UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L4 – Smart Grid and AMS

György Kálmán,
UiO
gyorgy.kalman@its.uio.no

Josef Noll
UiO
josef.noll@its.uio.no

https://its-wiki.no/wiki/TEK5530

Overview

- Recap: value chain and attack surface
- Electric grid
- Smart grid
- Smart metering
- Situation in Norway

Recap: Attack surface

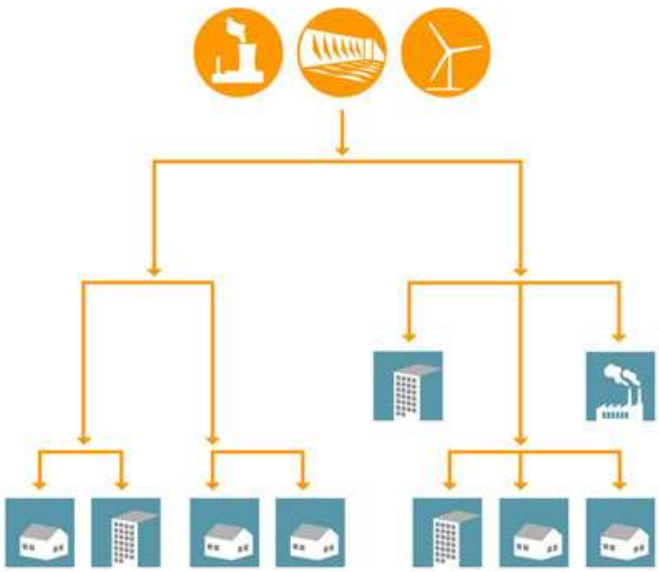
- It's not about the device. One shall see the big picture
- Structured approach with well-known steps: e.g. securing a web interface, analysis and setup of protocol parameters (e.g. avoid fallback to weak crypto), analysis of data to select correct protection
- Insecure network services: unfortunately, typical for industrial applications
- Transport encryption: use appropriate technological solutions
- Cloud interface
- Mobile interface
- Appropriate granularity in security configuration: e.g. monitoring, logging, password and lockout parameters
- Insecure software
- Physical security

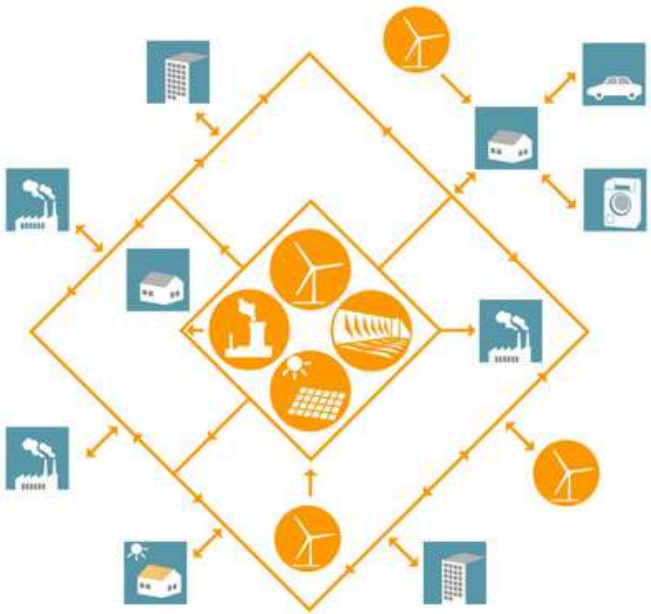
Electric grid

- Nation/continent-wide critical infrastructure
- Synchronized from production to consumer
- Key to most services of the society
- Reaches in practice every home and installation
- Very conservative (that's very much understandeable!)
- Was always kind of smart, the difference is in:
  - Resolution and timeliness of data
  - Use of IT
  - Ratio between consumers and producers

Electric grid – contd.

