Information Security for the future power grid

Göran Ericsson, *Docent and Adj Professor*

Head of R&D

Lecture Chalmers 2017-09-20

Infrastructure

Today’s society relies on:

- Datacommunication
- Electricity
  - E.g.: Payment depends on these are working

Agenda

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

Transmission system operators (TSO)

National grid =
Highway for eletricty

Highest voltage
(400 kV and 220 kV)

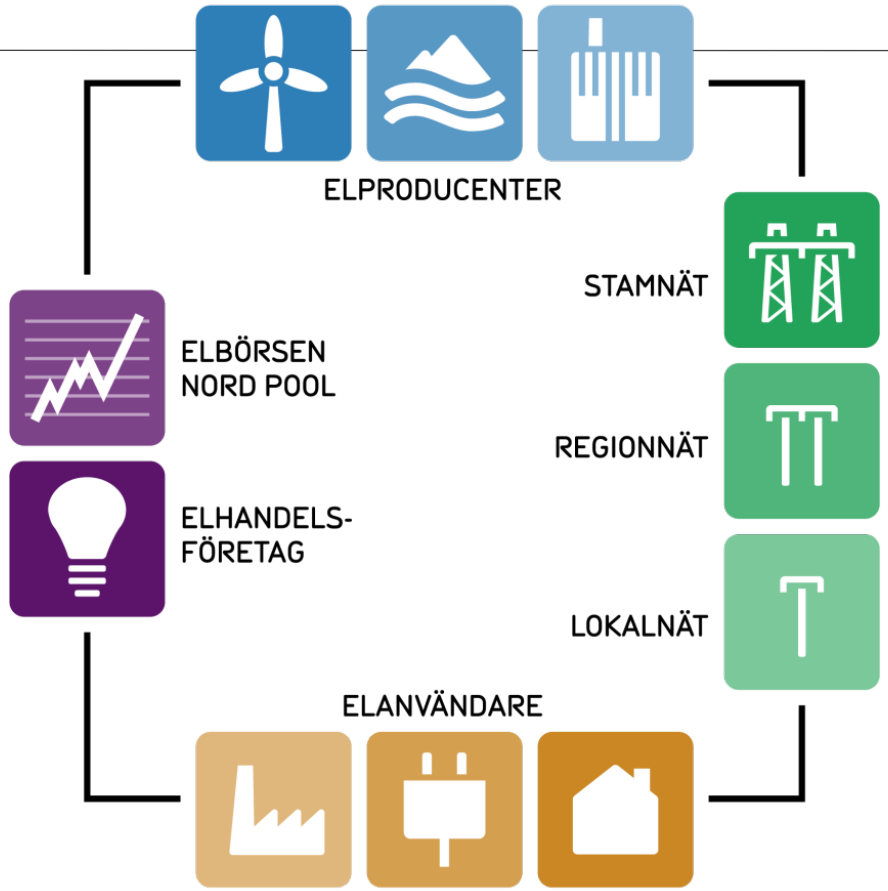
Broad scope

- Energy supply
- Infrastructure – critical for society
- Environment
- Technology
- Market issues
- National – Nordic – International

Deeper…

- Power flow – equations
- Technical solutions
- Price settings for the electricity market

- *Cyber security: The devil is in the details.*
  Small issues – big and strategically important!


ELPRODUCENTER
STAMNÄT
REGIONNÄT
LOKALNÄT
ELANVÄNDARE
ELHANDELS-
FÖRETAG
ELBÖRSEN
NORD POOL

Power system

- 15 000 km power lines
- 160 substations
- 16 international connections
- National Control Centre: Sundbyberg
- Nordic Monitoring center in Copenhagen, in operation 2017

