UNIK4750 - Measurable Security for the Internet of Things

L4 – Smart Grid and AMS

György Kálmán,
UiO/NTNU/mnemonic
gyorgy.kalman@its.uio.no

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

http://cwi.unik.no/wiki/UNIK4750, #IoTSec, #IoTSecNO

Overview

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

UNIK4750: Lecture plan

- 19.01 L1: Introduction
- 26.01 L2: Internet of Things
- 02.02 L3: Security of IoT + Paper selection
- **09.02**
  - **L4: Smart Grid, Automatic Meter Readings**
  - **L5: Service implications on functional requirements**
- 16.02
  - L6: Technology mapping
  - L7: Practical implementation of ontologies
- 23.02 ---- Vinterferie
- 02.03 L8-9: Paper analysis with 15 min presentation (6-7 hrs)
- 09.03 L10-11: Paper analysis with 15 min presentation (3 hrs)
  L12: Logical binding - industrial example
- 16.03
  - L13: Multi-Metrics Method for measurable Security
  - L15: System Security and Privacy analysis
- 23.03
  - L16: Real world examples, quest lecture (1.5 hrs)
  - L14: Multi-Metrics Weighting of an AMR sub-system (2.5 hrs)
  - L18: Real world IoT service evaluation group work (2 hrs)
- 30.03
  - ---- no lecture
- 06.04
  - L18: Real world IoT service evaluation group work – contd.
  - Wrap-up of the course
- 13.04 ---- Påskeferie
- 20.04 ---- Exam

Recap: Attack surface

- It’s not about the device. One shall see the big picture

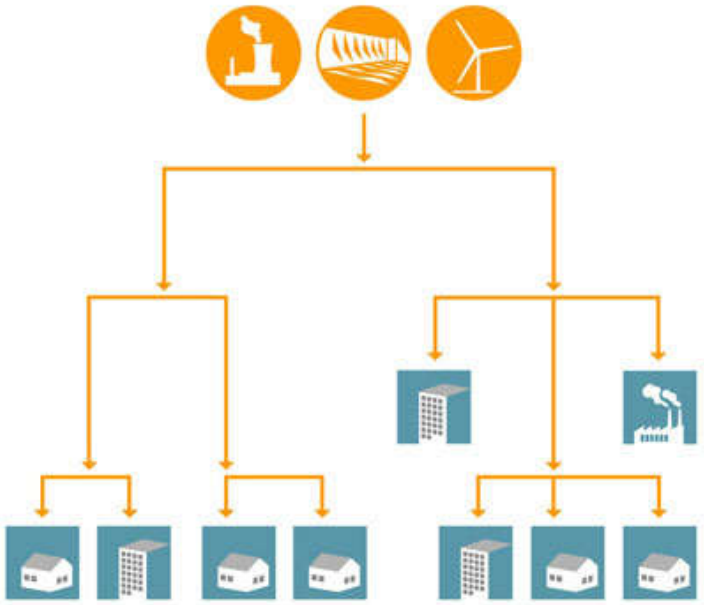
- Structured approach with well-known steps: e.g. securing a web interface, analysis and setup of protocol parameters (avoid fallback to weak crypto), analysis of data to select correct protection
- Insecure network services: unfortunately, typical for industrial applications
- Transport encryption: 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

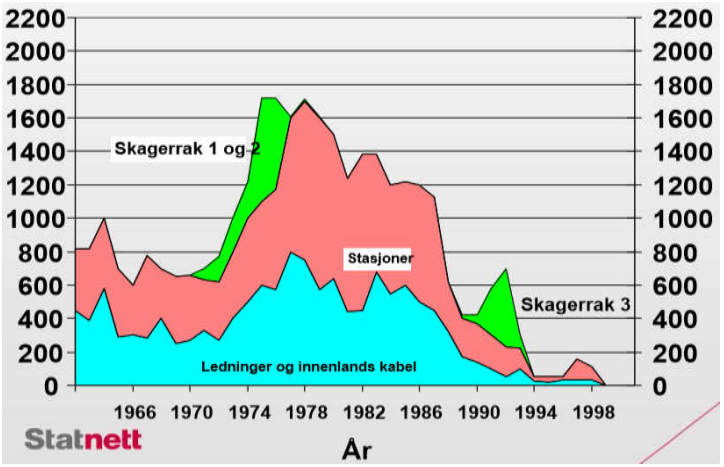
Electric grid – contd.