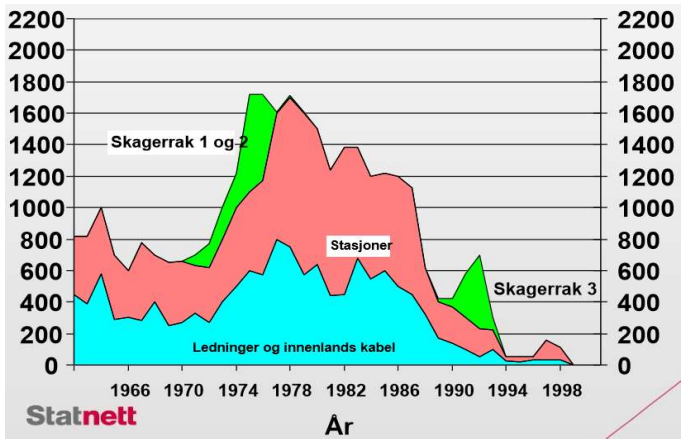
- traditional electric grid vs. smart grid, figure from ABB

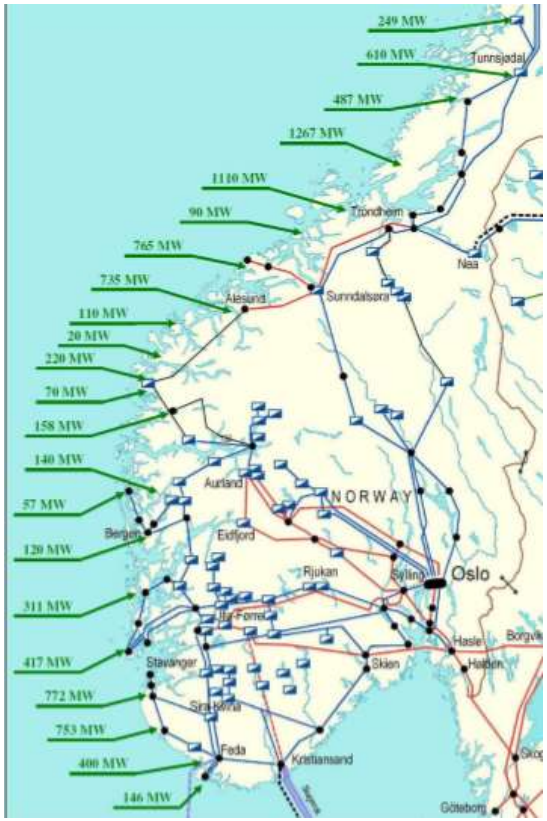




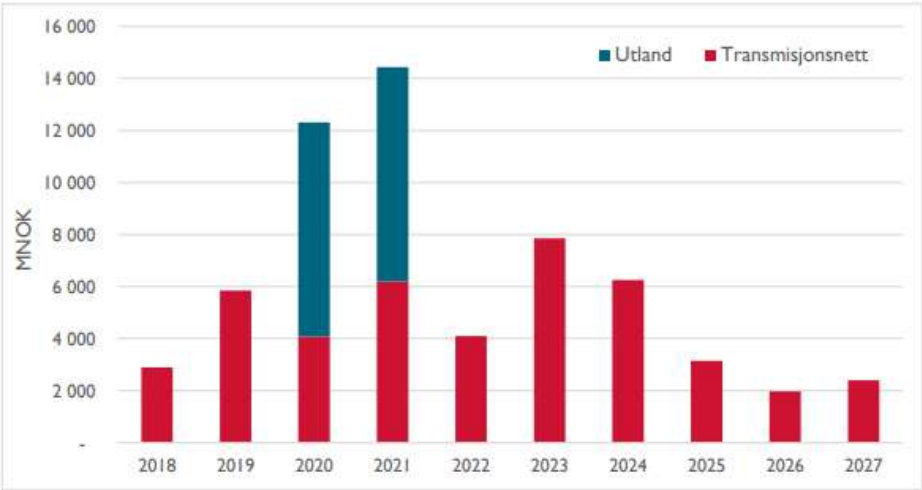
Smart Grid

- Motivation to build a smart grid: save on investments, higher profit rate, better stability, renewables, some cost reduction in emloyees
- Possible new services based on acquired data (big data)
- Operational stability
  - Integration of the volatile production of renewables
  - Synchrophasor operations
  - Microgrids – possibility for island operation – internet-like operation
- Higher electricity price for households
  - Can lower the pressure on the network for consumer peak hours
  - Can enable new services to be delivered by the utility
- Relevance for Norway:
  - Easy-controllable water plants
  - Low investment rate 90s-2000s