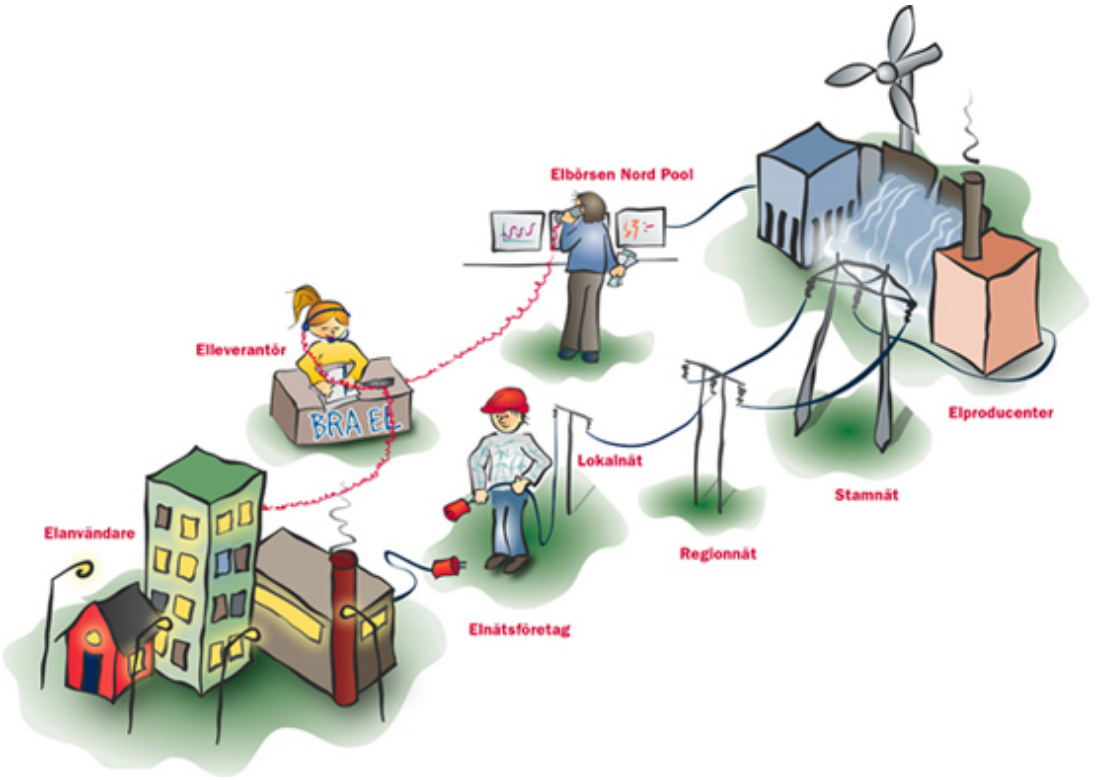
National – Regional and local networks

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

Home
- 230 V



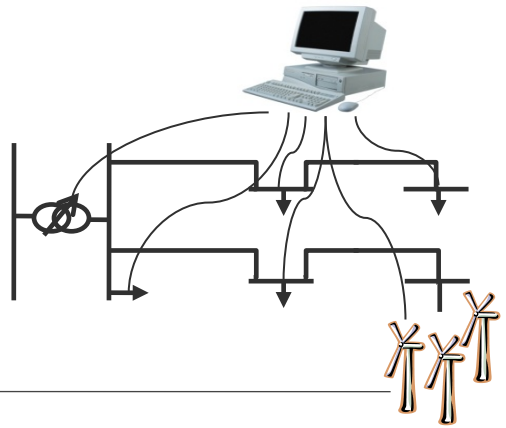
Before de-regulation 1996

- 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.

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)



