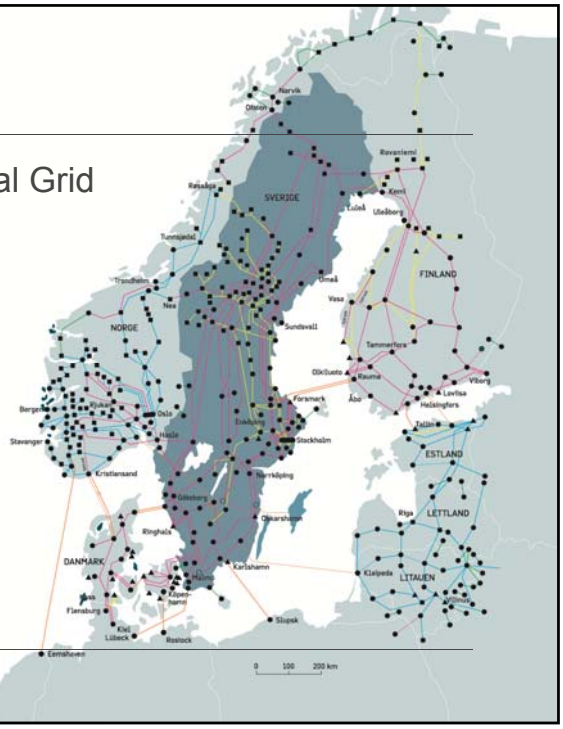
Agenda

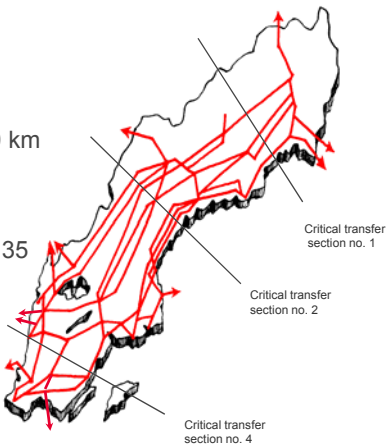
- What is Svenska Kraftnät (SvK, Swedish national grid)
- International/national perspectives
- R&D at SvK
- Cyber security
- Challenges
- Discussion (10-15 min)

The National Grid



The National Grid

- Transmission lines: 15 000 km
  - 220 - 400 kV
  - HVDC
- No. of switching stations: 135
- National Control Centre: Sundbyberg



5

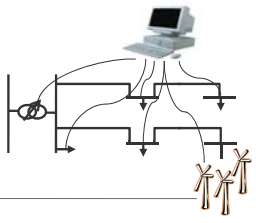
Before de-regulation 1996

- National, regional and local levels
- Statens Vattenfallsverk operated on all levels
- Cooperation (not competition) between companies, to optimallay operate
- SCADA/EMS-systems: Proprietary, not open.

6

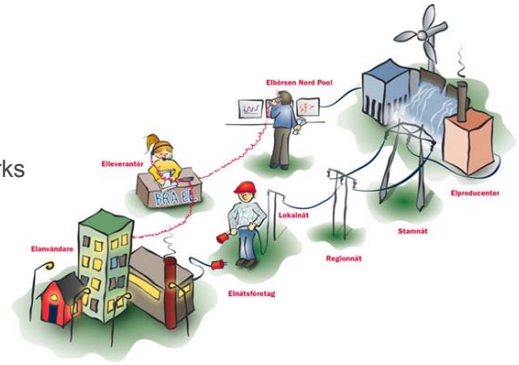
After de-regulation 1996

- Statens Vattenfallsverk was split:
  Affärsverket Svenska Kraftnät (Swedish National Grid)+
  Vattenfall AB
- Both SvK and VAB started to separate their structures for Operation/Control
  - SvK: KRASS (KRAftSystemStyrning)
  - VAB: DRISS (DRIftStödSystem)