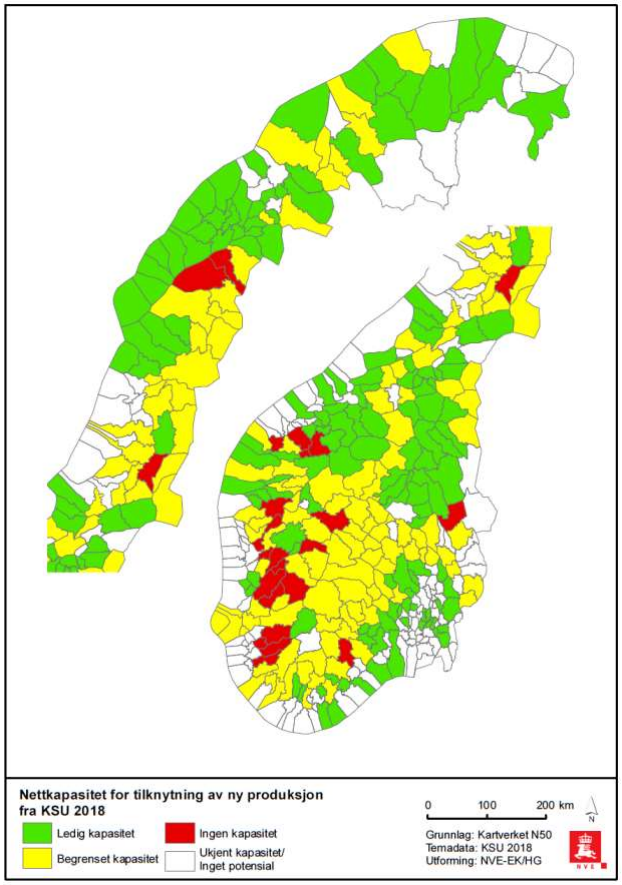




Two figures from NVE



Figur 14: Forventede investeringer i transmisjonsnettet per år for 2018–2027.



Figur 13: Oversikt over kommunenes kapasitet for ny småkraftproduksjon.

Smart Grid – contd.

- Technological points:
  - Network control has continous and real time picture of the network (compare to IT networks)
  - Multi-directional power flow – in practice it might not, implementation-dependent, but for sure a lot of generation plants compared to traditional grid
  - Not just monitoring, but direct control down to the end nodes

- Risk analysis and management
  - Clear, real time data with high resolution – this is new
  - Big data with correlation to e.g. weather, measurement data from neighbours, renewable prediction
  - Soft (price) and hard (switch off) measures to deal with high risk situations
  - Clear, high resolution, processed documentation of grid history – potentially high value

- Economics
  - Until now, small consumers were saved from the swings in the power-spot price
  - Cutting peaks reduces investment needs in distribution and core
  - Might lead to some reduction (I don't expect that)
  - Has a social aspect with e.g. prepaid power, free hours etc.

Smart Grid – technology challenges

- Time synchronization
  - Key in protection, control, monitoring
  - GPS or distributed signal
- Communication
  - Wired in parallel with the core network
  - Partly also with the distribution
  - Wireless or powerline to consumer – active research area: multihop, 5G
  - Licensed or unlicensed band, mesh, zigbee, ISA100 using e.g. 6LoWPAN
  - Quality of Service
    - Translation of engineering requirements to network metrics
- Security and privacy
  - Remote switch-off is required functionality – annoying if a bot is doing it
  - High resolution data with unlimited history on use

7

Advanced Metering Systems

- History: smart metering was present for big consumers since more than a decade, power factor corr.
- Now moving to the household, required by law (in Norway)
- Adds new possibility for load control: consumer (AMS), generation, big consumers, energy storage
  - Operations central (at grid control) [load control] – operations central (at local power utility) [load control] – consumer [smart meter with remote switch-off]
- Meter components
  - Tamper resistance is key (both for utility and consumer)
  - CPE with potentially one interface in home network (home automation) and utility (reporting)
  - Firewall? Future proofing? Ownership on traffic? Availability requirements?
  - Health-Safety-Environment

Advanced Metering Systems – assessment

- CPE: not within secured perimeter from the utility viewpoint, access needs cooperation from consumer
- consumer has no control on communication towards the utility
- Disassembly and probing already possible with a few hundred EUR investment
  scope, logic analyzer, a bit better soldering iron, cables, devel. circuit board
- In addition: analysis of the communication, analysis of the radio spectrum (if radio is used)
- From communication side: CLI, webinterface, multiple communication interfaces, limited resources in the device, will be the same for a decade or more
- Potentially millions of devices of same type
- Services (maybe the main point for customer satisfaction):
  - Opens communication with the AMS through the internet
  - Maybe also third party
  - Breaches here _will have_ a physical dimension