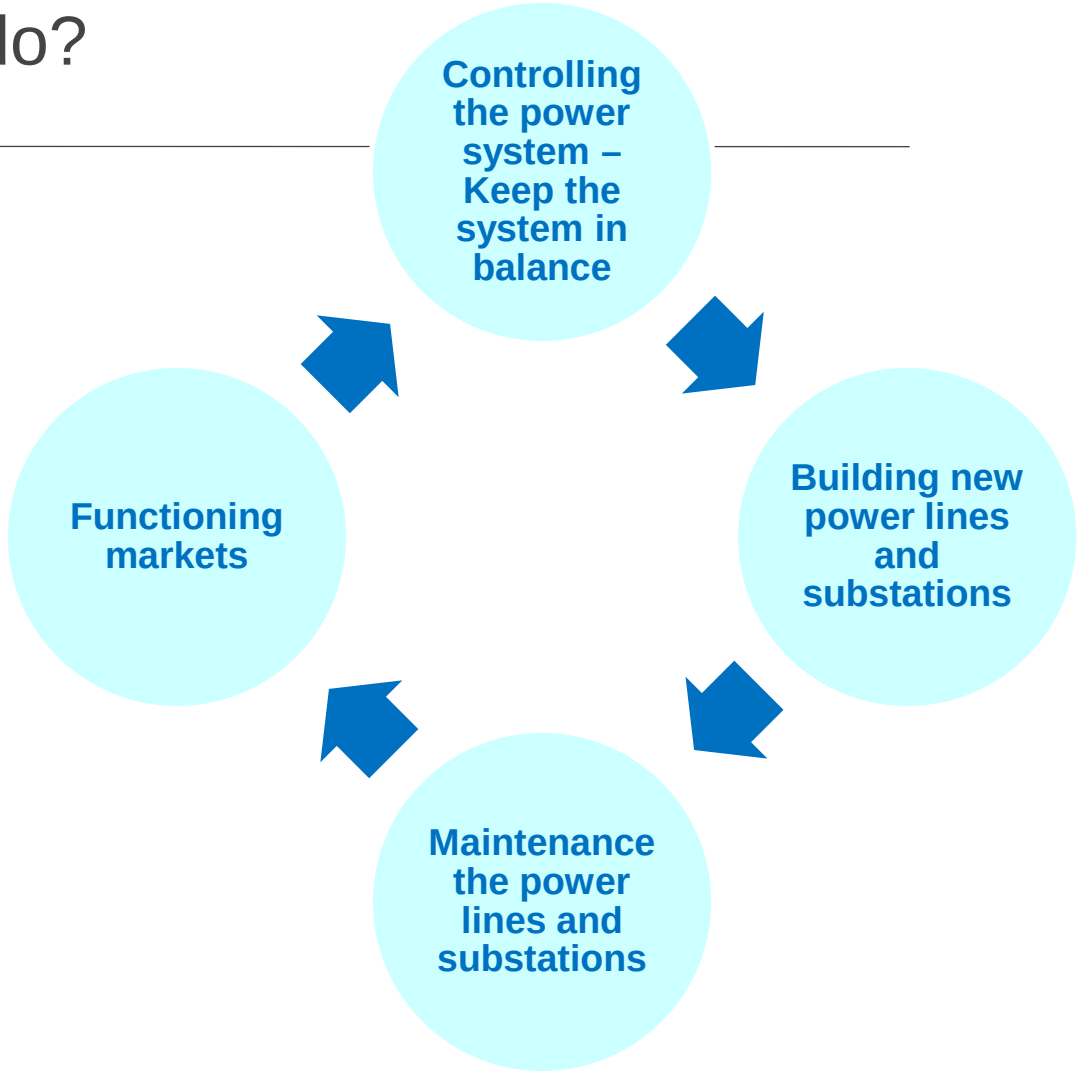
Dam – Three Gorges China

What do we do?

Order from the government

entsoe

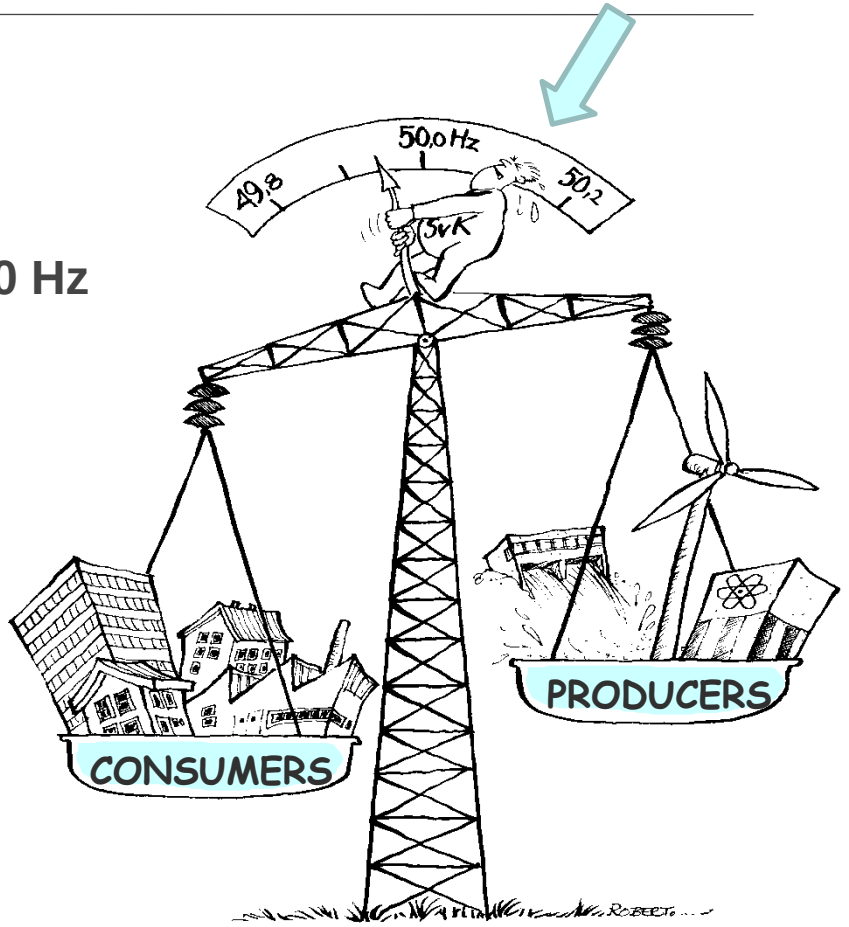
Reliable Sustainable Connected



System Operator Responsibility

Svenska Kraftnät

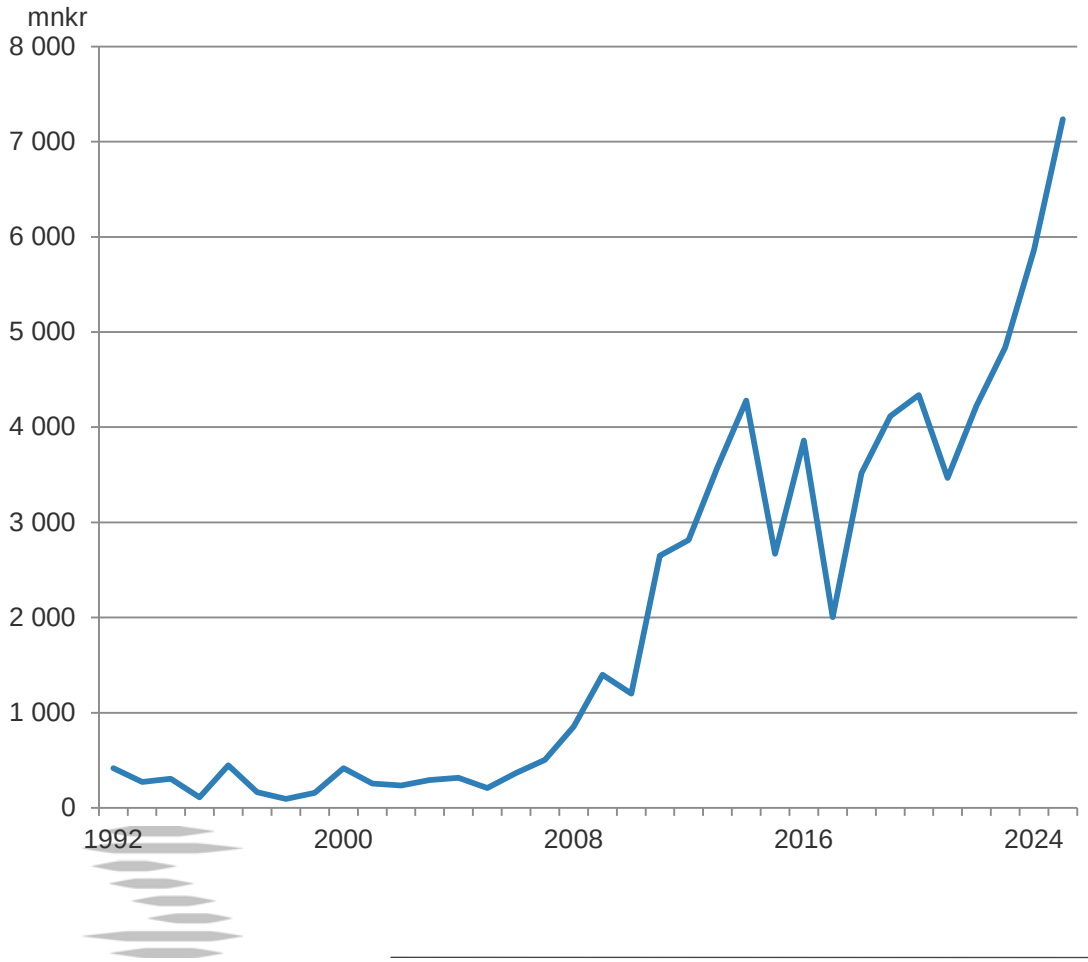
- **Power system in balance: 50 Hz**
  - Handles the national momentary balance
  - Manages bottlenecks
  - Distributes costs



Nordpool


40
35
30
25
20
15
10
EUR/MWh
28 Feb
2 Mar
4 Mar
6 Mar
8 Mar
10 Mar
12 Mar
14 Mar
16 Mar
18 Mar
20 Mar
22 Mar
24 Mar
26 Mar
Feb '17
Mar '17
SYS
SE1
SE2
SE3
SE4
FI
DK1
DK2
Oslo
Kr.sand
Bergen
Molde
Tr.heim
Tromsø
EE
LV
LT

Investments

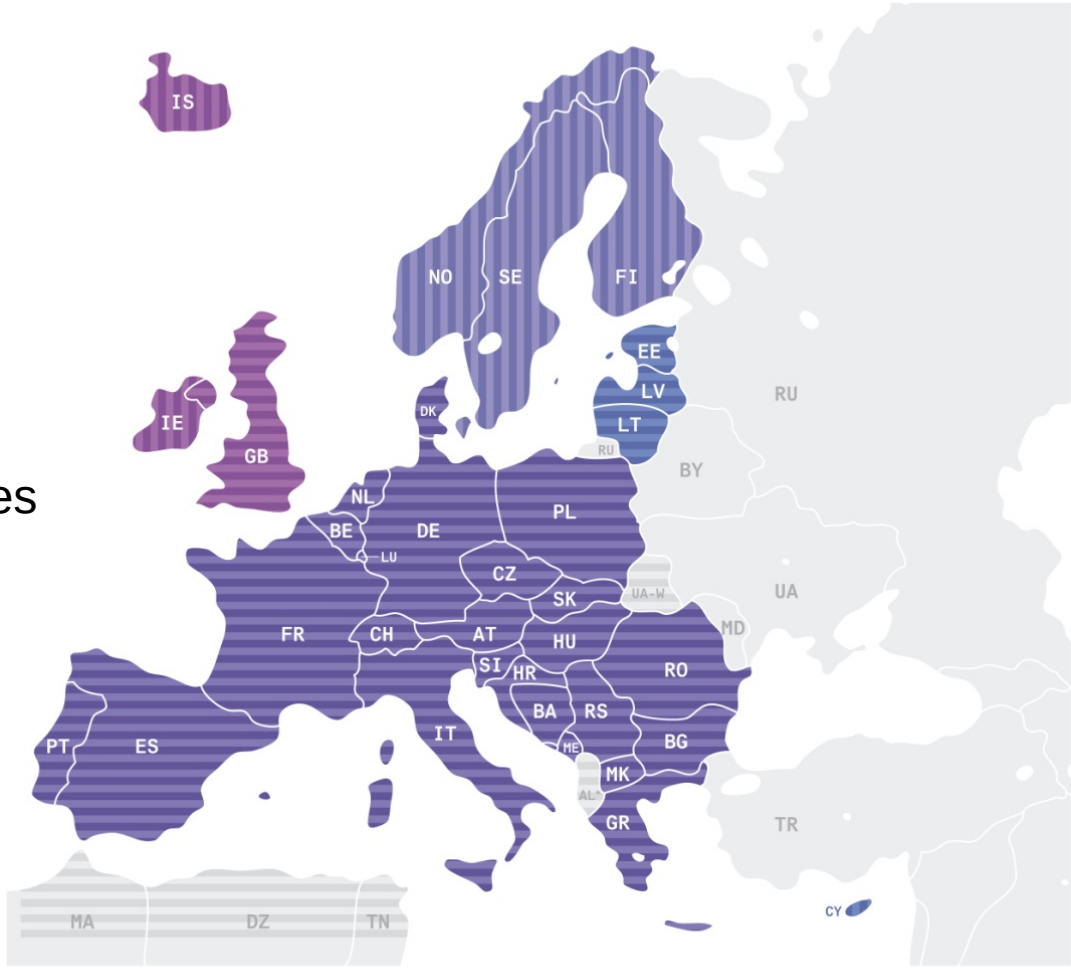


Building projects

- Sydvästlänken AC and HVDC, increase the capacity with 25 % - In operation 2017
- New AC kabel to Gotland – In operation 2021
- 400 kV cables in a new tunnel under Stockholm – In operation 2021
- Hansa PowerBridge: Sweden – Germany – In operation 2025

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&Innovation Committee (RDIC)
    - Plan and Roadmap

R&D Svenska Kraftnät

- R&D Plan. Three years, updated yearly.
  - New technology, Future power system, Operational and Planning.
  - Knowledge building: Support to MSc & PhD & PostDoc projects
- 3 MEuro / year
  - R&D companies, universities, consultants.
- Also: 0,5 Meuro / year – electricity preparedness
  - Dam safety. SCADA Security.

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?
  - Spilling water. Utility in Australia. 48 times… Radio controlled
  - Internet banking problems

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

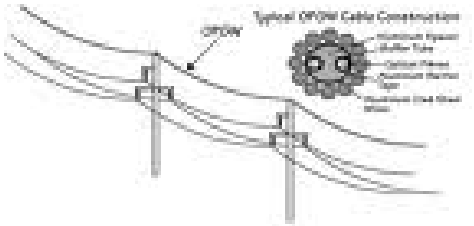
Comparison

- 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, …

Data communication

> ”Enabler” for operation/control



Increase in communication capabilility

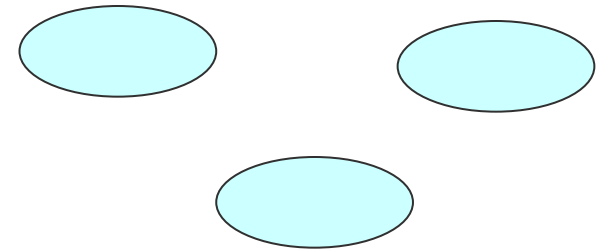
From

> Narrowband walking paths

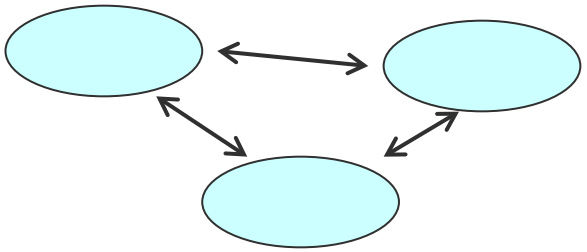
To

> Broadband 7-lane highways

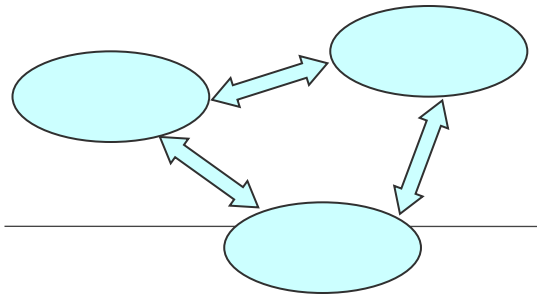
Development of Industrial Control Systems 1(2)



1. Islands of operation

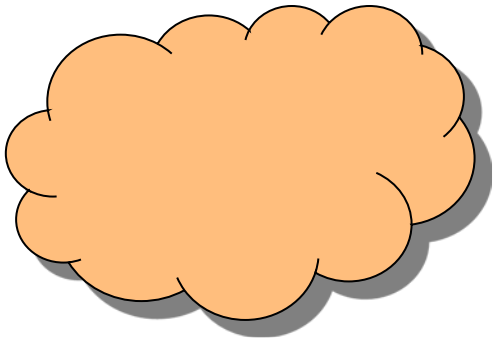


2. Interconnected



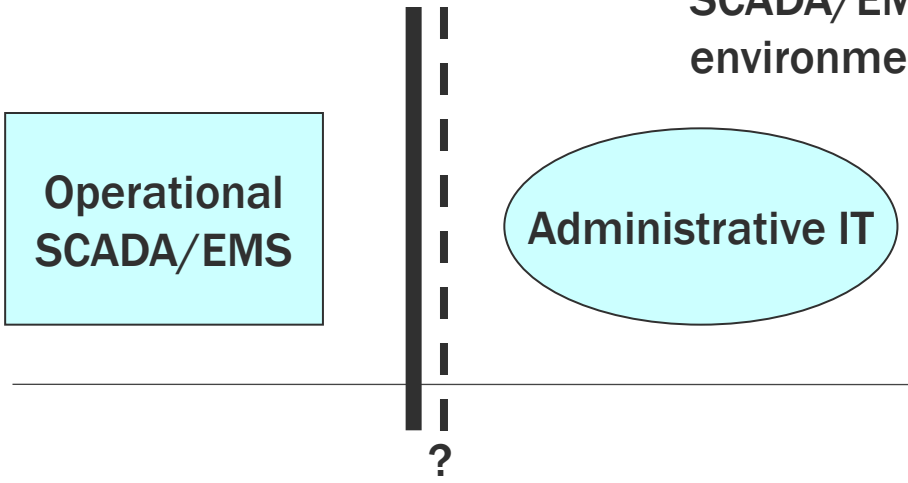
3. Partially Integrated

Development of Industrial Control Systems 2(2)



4. Today. Full integration system structure

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

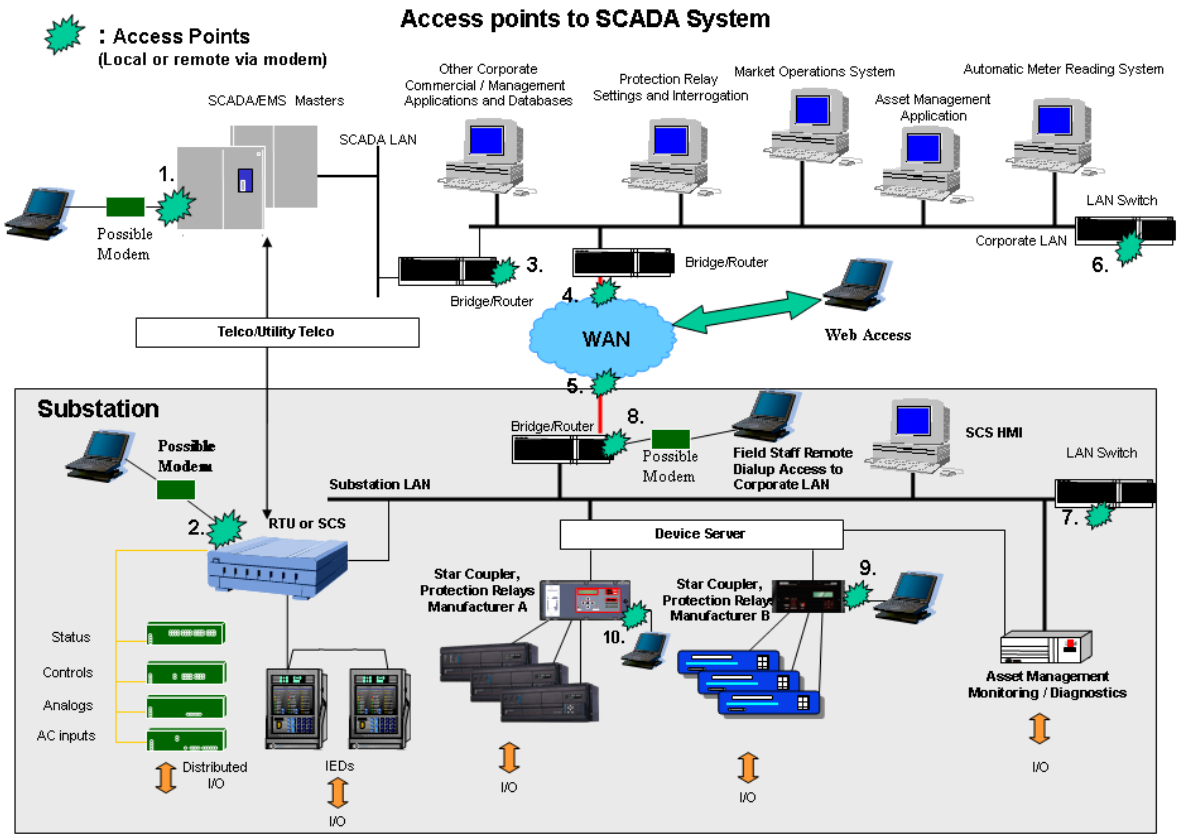


SCADA
Supervisory Control And Data Acquisition

Industrial Processes

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

Access points to SCADA-system
Threat and possibilities



SCADA
Supervisory Control And Data Acquisition

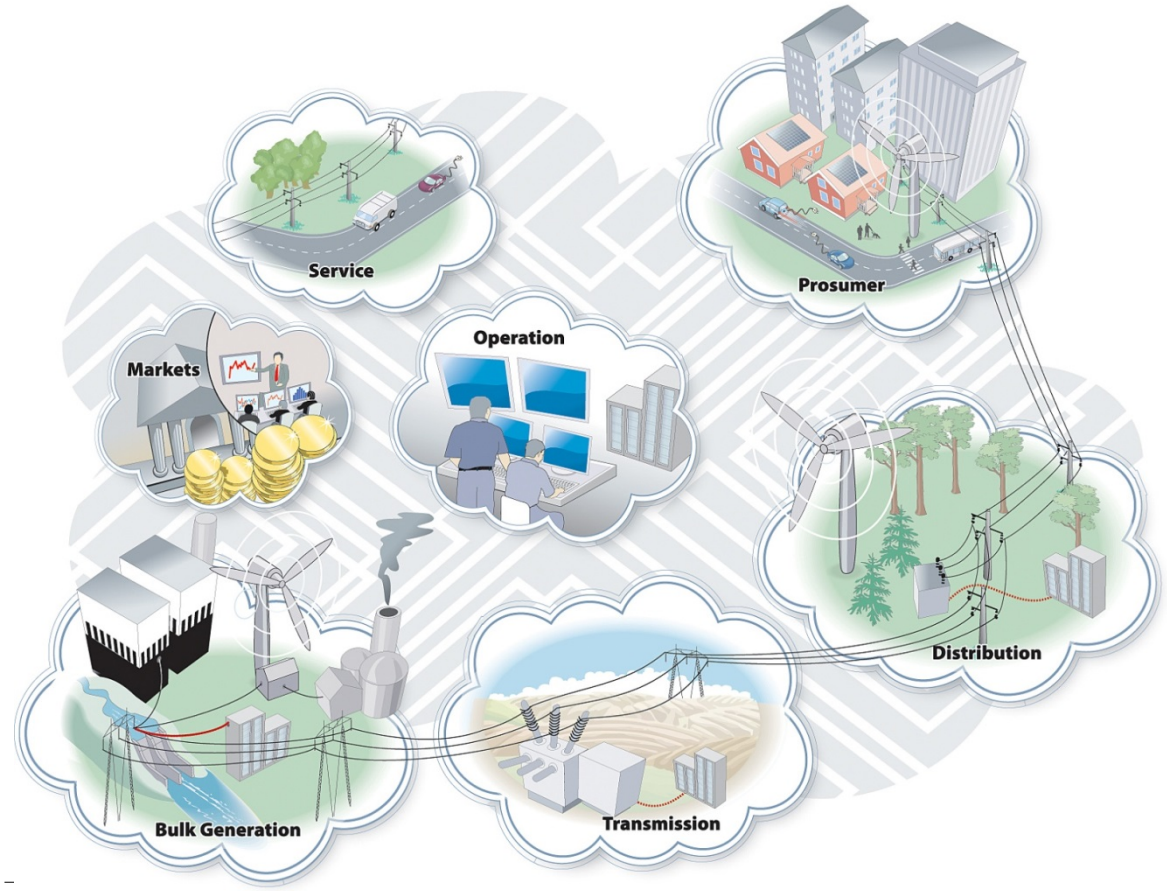
- Increasingly accessible via Internet
- Same technical solution as common office IT systems
- Process control system integrated with office systemsIntegrering med adminstrativa IT-system
- ***Same vulnerabilities for SCADA systems as for office IT! What to do?***
- Disturbances can have severe impact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

Delicate issues!