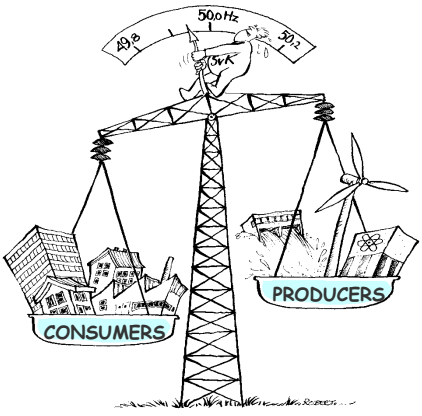
National – Regional and local networks

- National grid
  - 400 and 220 kV
  - Svenska Kraftnät
- Regional networks
  - 40 – 130 kV
  - ~ 40 networks
  - 10 companies
- Local networks
  - < 40 kV
  - ~ 310 networks
  - ~200 companies



System Operator Responsibility

- **Power system in balance: 50 Hz**
  - Handles the national momentary balance
  - Manages bottlenecks
  - Distributes costs



Svenska Kraftnät

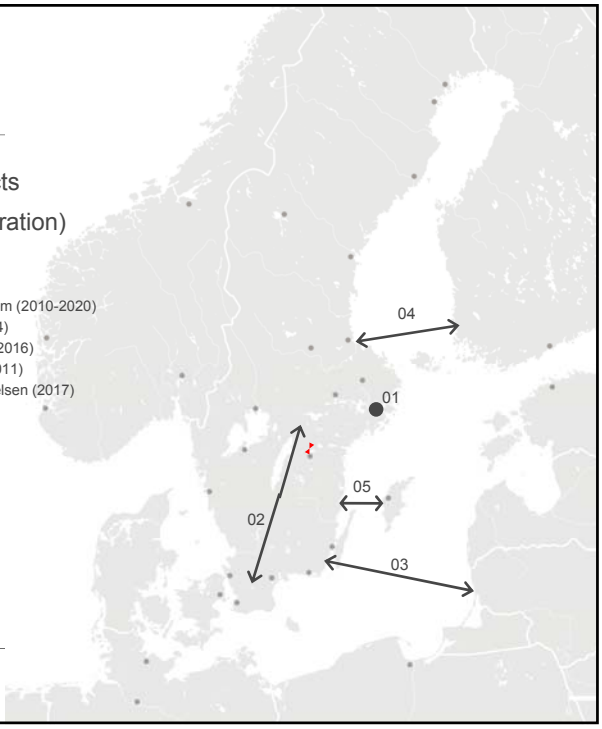
- **Power line highways + connections to neighboring countries**
- **System responsible authority**

Also: Nordic perspectives

- Nordic countries have lot of common interests
- Co-funding of projects

Large Projects
(put into operation)

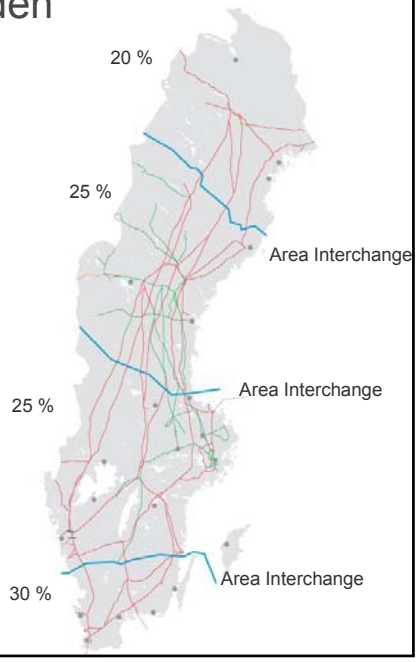
01 Stockholms Ström (2010-2020)
02 Sydlänken (2014)
03 NordBalt (2015/2016)
04 FennoSkan 2 (2011)
05 Gotlandsförbindelsen (2017)



Wind Power in Sweden

- **Goal**
  30 TWh / 12 000 MW
- **Identified projects**
  45 000 MW
- **Current capacity**

Hydro	16 000
Nuclear	9 000
	25 000 MW



Requests for connecting wind power

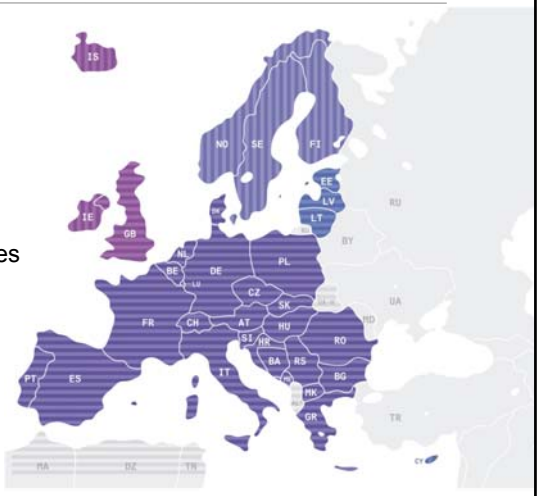
Total ≈ 36 000 MW

(corresponds to ≈90 TWh)
Sweden total 150 TWh/y

Q: Which projects will be realized?