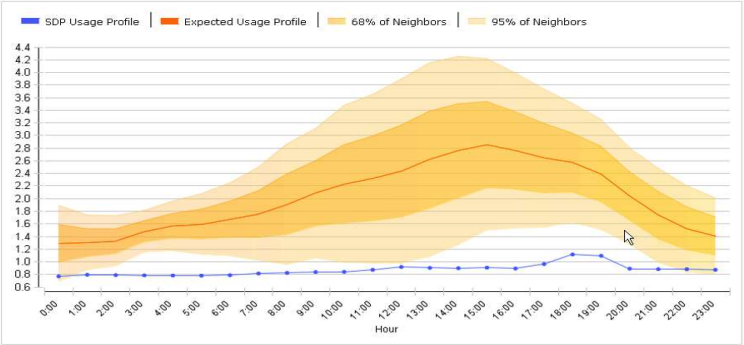


Figure from Siemens

Advanced Metering Systems – Network security

- Utility and consumer can't trust eachother
- Isolation of the AMS system from the rest of the utility
- Communication policies and configuration – segmentation, firewalling, patches
- Who owns the network?
- How to run an IDS/IPS in this infrastructure?
- How to monitor the whole system?
- Integration of data placed in common server area
- Best practice: test, preprod, prod environments

- Incident handling with heuristics
- Trusted external provider and/or detailed SLAs

- Attack surface again: CLI, webif,remote management, home automation, consumer services,data history, shared services

Advanced Metering Systems – Network security contd.

- Mitigation:
  - Engineering teams need to be extended with IT security members – see on the safety example!
  - Some kind of transformation solution for requirements between engineering and IT
  - Software Development Life-Cycle change
  - External entity monitoring security compliance

  - Tamper resistance
  - VPN/MPLS/overlay networks
  - Crypto
  - Traffic shaping

  - Traffic filtering (e.g. No egress traffic from AMS network or internet from servers)
  - Software security analysis (e.g. Monitoring software shall not do modifications)
  - External access to production systems, typically services
  - Confirmed good implementation of logging
  - Avoid «compatiblity-solutions», like auth. fallback

A short example

SHODAN | kamstrup | Explore | Enterprise Access | Contact Us

Exploits | Maps

TOP COUNTRIES

South Africa	1
Sweden	1
France	1
Denmark	

Total results: 4

78.79.193.77
host-78-79-193-77.mobileonline.telia.com
Telia Sonera AB
Added on 2017-01-23 05:19:51 GMT
Sweden, Uppsala
Details

```
HTTP/1.1 302 Moved Temporarily
Connection: Keep-Alive
Keep-Alive: timeout=900
Transfer-Encoding: chunked
Date: Mon, 23 Jan 2017 05:19:41 GMT
Server: Chero
Location: htt
X-Powered-By:
Set-Cookie: P
Ex...
```

166.159.88.107
107.sub-166-159-88.myvzw.com
Verizon Wireless
Added on 2018-02-03 12:03:56 GMT
United States
Details

```
□[0;22;27;25;24m□[0m□[2J□[1;1H□[?25h
                Rugged Operating System v3.9.1 (May 18 2011 09:26)
        Copyright (c) RuggedCom, 2008 - All rights reserved

        System Name:    CCV 81 77N
        Location:       Location
        Contact:        Contact
        Pro...
```

166.130.140.13
mobile-166-130-140-13.mycingular.net
AT&T Wireless
Added on 2018-02-02 06:10:04 GMT
United States
Details

```
RuggedCom RX1510
```

63.120.127.26
Georgia Public Web
Added on 2018-02-02 00:16:51 GMT
United States, Sandersville
Details

```
□[0;22;27;25;24m□[0m□[2J□[1;1H□[?25h
                RuggedSwitch Operating System v1.6.1
        Copyright (c) RuggedCom, 2004 - All rights reserved

        System Name:    chakotay
        Location:       SYNCHRONODE #1
        Contact:        Kelly McQuaig (478-232-7004)
```

kamstrup

Radio Link Concentrator

Role Admin
Password •••••
Login

A short example - 2

Alert (ICS-ALERT-16-263-01)