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

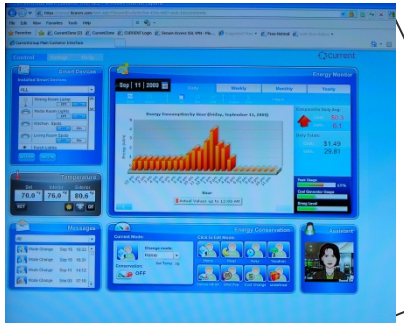
  => Low priority for Confidentiality – Risk for Intrusion?
- SCADA Security
- (Still) Enormous need for education awareness!

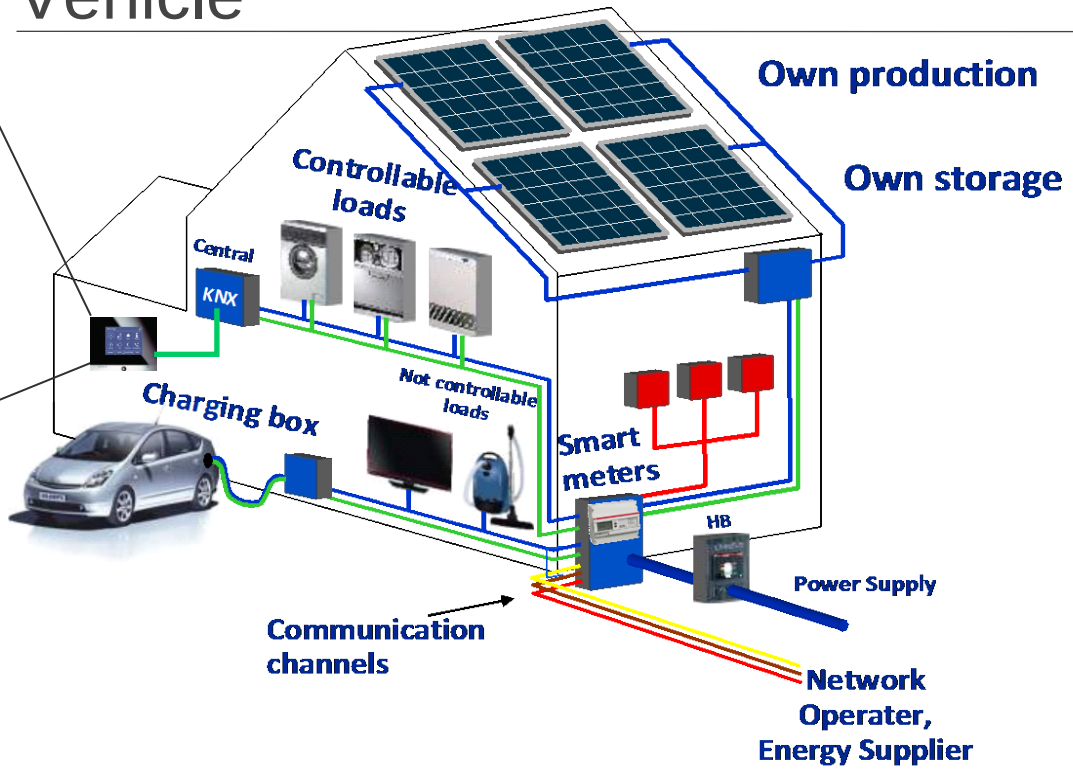
Challenges – future is integrated
Power + ICT = True



Smart Grid components: Integrated Active House and Electric Vehicle

Home **E**nergy **M**anagement **S**ystem





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

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;

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”?

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.

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.
- BUT: We must deal with cyber security issues, on *all* levels!

Recommendations

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

Research issues

- Develop models which can be tested in lab and reality
- Methods to measure and design secure control systems - How secure is an Industrial Control Systems structure ?
- System architectures - include security from the beginning.
- Analysis of critical infrastructures - SCADA systems
- 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

Concluding remarks

- SCADA security: important for society criticial infrastructures

  power, commuiction, water, transport, …

- Include security from the beginning
- R&D – an important success factor!

Thanks for your attention!
Questions?