European Collaboration – ENTSO-E

- 41 TSOs from 34 countries
- Founded on 19 Dec 2008 and fully operational since July 2009
- A trans-European network
  - 532 million citizens served
  - 880 GW generation
  - 305,000 Km of transmission lines
  - 3,200 TWh/year demand
  - 380 TWh/year exchanges



European Network for Transmission System operators – Electricity: ENTSO-E

- ENTSO-E committees (www.entsoe.eu):
  - System Operation Committee (SOC)
  - Market Committee (MC)
  - System Development Committee (SDC)
  - R&D Committee (RDC)
    - R&D Plan

Broad scope

- Energy. Power supply
- Critical for the society
- Environment
- Technical issues
- Market issues
- Swedish, Nordic, International

- *Cyber security: Devil is in the details. Small issues are big and strategically important!*

Why is cyber security important for electric utilities?

- Important – society critical – infrastructure for society
  - Power, telecom, water, gas, transport, …
- More and more dependent on functioning IT-systems
- If IT-systems do not work:
  - No-one knows why…
  - Delays : SJ did not know why a signal error occurred. Sabotage?

Dam – Three Gorges China

R&D Svenska Kraftnät

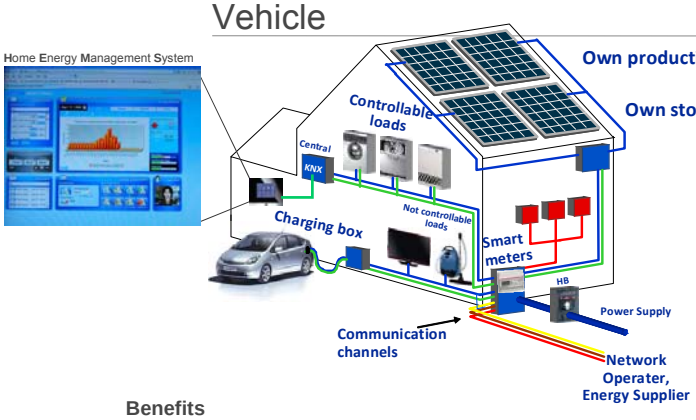
- R&D Plan 2015-2017. Updated yearly.
  - System aspects, Operation, robustness, Security, Environment, IT and telecommunications, Network technology, Maintenance of the grid, Energy market, Maintenance knowledge and education. Dam safety.
  - E.g. Wind power connection research, Support to PhD & MSc projects
- 3 MEuro / year
  - R&D companies, universities, consultants,
- Also: 0,5 Meuro / year – electricity preparedness
  - Dam safety. SCADA Security.

Stockholm Royal Seaport – *A world class sustainable city, with a Smart Grid as the enabler*

Objectives

- 2030: fossil free
- 10 000 apartments
  30 000 office places
- 30 % in-house renewables
- Demand Side Participation

Smart Grid components: Integrated Active House and Electric Vehicle



Benefits

- Active 'prosumer' benefits from most favorable spot price
- Peak load shaving by local production, storage and time shift of consumption
- Overall reduction of energy consumption by increased consumer awareness

Cyber Security

- Digital security (not yet mature)

Versus

- Physical security (well established)

Information Security acc. to Wikipedia

- **Information security** (sometimes shortened to InfoSec) is the practice of *defending* *information* from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc)

IT Security acc. to Wikipedia

- Sometimes referred to as computer security,
- (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems

Comparison

- Information security: Routines, policies, knowledge – ”softer”
- IT-security: technically – firewalls, log-in keys– ”harder”

- But: Small technical details may have strategic importance:
  - Lost USB-sticks, computers which are not locked, …