More Alerts

BINOM3 Electric Power Quality Meter Vulnerabilities

Original release date: September 19, 2016

Print | Tweet | Send | Share

Legal Notice

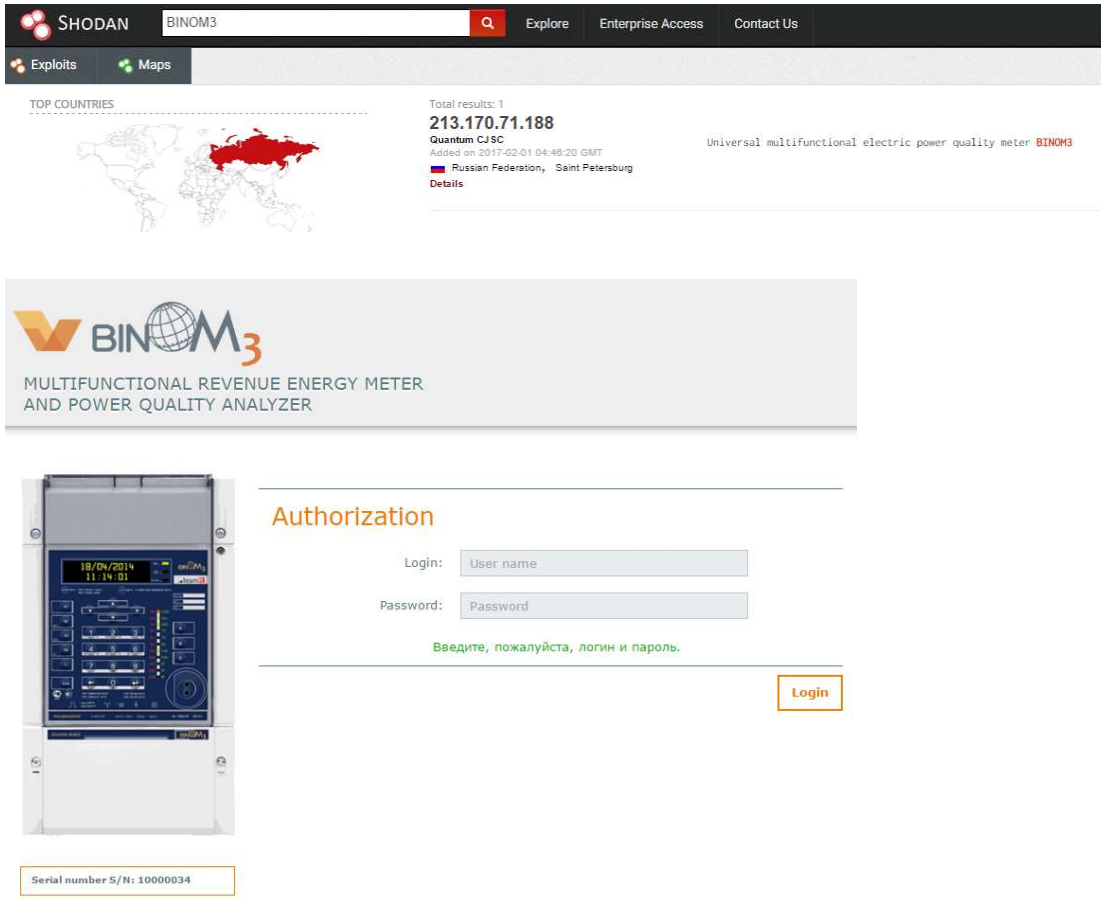
All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

NCCIC/ICS-CERT is aware of a public report by Karn Ganeshen of vulnerabilities affecting the BINOM3 Electric Power Quality Meter, a meter designed for autonomous operation in automated systems. According to this report, the vulnerabilities are remotely exploitable. This report was released after the researcher coordinated with ICS-CERT. ICS-CERT has attempted to notify the affected vendor of the report without success. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details for the following vulnerabilities:

Vulnerability Type	Remotely Exploitable	Impact
Reflected and stored Cross-site Scripting	Yes	Injection of arbitrary Java Script
Clear Text Passwords	Yes	Privileged access to device
Sensitive information leakage in GET request	Yes	Privileged access to device
Access Control Issues	Yes	Password authentication is not enabled on Telnet Access



L4 Conclusions

- Converged infrastructure
- IoT expands the attack surface
- Security requirements do also depend on type of data processed
- Devices with multiple intefaces present a risk
- End-to-end security and life-cycle support is key
- Privacy
- Why is this all good for the user?