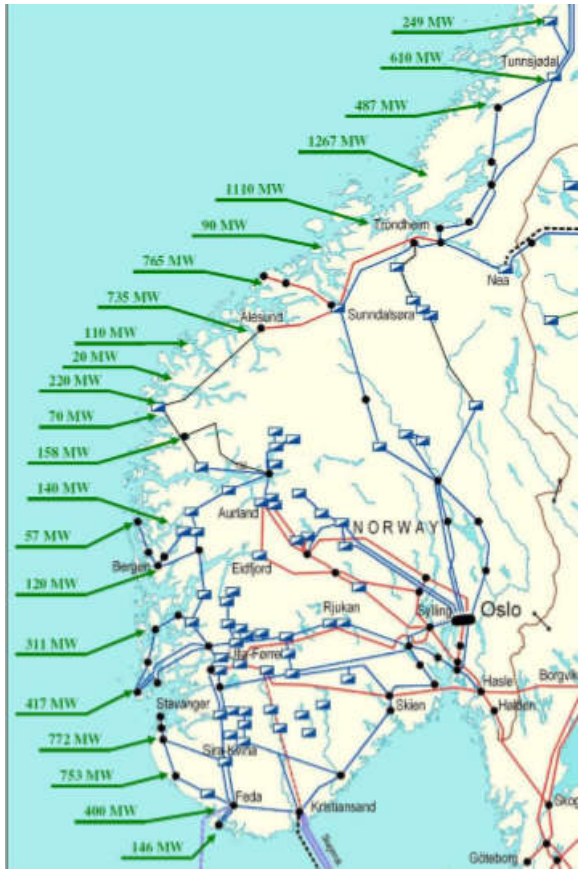
- traditional electric grid vs. smart grid, figure from ABB



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





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 (tax on company car because of roadtoll logs)

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

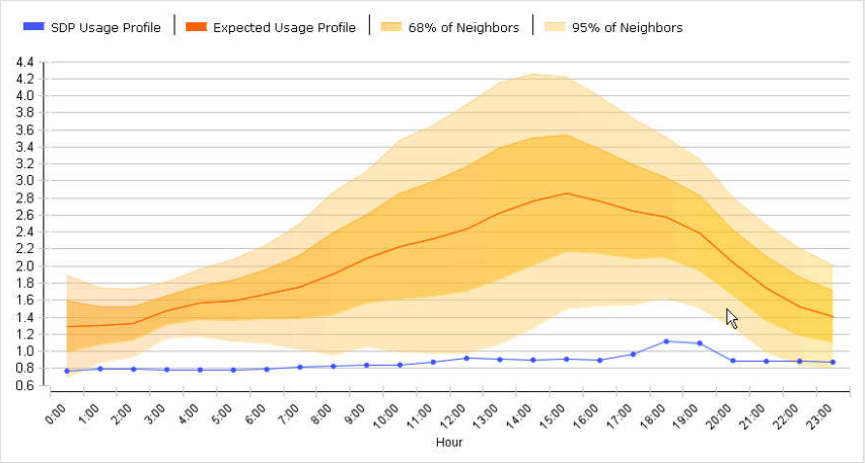
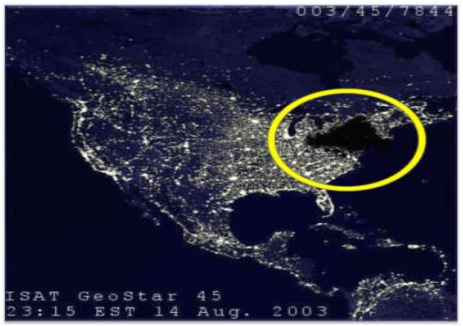


Figure from Siemens

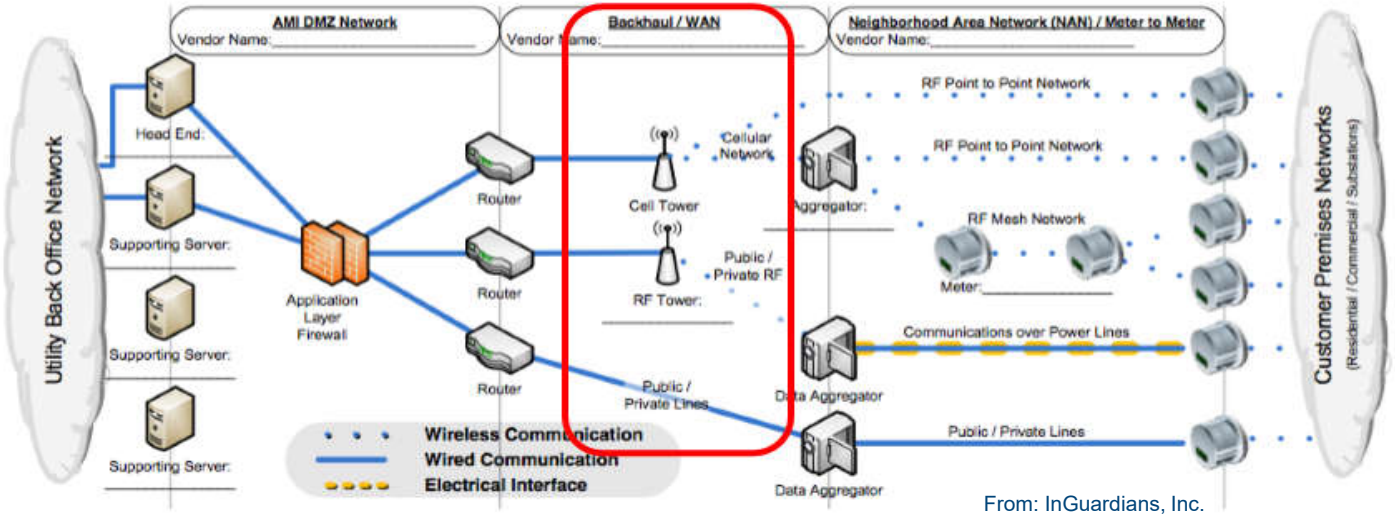
Advanced Metering Systems – Network security

- 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

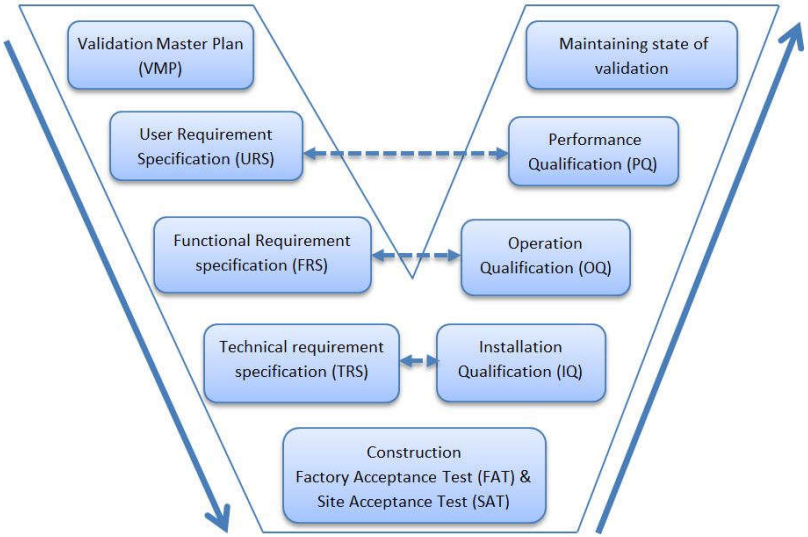


From: InGuardians, Inc.

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



Advanced Metering Systems – Risk management

- Analyze vulnerabilities
  - They are not unique (see L3): CLI, web interface, SQL injection, cross-site request forgery – all the typical things one is getting when testing a web service
- Mitigate risk
  - Again, crypto, but this is not a universal answer
  - Data processing
  - Development and operation life-cycle

L3 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?