Smart Grids
Definitions

> ”**The application of digital technology to the electric power infrastructure**”

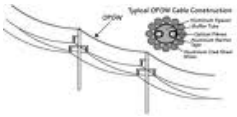
> ….and many others

Seven key EU technology challenges for the next 10 years to meet the 2020 targets, the SET-plan:

1. Make second generation **biofuels** competitive alternatives to fossil fuels, while respecting the sustainability of their production;
2. Enable commercial use of technologies for **CO2 capture**, transport and storage through demonstration at industrial scale, including whole system efficiency and advanced research;
3. Double the power generation capacity of the largest **wind** turbines, with offshore wind as the lead application;
4. Demonstrate commercial readiness of large-scale **Photovoltaic** (PV) and Concentrated Solar Power;
5. Enable a single, **smart European electricity grid** able to accommodate the massive integration of renewable and decentralised energy sources;
6. Bring to mass market more **efficient energy** conversion and end-use devices and systems, in buildings, transport and industry, such as poly-generation and fuel cells;
7. Maintain competitiveness in **fission technologies**, together with long-term waste management solutions;

Data communication

> ”Enabler” for operation/control



Increase in communication capabilility

From

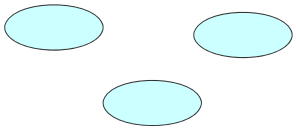
> Narrowband walking paths

To

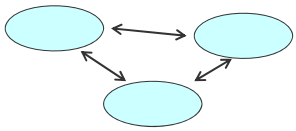
> Broadband 7-lane highways

29

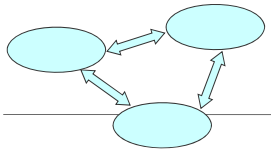
Development of Industrial Control Systems 1(2)



1. Islands of operation



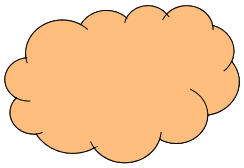
2. Interconnected



3. Partially Integrated

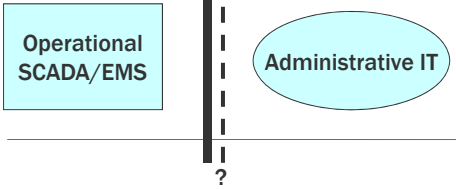
30

Development of Industrial Control Systems 2(2)



4. Today. Full integration system structure

5. De-coupling between Operational SCADA/EMS and Admin IT environments



31

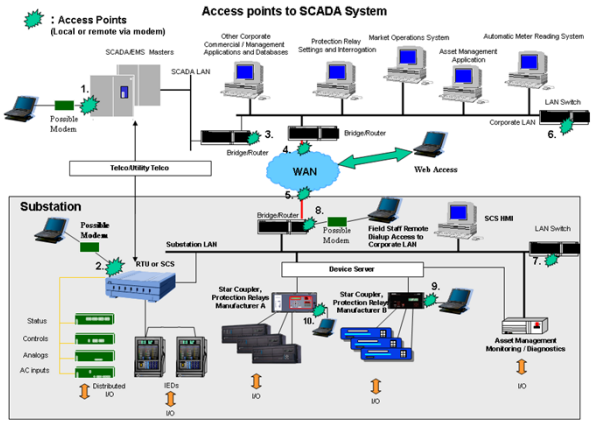
SCADA
Supervisory Control And Data Acquisition

Industrial Processes

> Power Network
> Power Production
> Telecommunication network
> Water
> Transport
> …

32

Access points to SCADA-system
Threat and possibilities



SCADA
Supervisory Control And Data Acquisition

- Increasingly accessible via Internet
- Same technical solution as common office IT systems
- Process control system integrated with office systemsIntegrering med adminstrativa IT-system
- ***Same vulnerabilities for SCADA systems as for office IT! What to do?***
- Disturbances can have severe impact on critical infrastructutes
  - Power, water, gas, transport
- ”CIP = Critical Infrastructure Protection”
- ”CIIP = Critical **Information** Infrastructure Protection”

Challenges

Interesting Topics for the Smart Grid

- **SCADA system security**, incl. evolution and legacy systems and environments
- **AMI (Automatic Meter Infrastructure) security**, incl. larger attack surface and switch between back-end (meters, earlier) to front-end (e-meters, now+future)

- Risks implied vs benefits to expect from "smartness" and balance between the two
- Risks implied by remote, network-communicated operations (+ to use Internet or not to use it)
- Privacy issues
- Can regulations imply increased security?
- What is expected from utilities vs other actors

Smart meters

- Technical possibilities. Broadband => faster, bulky
- From the households:
  - collect kWh-data, basis for billing
- To the households
  - Price information
  - **Controls** – opens up new cyber security issues
- ***"Which party will be responsible when, by mistake or by intentional digital tampering, a household is disconnected for two weeks, and that the owner of the house gets damages by destroyed food or water leakage, when he is away on two weeks of vacation?"***
  - The owner? The utility? Who?
- These issues are clearly related to cyber security and they must be raised within the electric power arena.

Delicate issues!

- ”AIC” rather than ”CIA” in electric arena
  - Confidentiality (”Sekretess”)
  - Integrity (”Riktighet”)
  - Availability (”Tillgänglighet”)

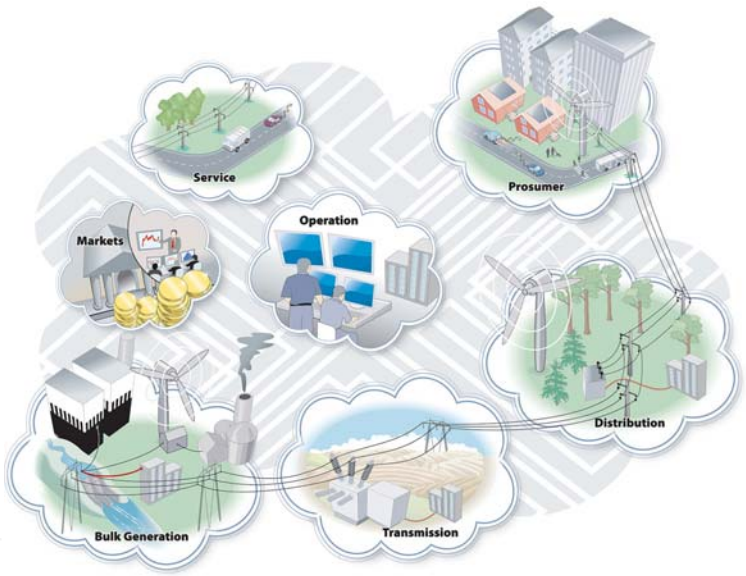
  => Low priority for Confidentiality – Risk for Intrusion?
- SCADA Security
- (Still) Enormous need for education awareness!

Smart Grid System – A way towards the use of wind power

- 20-30 TWh out of 150 TWh may be based on wind power within 10 years
- Wind power not marginal for Svenska Kraftnät
- Wind – intermittent. How maintain electrical balance?
- What kind of IT-systems are needed?
  How to present just what is needed, and not ”nice to have”?

Research issues

- Develop models which can be tested in lab and reality
- Methods to measure and design secure control systems E.g.: How secure is an Industrial Control Systems structure ?
- System architectures which include security from the beginning.
- Analysis of critical infrastructurer (SCADA system)
- How incorportare security into an existing ”legacy system”?
- …



Concluding remarks

- Swedish –> Nordic –> European R&D issues
- Climate goals => Introduction of renewables =>change in power transmission
- Smart Grid –> Smart System
- From islands-of-automation to fully integrated

Concluding remarks

- Openness. Communication capabilities
- Digital/Cyber security
  - New issue for the utility
  - Essential issue in a smart grid cirtical infrastructure
- Proprietary -> Standard and 3rd party software
- Openness creates possibilities, which we want to have
- Openness creates new problems to solve: digital security

- SCADA security: important for society criticial infrastrtucture

  power, water, transport, …
- Include security from the beginning
- R&D – an important success factor!

Recommendations

- Power utilities / customers – address security from the beginning!
- Vendors – be pro-active! Include security in solutions from the beginning!

Know incidents

- Spilling water utility Australia 48 times. Radio controlled.
- Stuxnet Siemens PLC 24 months
- Log-in issues in banks

Reflection

- IT-incidents – nothing you talk about– embarracing.

Thanks for your attention! Questions?