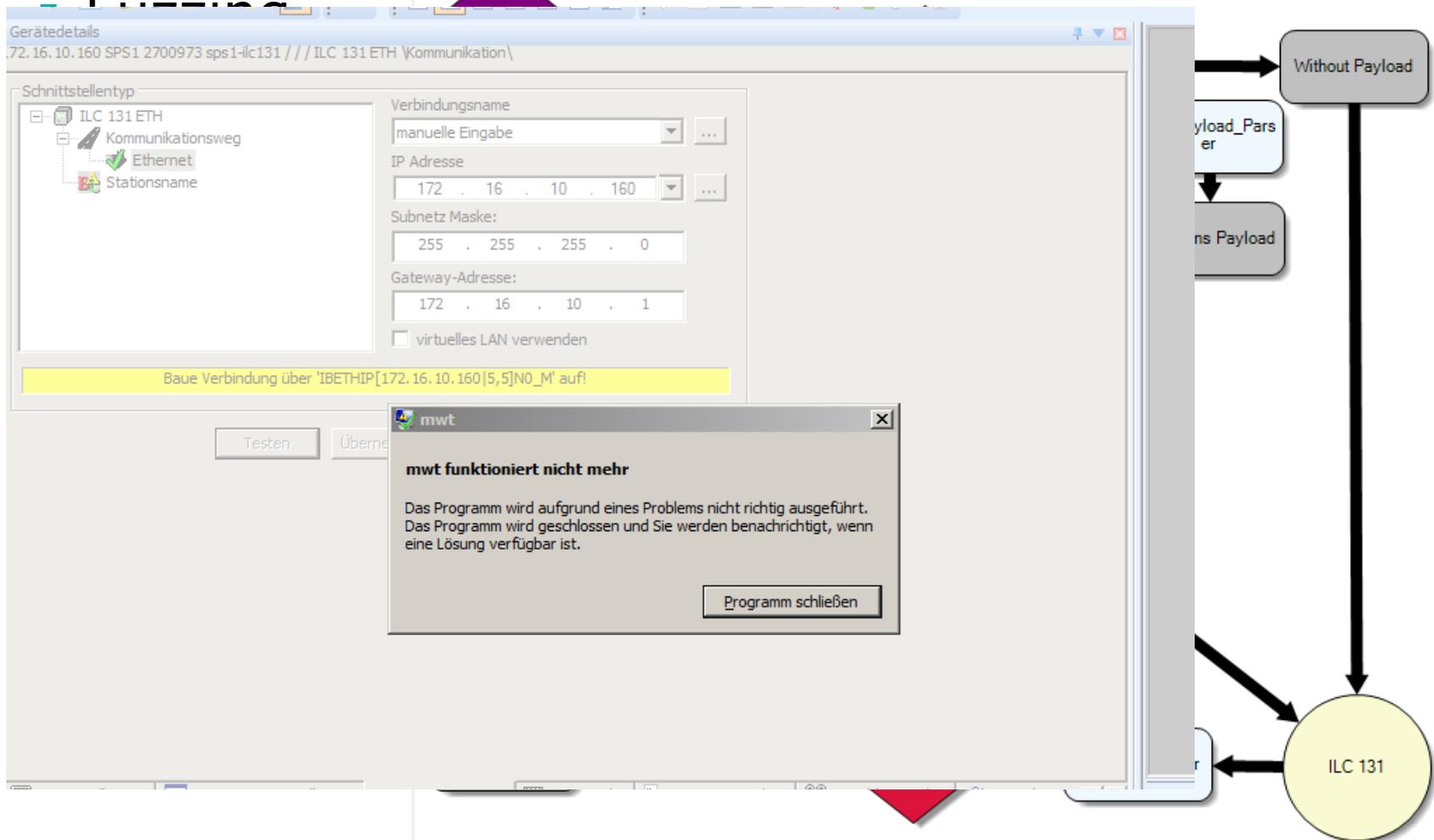
: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F - 0123456789ABCDEF
-----:
00000000: 01 05 00 16 00 01 00 00 88 B3 00 4B 00 00 00 3E - .....K...>
00000010: 00 04 02 95 00 00 - .....
  
```

CPU Request Structure:

```

<CPU_Get_Version_Info_Request>
0295 (* Code *)
xxxx (* Parameter Count *)
  
```

The interface also shows a list of request types on the right, including File_Request, IP_Addr_Request, RTC_Request, Value_Request, Version_Info_Request, Controller_Request, IP_Addr_Request, CPU_Set_RTC_Request, CPU_Set_Value_Request, and Firmware_Update. The status bar at the bottom indicates the device is offline and provides navigation options like 'Senden' and 'Bibliothek <<'.



- 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

■ Industrielle Kontrollsysteme (ICS)

- Was ist das eigentlich?
- Ein weiteres Beispiel:

