



UiO : Department of Technology Systems
University of Oslo

TEK5370 - L9 Grid Conversion

L9 from Grid to Smart Grid

Josef Noll,

Professor, University of Oslo, Department of Technology Systems

Secretary General, Basic Internet Foundation

Kjeller, Norway, m: +47 9083 8066, e: josef@jnoll.net



György Kálmán, Ph.D., CISM, CCSP · 1st
Technical Information Security Officer (TISO) at DNB Retail
and Corporate

Nordby, Akershus, Norway · [497 connections](#) · [Contact info](#)

Agenda

- Electric grid as critical infrastructure
- Smart grid: motivation, actors, features, challenges
- Automatic Metering System
- Quality of Service
- Safety



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
- Was always kind of smart, the difference is in:
 - ➔ Resolution and timeliness of data
 - ➔ Extent of IT
 - ➔ Ratio between consumers and producers
 - ➔ Control possibilities

Transmisjonsnett
i Norge
2019

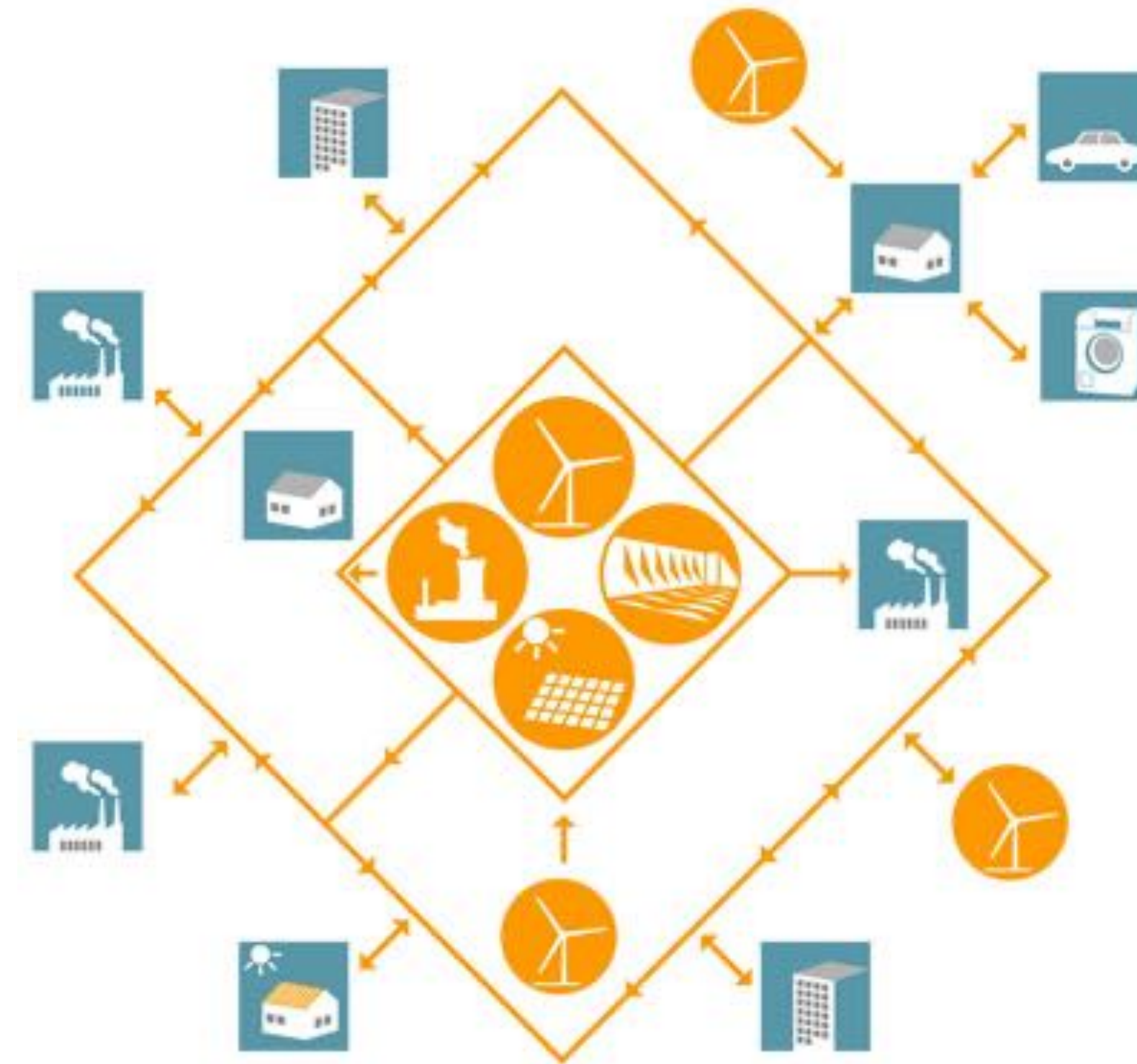
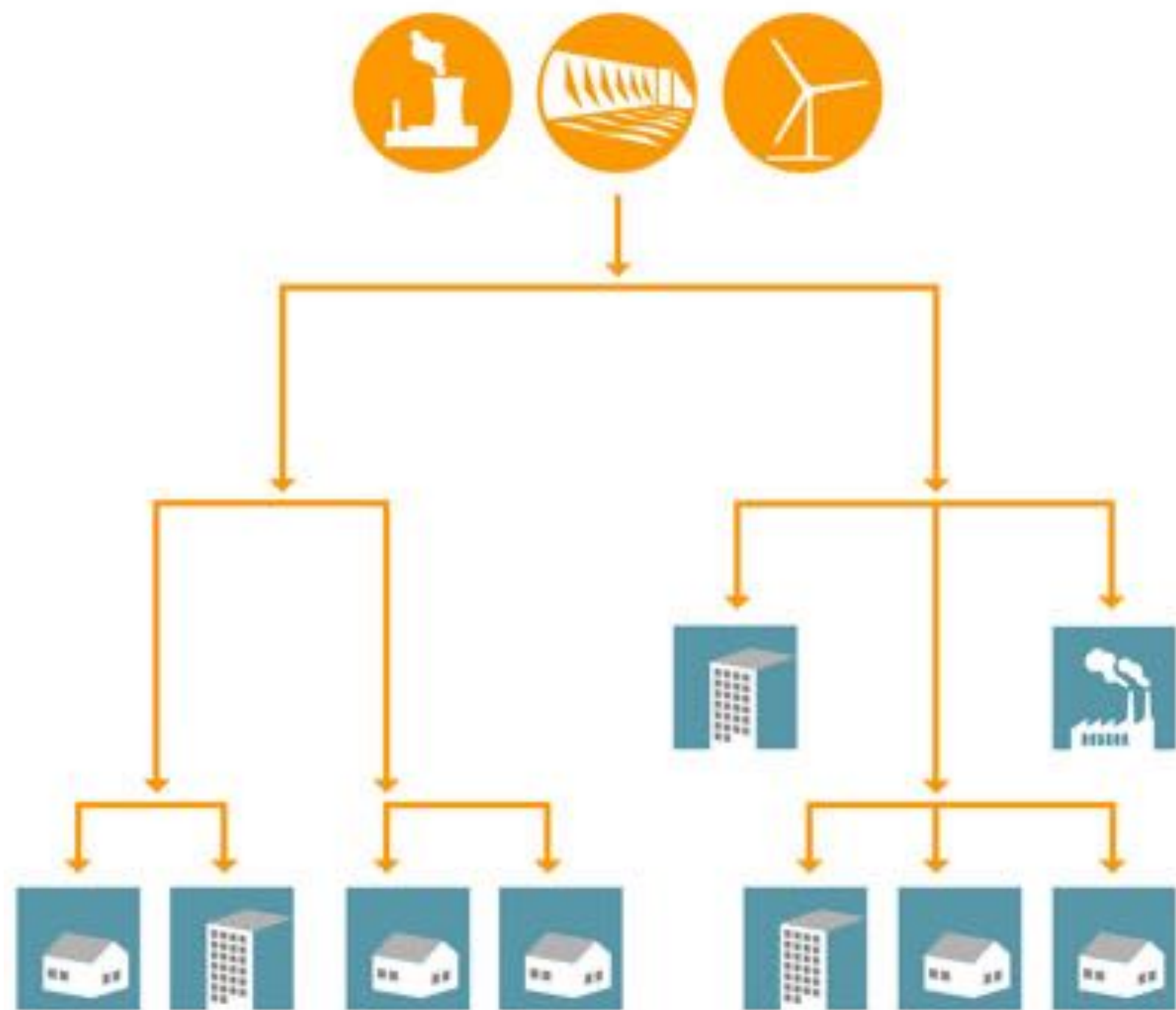


Figure from Statnett's development plan 2019



Electric grid – contd.

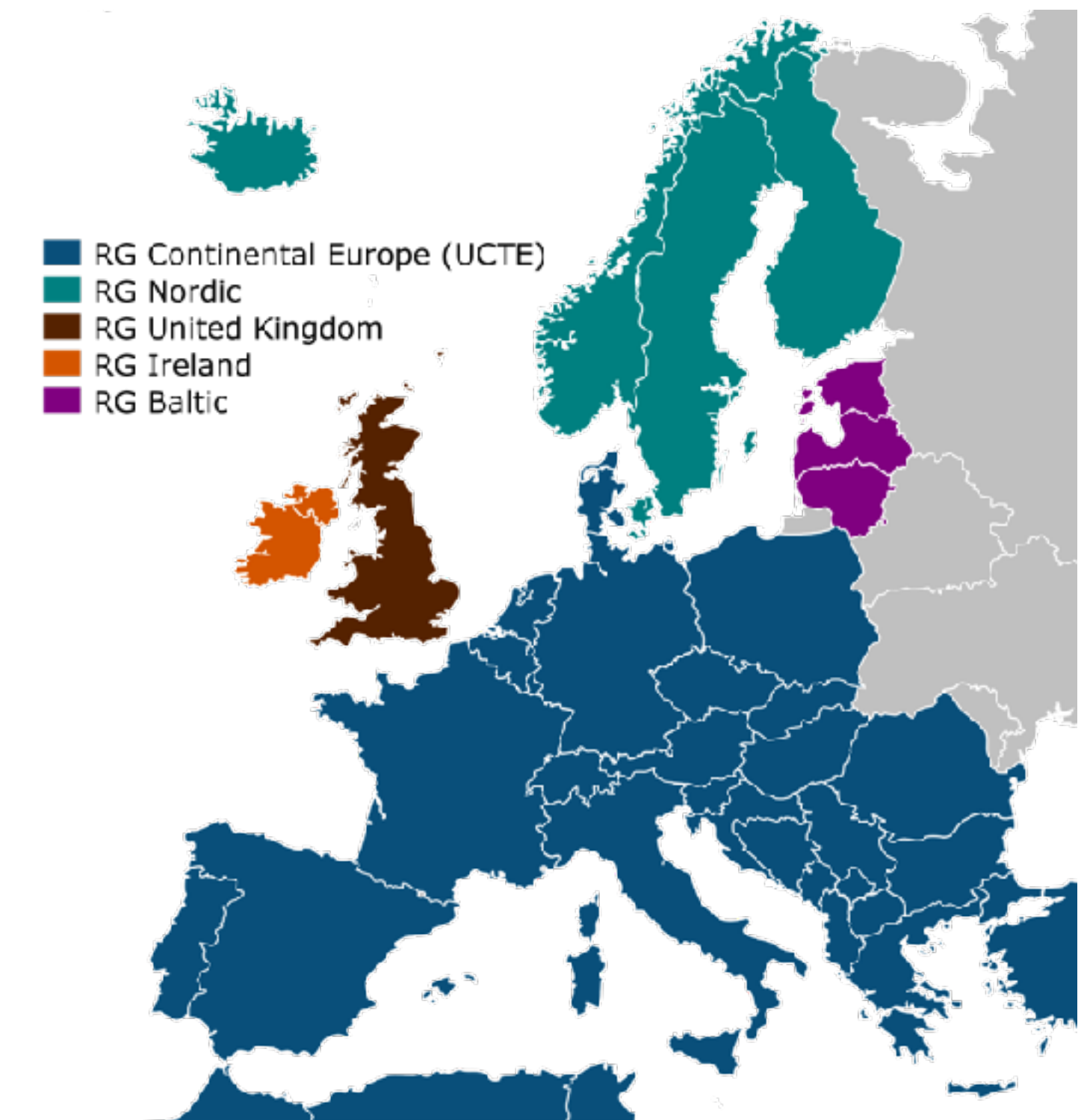
- traditional electric grid vs. smart grid, figure from ABB



Electric grid challenges

- Change in generator/consumer balance
- Lack of investments to cover consumption peaks in production
- Lack of investments to cover peaks in distribution
- Most smart-grid scenarios focus on consumers

- Early solutions include:
 - ➔ secondary power circuits for controlled use («night tariff»),
 - ➔ not accepting generation from consumers, but allowing local use,
 - ➔ quick-reaction power plants,
 - ➔ continentwide power system-interconnections



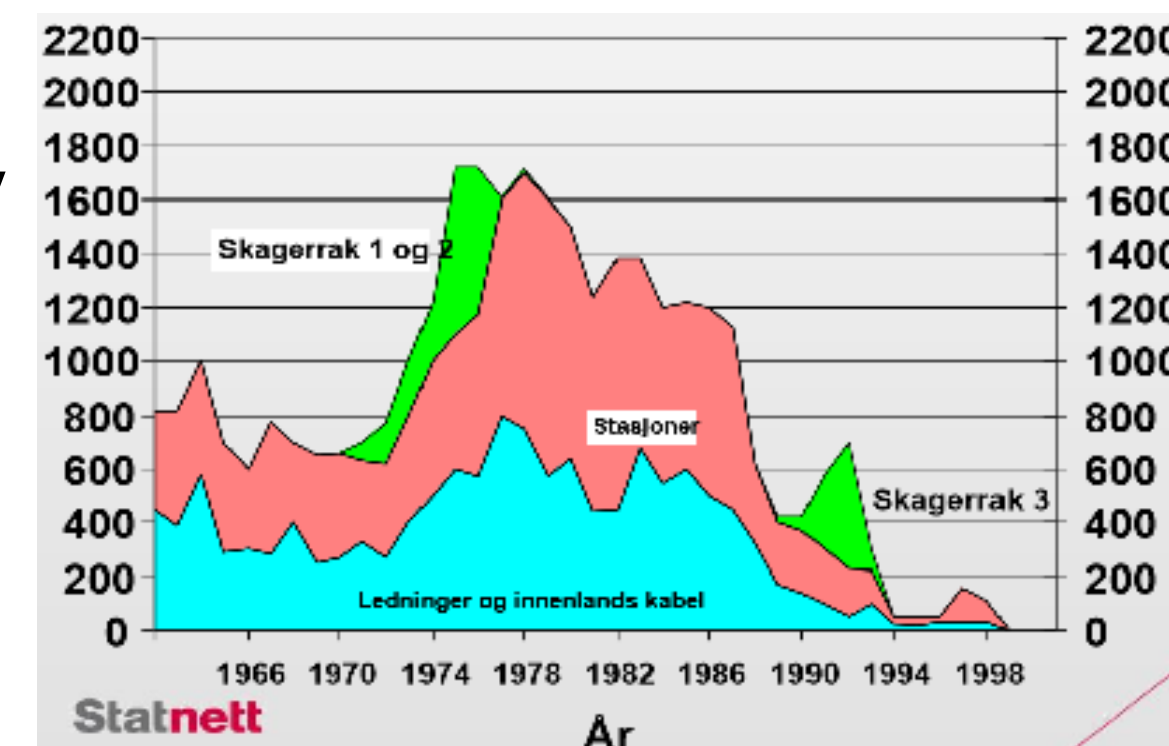
Smart Grid

- Applications of smart grid:
 - ➔ Demand management, better resource control and utilization
 - ➔ Smart integration of local generation
 - ➔ Data gathering and processing for further enhancements, better forecasting models
 - ➔ Load control
- Electricity as main power source for the society
- Exploit parallels with communication networks



Smart Grid

- Motivation to build a smart grid: save on investments, higher profit rate, better stability, renewables, some cost reduction in employees
- 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

- Actors in the smart grid:
 - ➔ Transmission System Operators (TSOs) e.g. Statnett
 - ➔ Distribution System Operators (DSOs) e.g. Follo Energi
 - ➔ Equipment vendors: both grid and CPE
 - ➔ Elhub
- Cost of power outage (KILE - Kvalitetsjusterte Inntektsrammer ved ikke-Levert Energi)
- Willingness to pay vs length of outage

INDUSTRY	AMOUNT
Cellular communications	\$41,000
Telephone ticket sales	\$72,000
Airline reservation system	\$90,000
Semiconductor manufacturer	\$2,000,000
Credit card operation	\$2,580,000
Brokerage operation	\$6,480,000

Ref: U.S. Department of Energy

Tabell 6 *Kostnaden ved avbrudd øker med varigheten av strømbruddet*

Varighet på avbrudd	Oppvarming av rom	Oppvarming av vann	Elspesifikt forbruk
1 minutt	Ingen endring	Ingen endring	Liten endring
1 time	Noe lavere temperatur for husholdninger uten alternativ oppvarming	Trolig liten endring: Hvorvidt dusjen/oppvasken avhenger av størrelsen på varmtvannstanken	Mister tilgang på alt elektrisk utstyr som ikke er koblet mot batterier (lys, tv, komfyr)
4 timer	Lavere innetemperatur for husholdninger uten alternativ oppvarming	Husholdningen må utsette dusj og oppvask, evt. dusje kortere, vaske opp i mindre varmt vann	Begynner også å miste tilgang til elektrisk utstyr med batteri.
8 timer	Svært lav innetemperatur for boliger med dårlig isolering og uten alternativ oppvarming	Husholdning må utsette dusj og oppvask	Mister tilgang til mesteparten av det elektriske utstyret. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang.
24 timer	Det blir kaldt i de fleste hus uten alternativ oppvarming	Husholdningen kan ikke dusje eller vaske opp	Mister tilgang til alt elektrisk utstyr. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang.
48 timer (2 døgn)	Det blir så kaldt i de fleste hus uten alternativ oppvarming at husholdningen må basere seg på substitutter (innkjøp av oppvarmingsutstyr som er uavhengig av elektrisitet eller midlertidig flytte til husrom med oppvarming).	Husholdningen kan ikke dusje eller vaske opp	Mister tilgang til alt elektrisk utstyr. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang, vann- og avløpssystemer fungerer ikke lenger
72 timer (3 døgn)	Det blir så kaldt i de fleste hus uten alternativ oppvarming at husholdningen må basere seg på substitutter (innkjøp av oppvarmingsutstyr som er uavhengig av elektrisitet eller midlertidig flytte til husrom med oppvarming).	Husholdningen kan ikke dusje eller vaske opp. Husholdningen opplever et tap av komfort som følge av at de ikke har vasket seg på 3 døgn. Dersom avbruddet rammer et større område reduseres husholdningens substitusjonsmuligheter da det er lite poeng å finne alternative oppvarmingskilder til vann (har ikke tilgang til vann).	Mister tilgang til alt elektrisk utstyr. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang, vann- og avløpssystemer fungerer ikke lenger
96 timer (4 døgn)	Det blir så kaldt i de fleste hus uten alternativ oppvarming at husholdningen må basere seg på substitutter (innkjøp av oppvarmingsutstyr som er uavhengig av elektrisitet eller midlertidig flytte til husrom med oppvarming).	Husholdningen kan ikke dusje eller vaske opp. Husholdningen opplever et tap av komfort som følge av at de ikke har vasket seg på 4 døgn. Dersom avbruddet rammer et større område reduseres husholdningens substitusjonsmuligheter da det er lite poeng å finne alternative oppvarmingskilder til vann (har ikke tilgang til vann).	Mister tilgang til alt elektrisk utstyr. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang, vann- og avløpssystemer fungerer ikke lenger
120 timer (5 døgn)	Det blir så kaldt i de fleste hus uten alternativ oppvarming at husholdningen må basere seg på substitutter (innkjøp av oppvarmingsutstyr som er uavhengig av elektrisitet eller midlertidig flytte til husrom med oppvarming).	Husholdningen kan ikke dusje eller vaske opp. Husholdningen opplever et tap av komfort som følge av at de ikke har vasket seg på 4 døgn. Dersom avbruddet rammer et større område reduseres husholdningens substitusjonsmuligheter da det er lite poeng å finne alternative oppvarmingskilder til vann (har ikke tilgang til vann).	Mister tilgang til alt elektrisk utstyr. Dersom strømbruddet rammer et større område – tap av mobil- og internetttilgang, vann- og avløpssystemer fungerer ikke lenger



Smart Grid

KILE

Kundegruppe	Kostnadsfunksjon for $k_{p,ref}(t = \text{avbruddsvarighet angitt i timer})$				
	$< 1 \text{ min}$	$\geq 1 \text{ min og } < 1 \text{ timer}$	$\geq 1 \text{ timer og } < 4 \text{ timer}$	$\geq 4 \text{ timer og } < 8 \text{ timer}$	$\geq 8 \text{ timer}$
Jordbruk	$5+14.3*t$	$5+14.3*t$	$19+15.6*(t-1)$	$66+14.3*(t-4)$	$66+14.3*(t-4)$
Husholdning	$1,1+9,8*t$	$1,1+9,8*t$	$1,1+9,8*t$	$1,1+9,8*t$	$1,1+9,8*t$
Industri	34	$34+84.7 * t$	$118+82.3*(t-1)$	$365+55.6*(t-4)$	$588+36.5*(t-8)$
Handel og tjenester	16	$28 + 168.3*t$	$196+91.1*(t-1)$	$469+141.3 *(t-4)$	$1034+102.4*(t-8)$
Offentlig virksomhet	7	$60+113.2*t$	$173+27.9*(t-1)$	$257+51.8*(t-4)$	$464+17.6*(t-8)$
Industri med eldrevne prosesser	$49+2.8*t$	$49+2.8*t$	$49+2.8*t$	$91+2.8*t$	$91+2.8*t$

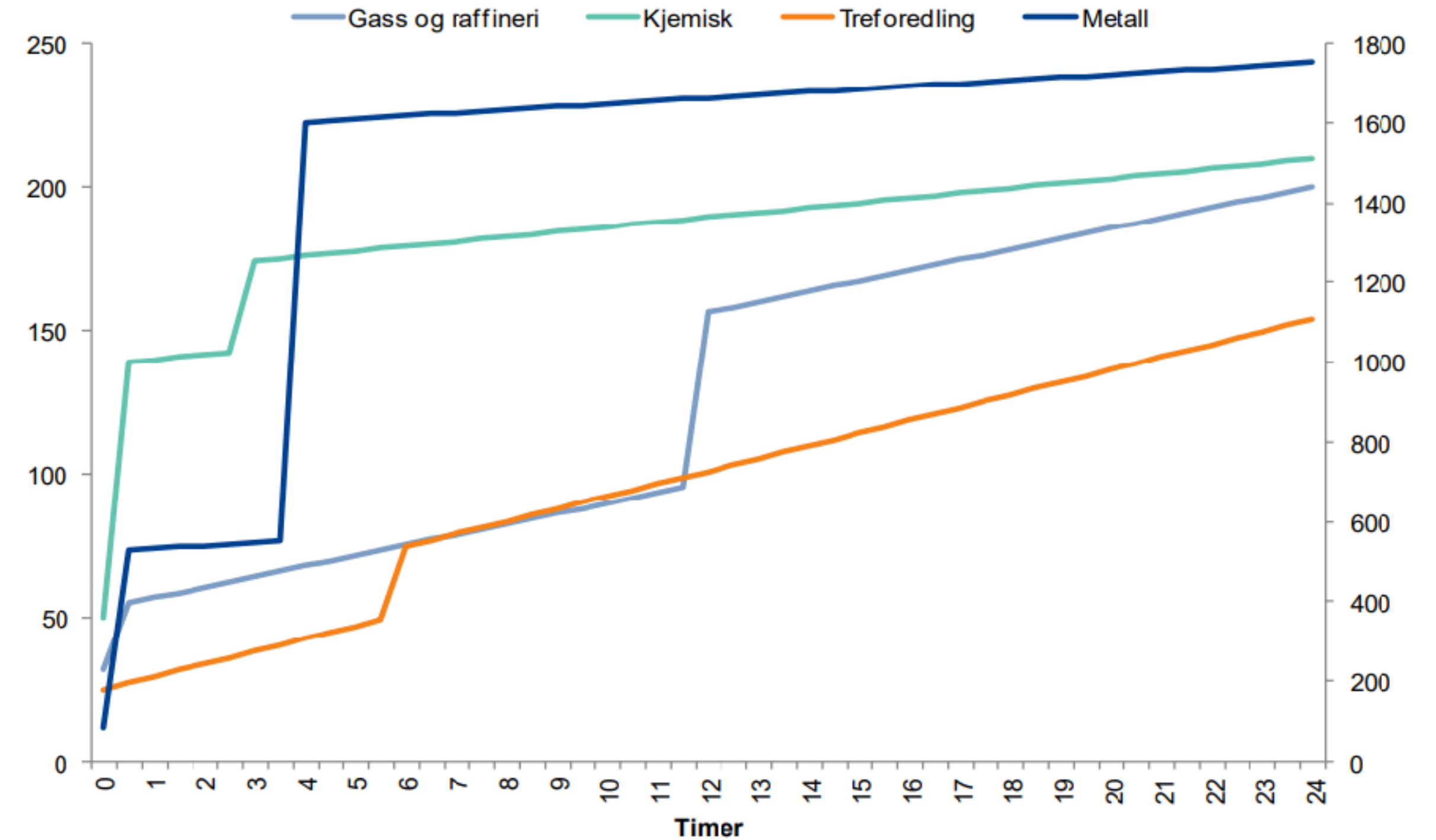
Referansetidspunktene for de respektive kundegruppene er:

Jordbruk	Husholdning	Industri	Handel og tjenester	Offentlig virksomhet	Industri med eldrevne prosesser
Torsdag i januar kl. 06:00	Hverdag i januar kl. 16:00	Hverdag i januar kl. 10:00	Hverdag i januar kl. 10:00	Hverdag i januar kl. 10:00	Hverdag i januar kl. 10:00

http://publikasjoner.nve.no/rapport/2013/rapport2013_76.pdf

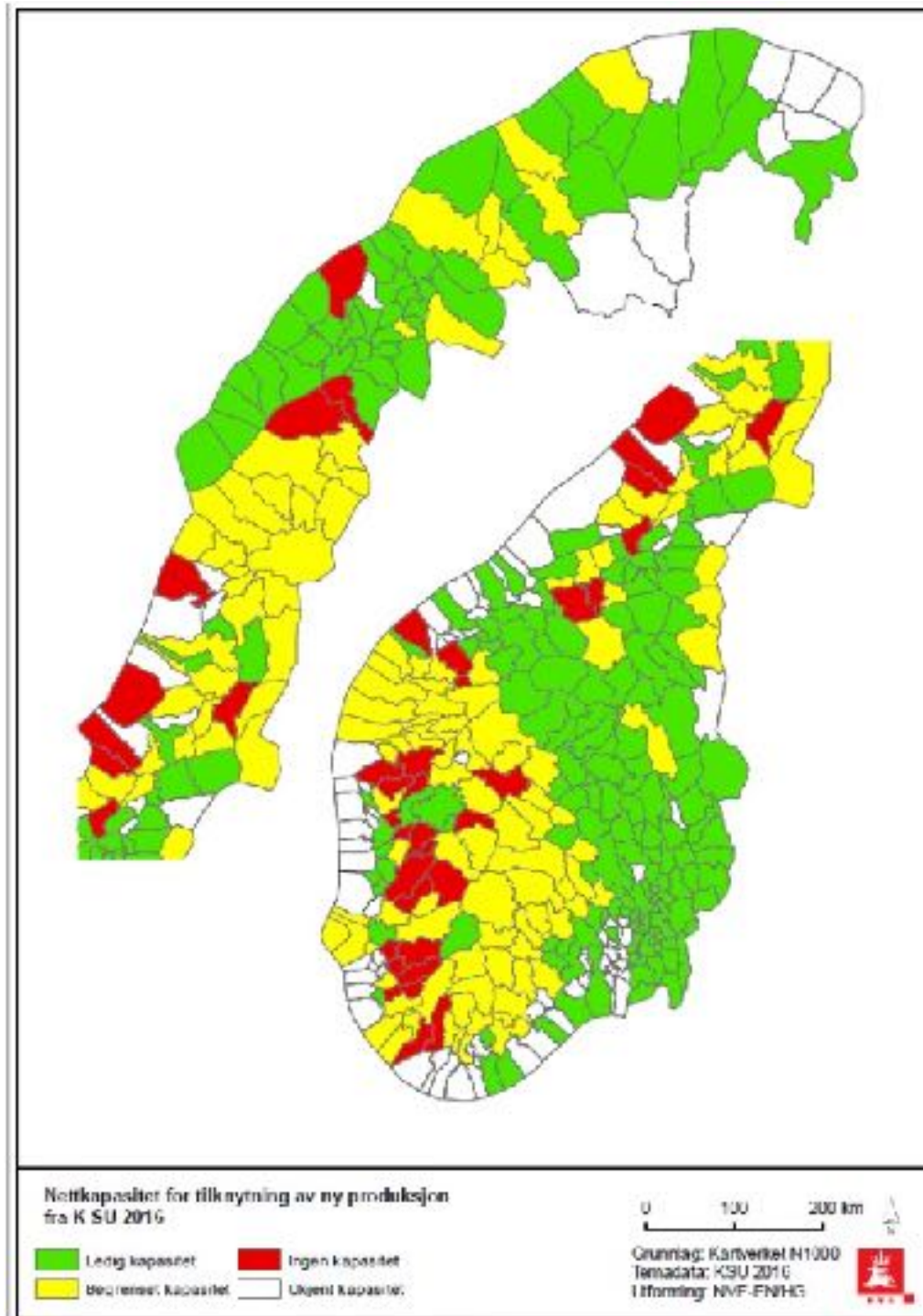
Figur A

Estimerte kostnadsfunksjoner for avbrudd som funksjon av antall timer avbruddet varer. kr/kW



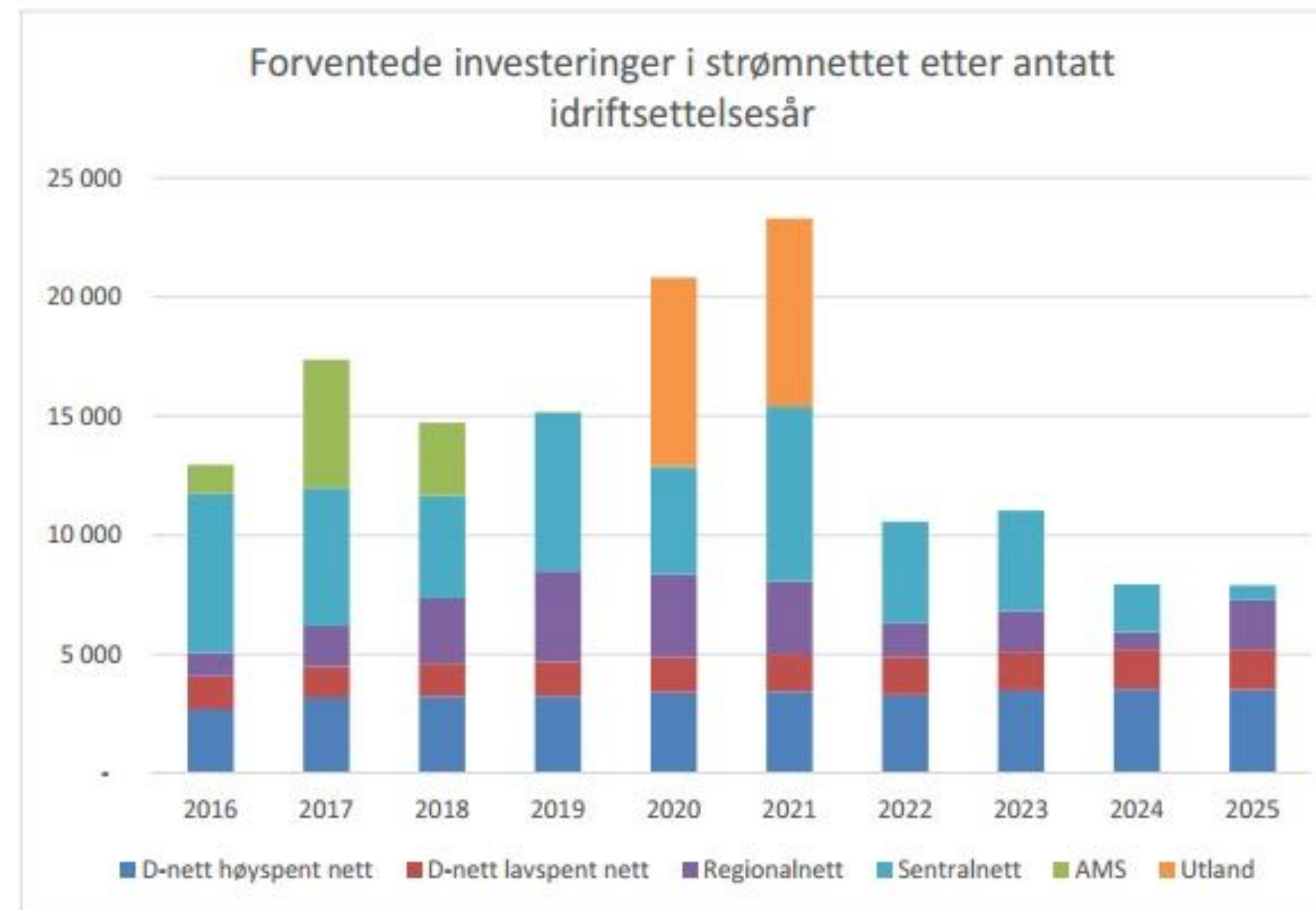
https://www.nve.no/Media/3197/350_2012-bedrifter-med-eldrevne-prosesser.pdf

Figures from NVE and Statnett

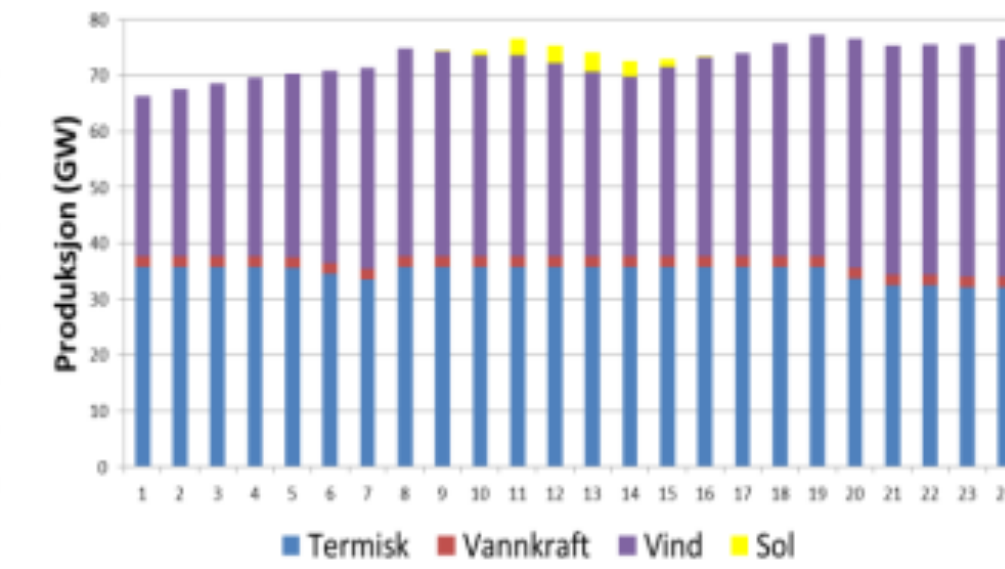
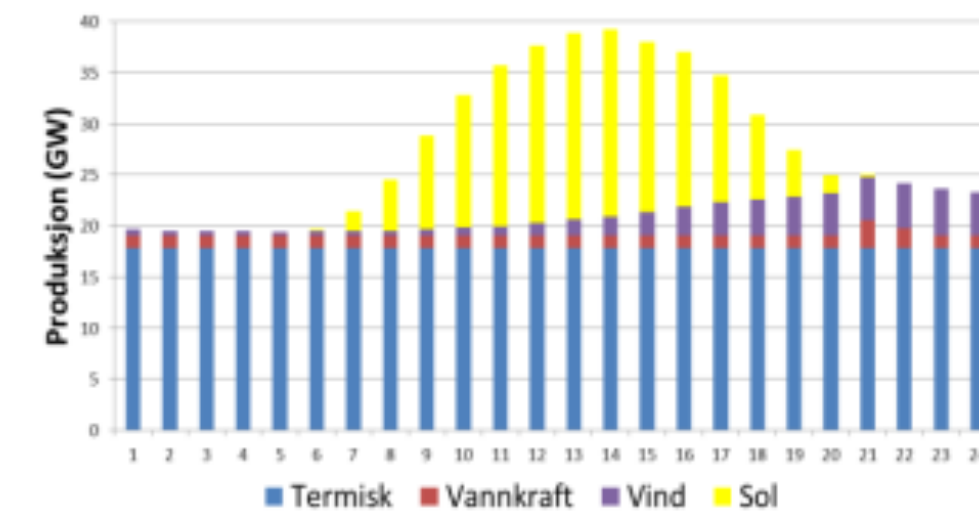


6.5 Totale forventede investeringer i nettet

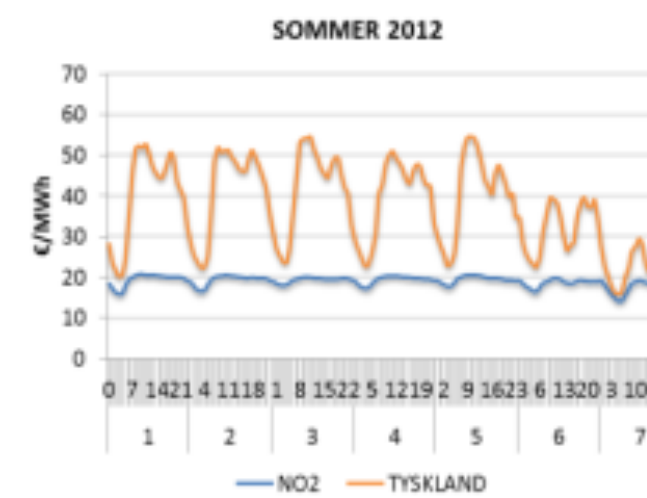
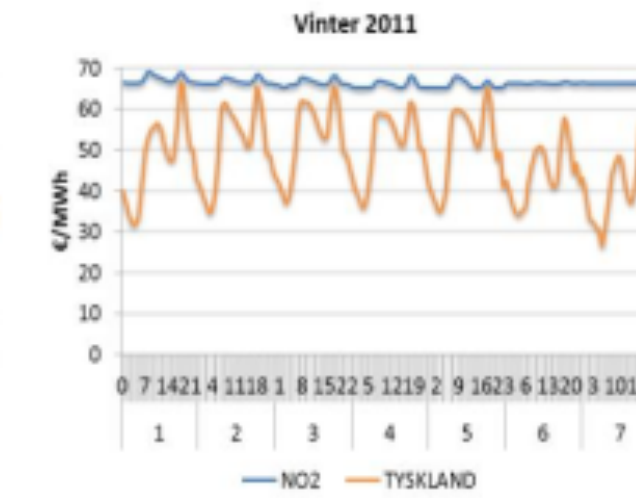
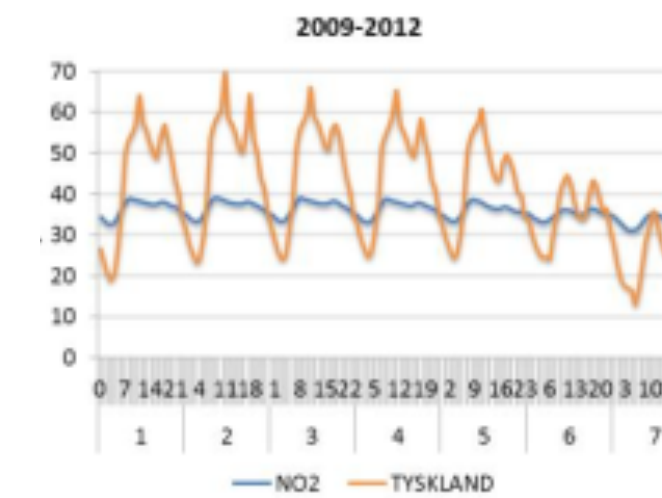
Figur 22 sammenstiller Figur 13, Figur 18 og Figur 21 for å gi et bilde av alle forventede investeringer i kraftnettet de neste ti årene.



Figur 22 Totale investeringskostnader i Norges strømmnett etter idriftsettelsesår.



Figur 44: Døgnproduksjon for en sommerdag til venstre og vinterdag til høyre. Solkraft dekker mye av forbruket om sommeren.



Figur 4 Prisene i en representativuke for hele perioden 2009-12, vinteren 2011 og sommeren 2012.



Statnett's network-development plan 2019

- Published on 1st of October, 2019
- Investment budget of 4-6 mrd kr, to drive further electrification of the society
- Aim for balanced development, including:
 - HV distribution
 - Upgrades towards large cities, regions with high population
 - Transformation capacity between high and medium voltage
- Explore possibilities on grid upgrade based on today's 420kV lines or HVDC
- <https://www.statnett.no/for-aktorer-i-kraftbransjen/planer-og-analyser/publiserte-rapporter-og-utredninger/>



Figure from Statnett's transport channel analysis 2019-2040



Smart Grid – contd.

- Technological points:
 - ➔ Network control has continuous 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

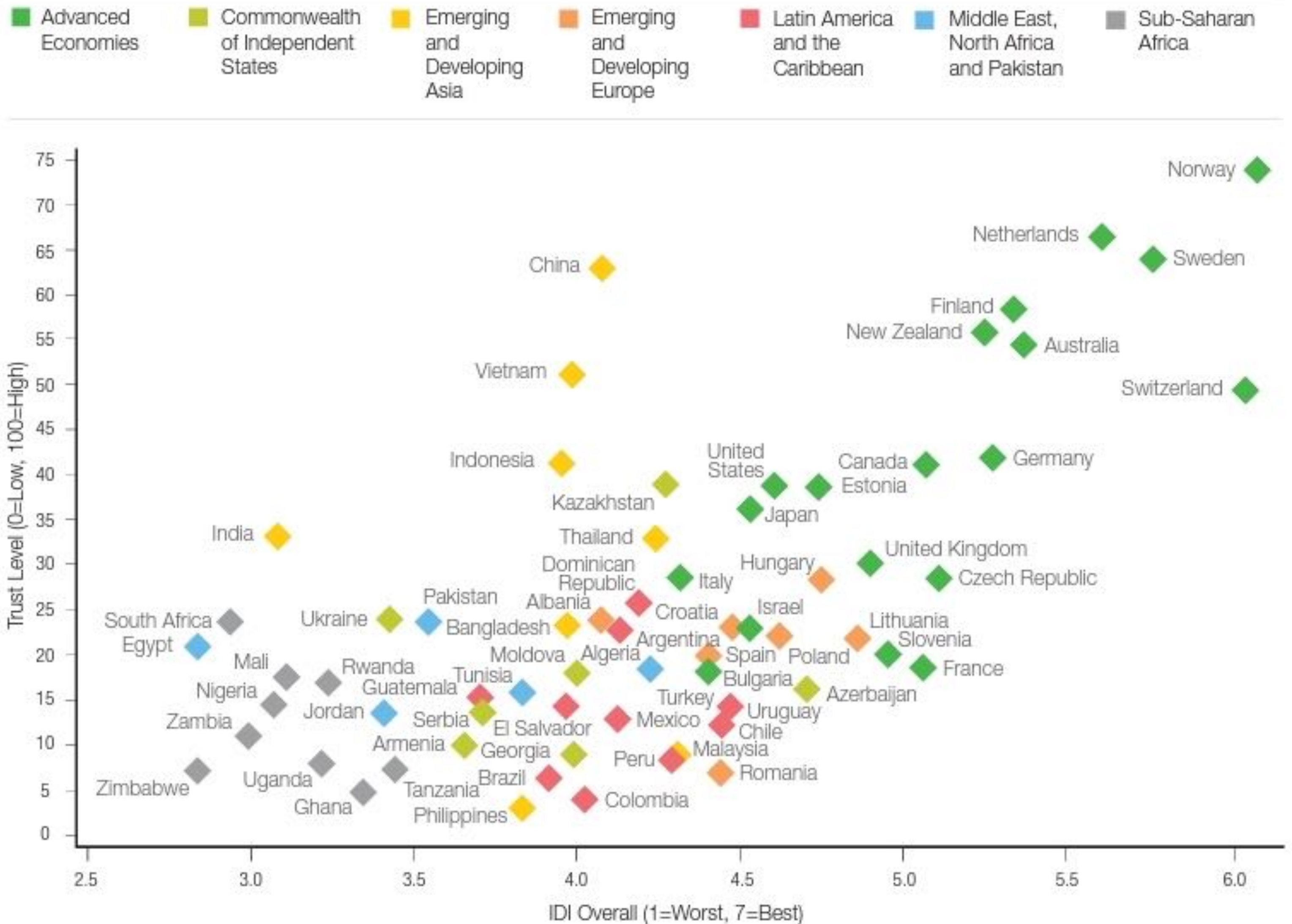
- History: smart metering was present for big consumers since more than a decade, power factor corr.
- Now moving to the household, required by law (in Norway)
- Adds new possibility for load control: consumer (AMS), generation, big consumers, energy storage
 - Operations central (at grid control) [load 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?
 - Privacy of customer?
 - Health-Safety-Environment



Trust and Privacy in Smart Grids

- Goal: An innovative society with trust

Figure 4: Inclusive Development Performance and Interpersonal Trust

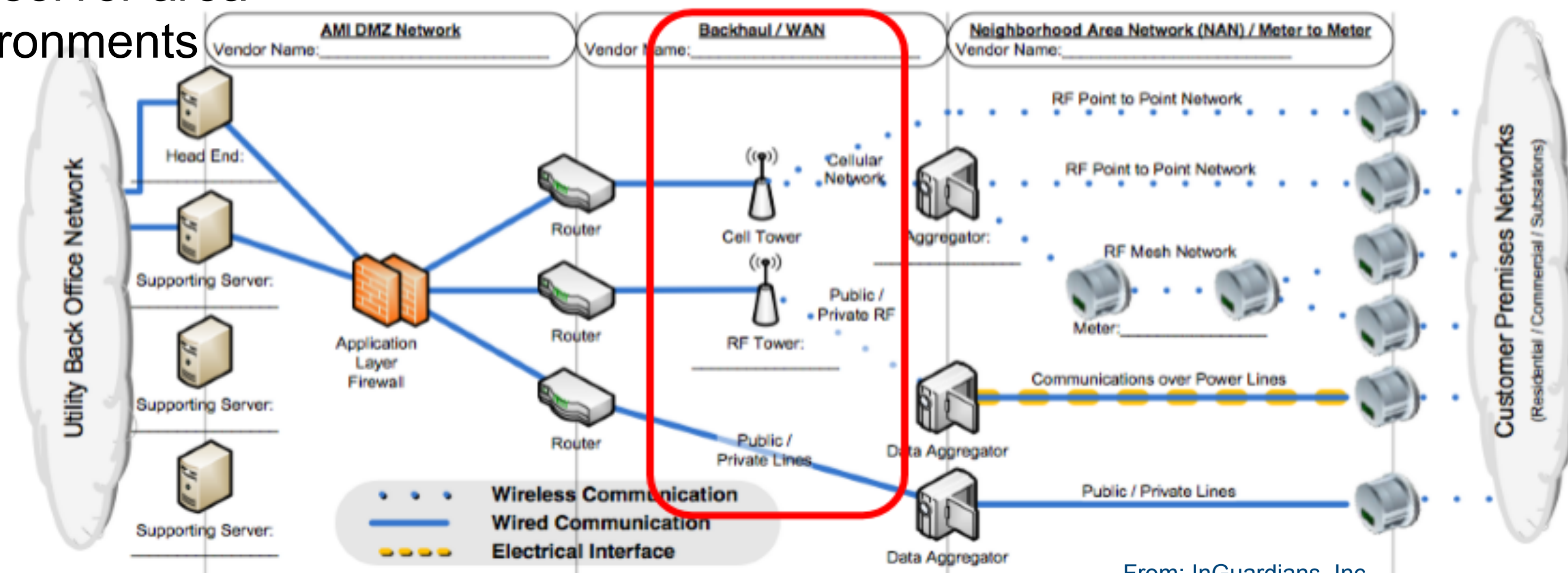
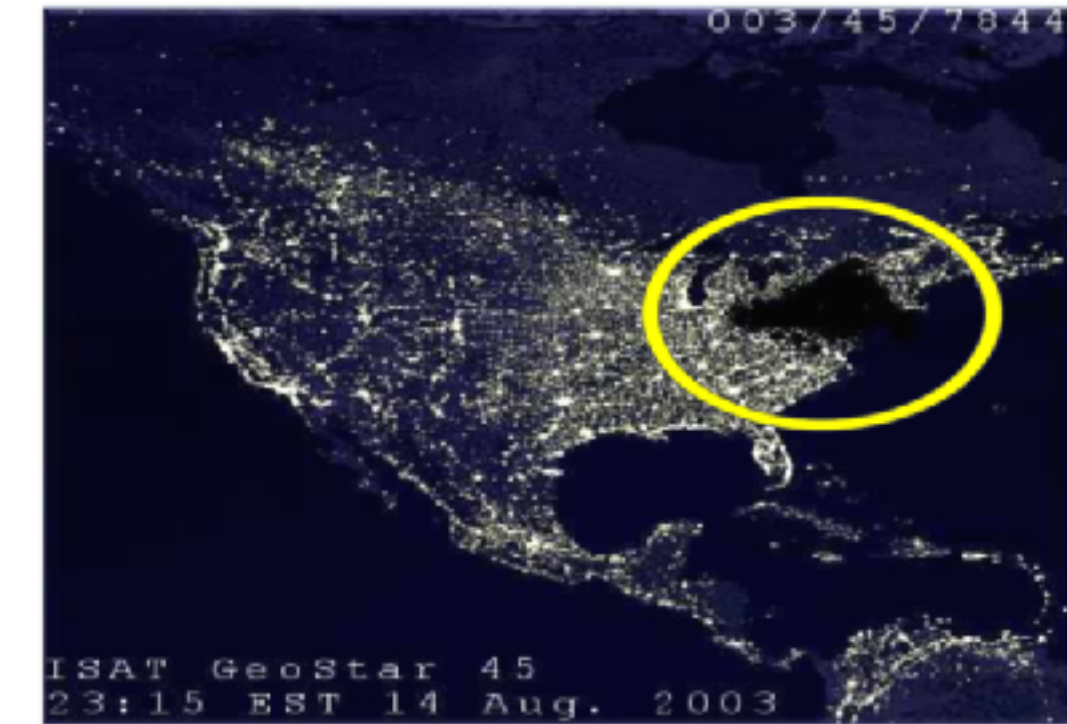


Sources: World Values Survey (2014), World Economic Forum



Advanced Metering Systems – Network security

- Utility and consumer can't trust each other
- 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 – 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



A SHODAN kamstrup  Explore Enterprise Access Contact Us

Exploits Maps

TOP COUNTRIES

South Africa	1
Sweden	1
France	1
Denmark	1


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: Cherokee/0.99.9 (UNIX)
Location: https://78.79.193.77/
X-Powered-By: PHP/5.6.17
Set-Cookie:
Ex...
```


166.159.88.107

107.159.159-00.myvzw.com
Verizon Wireless
Added on 2018-02-03 12:03:56 GMT
 United States
[Details](#)

```
0:22:27:2b:21m0[00]0[0]1:1H0[2]5h
RuggedSwitch Operating System v3.9.1 (May 18 2011 09:20)
Copyright (c) RuggedCom, 2006 - All rights reserved
```


System Name: CCV 81 /78
Local In: Local In
Contact: Contact
Pin

166.130.140.13

mobile.130.140.130.13.myatt.net
AT&T Wireless
Added on 2018-02-02 00:10:04 GMT
 United States
[Details](#)

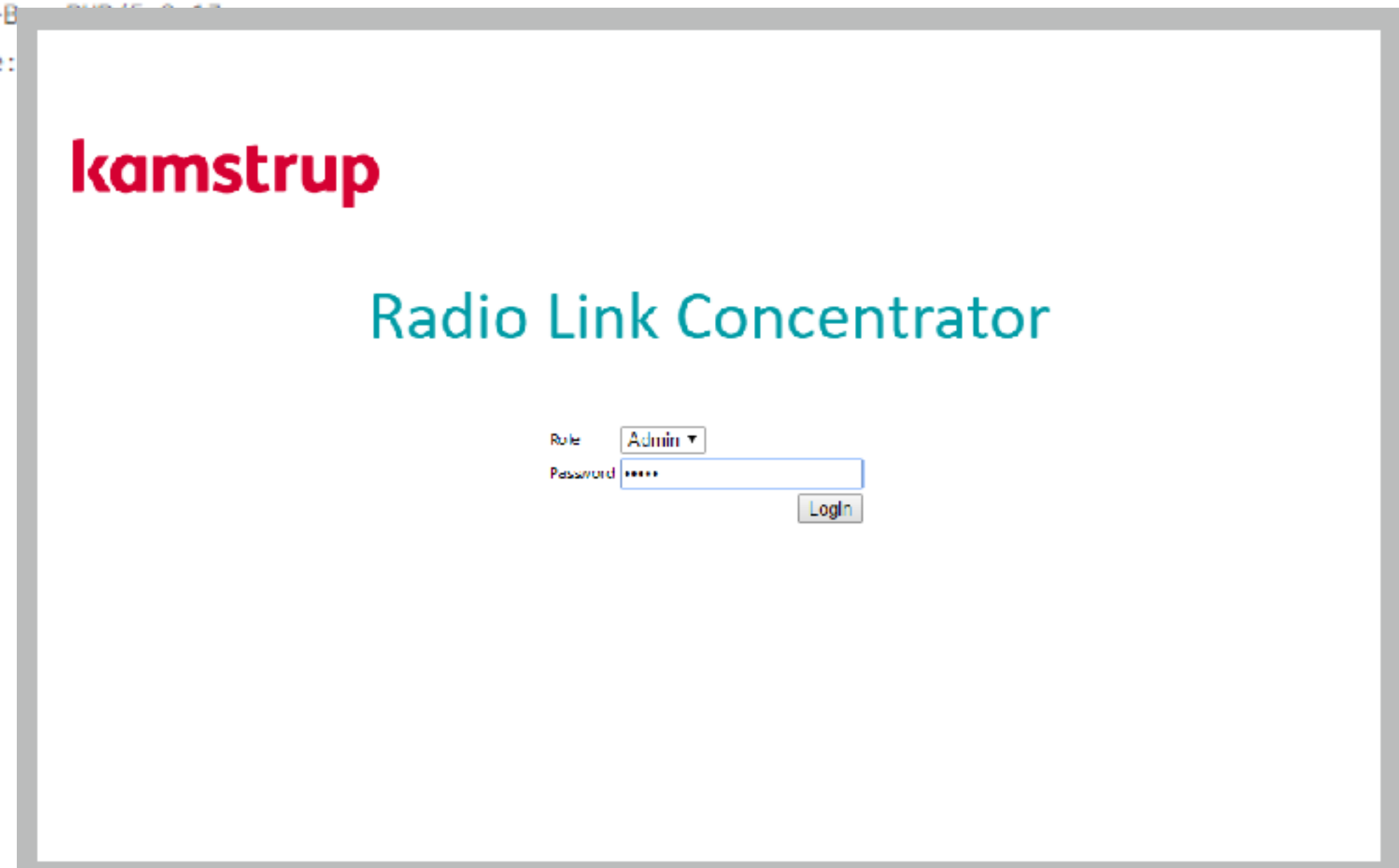
RuggedCom R31510

63.120.127.26

Georgia Public Web
Added on 2018-02-02 00:10:51 GMT
 United States, Sandersville
[Details](#)

```
0:22:27:2b:21m0[00]0[0]1:1H0[2]5h
RuggedSwitch Operating System v3.9.1
Copyright (c) RuggedCom, 2006 - All rights reserved
```

System Name: Cherokee
Local In: SYNCHRONOUS #1
Contact: Kelly McQuigg (718-252-7001)



The screenshot shows a web interface for 'kamstrup Radio Link Concentrator'. The title 'kamstrup' is in red, and 'Radio Link Concentrator' is in teal. Below the title, there is a login form with a 'Role' dropdown menu set to 'Admin', a 'Password' field with masked characters, and a 'Login' button.



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

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 Kam 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

[More Alerts](#)

SHODAN BINOM3

Exploits Maps

TOP COUNTRIES

Total results: 1
213.170.71.188
 Quantum CJSC
 Added on 2017-02-01 04:40:20 GMT
 Russian Federation, Saint Petersburg
[Details](#)

Universal multifunctional electric power quality meter BINOM3

BINOM3

MULTIFUNCTIONAL REVENUE ENERGY METER AND POWER QUALITY ANALYZER



Serial number S/N: 10000034

Authorization

Login:

Password:

Введите, пожалуйста, логин и пароль.

Login

More IT in the electric grid vs Quality of Service

- ◉ Ref. to KILE-rules -- Quality of Service is also impacted by the IT systems
- ◉ Evolution of communication networks
- ◉ Best effort is the most efficient and is dominating in virtually all segments
- ◉ Typical communication with at least one human party tolerates very much

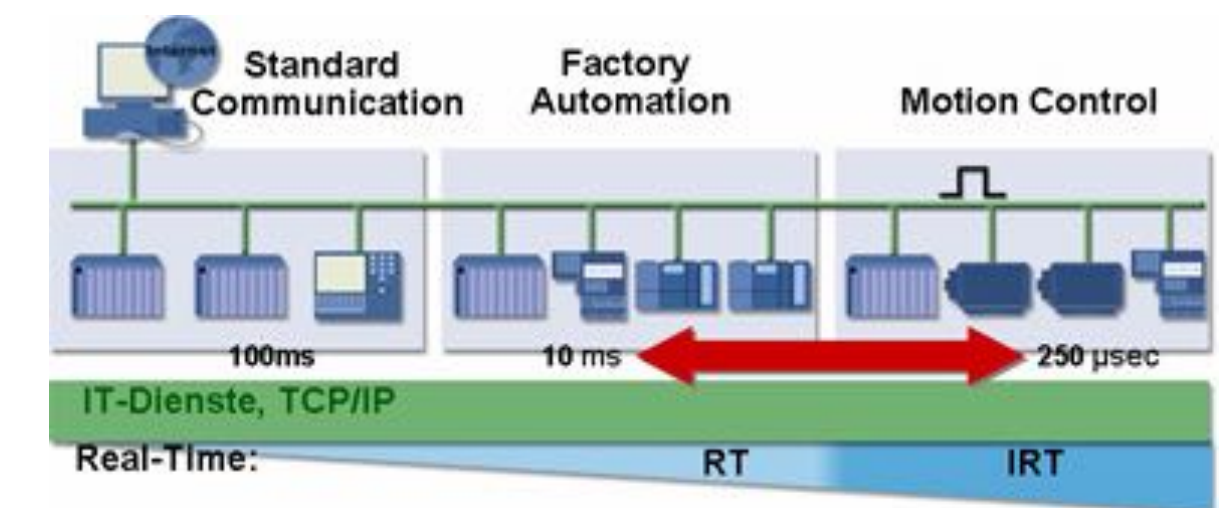
- ◉ Automation: has requirements because of the physical relation

- ◉ QoS for the control loop
- ◉ QoS over the internet



Intrinsic QoS

- Taking the most problematic part of the automation QoS
 - E.g. Profinet IRT or EtherCAT
- Relaxed QoS
 - Supervisory Control and Data Acquisition
 - Remote management
- High QoS
 - Electric grid
 - Electrified production platforms



Identifying QoS metrics in automation

Conversion of requirements:

- ➔ Delay, jitter: this is the same
- ➔ But: frequency, number of samples
- ➔ Communication overhead

The bay units send to the central unit the following information:

- the current values of each phase sampled with 1 ms time intervals
- presence or absence of the three phase voltages
- the status of bus disconnecting switches of the bay using two bit status signals
- starting command for the bay breaker failure protection
- trip signals

The central unit sends to the bay units the following information:

- synchronizing signal with 1 ms time intervals
- trip command, when protection activates

Parameter	Value	Type	Unit	Min	Max
Interval Time VerySlow	8000	dint	ms	60	864C
Interval Time Slow	4000	dint	ms	60	864C
Interval Time Normal	2000	dint	ms	60	864C
Interval Time Fast	1000	dint	ms	60	864C
Interval Time VeryFast	500	dint	ms	60	864C
CV VerySlow 1131 Task timeout before ISP	24000	dint	ms	60	864C
CV Slow 1131 Task timeout before ISP	12000	dint	ms	60	864C
CV Normal 1131 Task timeout before ISP	6000	dint	ms	60	864C
CV Fast 1131 Task timeout before ISP	3000	dint	ms	60	864C
CV VeryFast 1131 Task timeout before ISP	1500	dint	ms	60	864C
Protocol	MMS	string			150

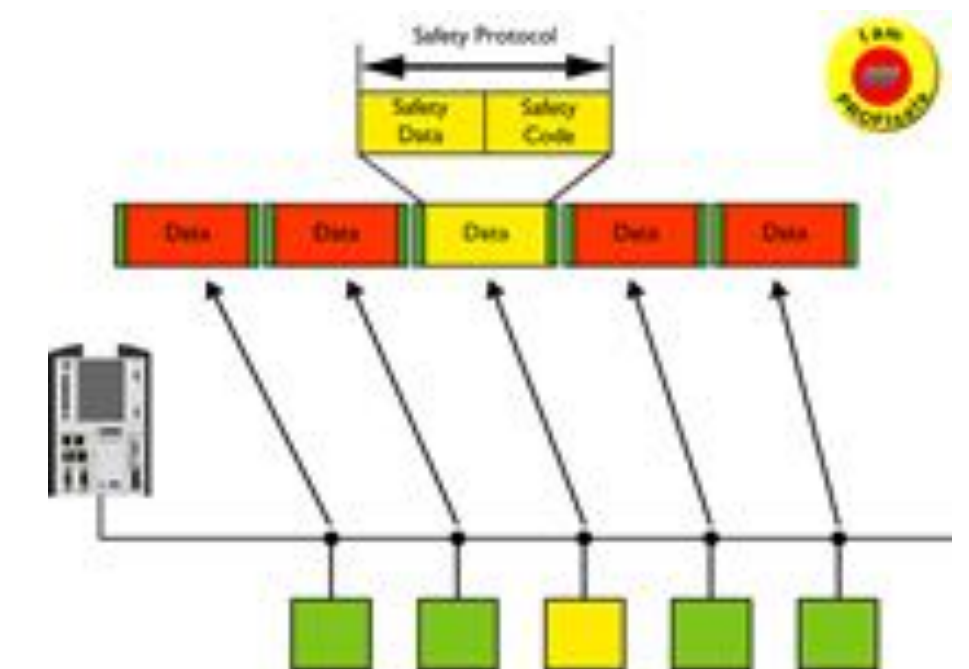
Applications	Source IED	IEC 61850 Message Type	SCN Traffic Type	Destination IED	Sampling Frequency (Hz)	Packet Size (Bytes)
Sampled value data	MU IED	4	Raw data message	Protection IEDs	4800 Hz	126
Protection	Protection IED	1, 1A	GOOSE trip signal	CB_IEDs	—	50
Controls		3	Control signals	Protection IED, CB_IED	10 Hz	200
File transfer		5	Background traffic	Station server	1 Hz	300 KB
Status updates	Protection IED CB_IED	2	Status signals	Station server	20 Hz	200
Interlocks	Protection IED	1, 1A	GOOSE signal	CB_IEDs	—	200

<http://www.tandfonline.com/doi/pdf/10.1080/23317000.2015.1043475>



Safety integrated systems

- Imagine as yellow envelopes mixed into the traffic
- Requires software and might require hardware extensions
- The safety function is not depending on QoS!
- Safety levels: SIL 2, 3 and 4
- Until approx. SIL 3, a normal, RSTP-redundant LAN is sufficient



Safety and security

- Connected because security threats are resulting in safety threats, which have to be mitigated
- Different fields but approaching similar problems
- The process behind is completely different: safety deals with a static statistical process, while security problems are the result of an active, changing process

- Stopping somebody to do something to avoid damage
- Even if something has happened, avoid or limit damage

- Cyber-physical interactions
- IT security is not covering this field
- Safety is focusing on the physical interactions
- Safety is using extensive diagnostics to check itself
- Timescale of protection and data validity



Expected outcome

- Overview on electric grid in a national and international perspective
- What makes an electric grid smart
- Challenges and motivations for building a smart grid
- What incentives are presented for the consumer
- Security, privacy and safety dimensions

