Risk Analysis for Smart Grids

György Kálmán, Ph.D., gyorgy.kalman@ntnu.no

Critical Infrastructure Protection Group, CCIS
mnemonic AS

Trondheim – Gjøvik – Ålesund

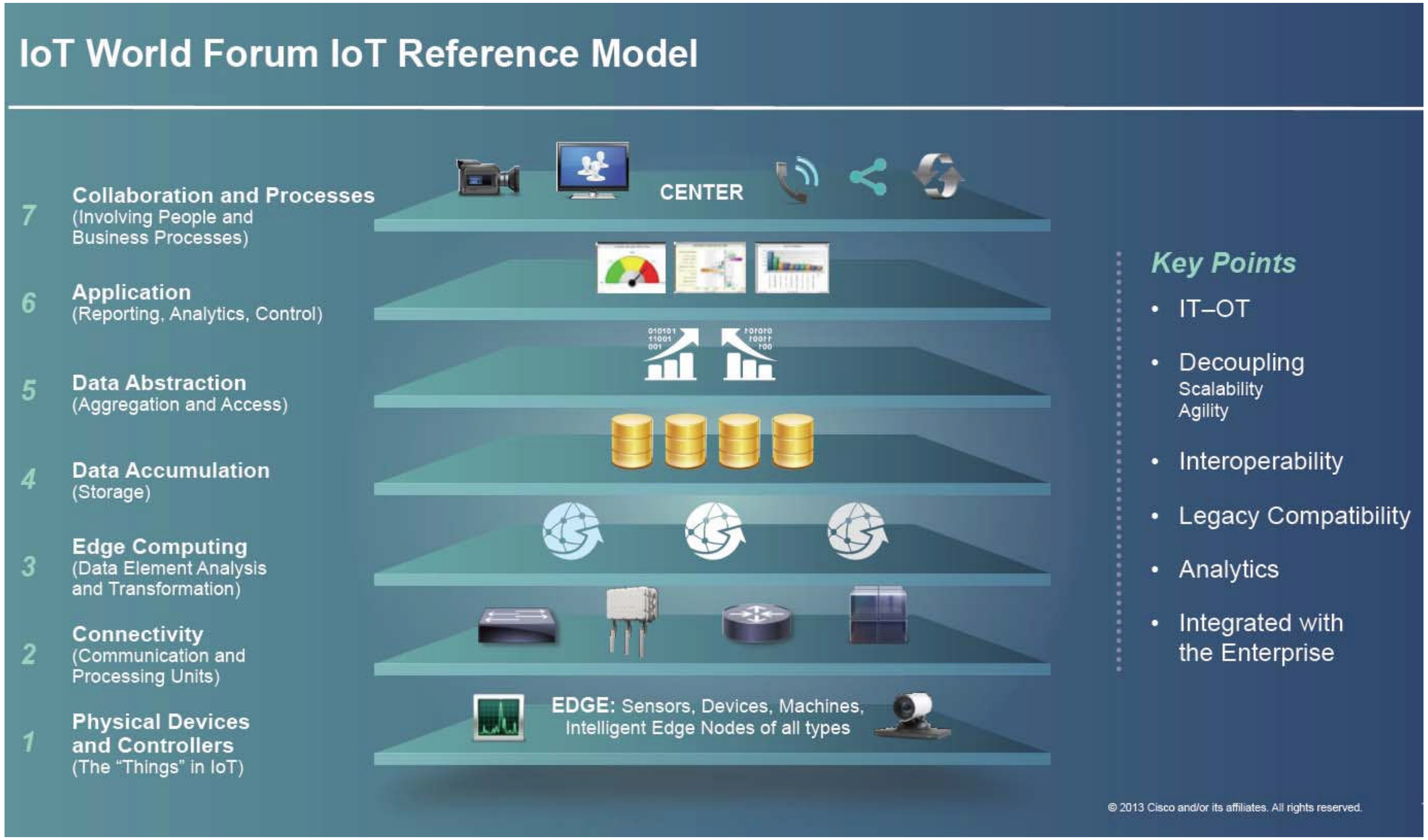
NTNU

Agenda

- Internet of Things
- Overview of the power grid
- Smart grid: motivation, differences
- Risk sources, attack surface
- Physical and cyber security
- Smart metering
- Conclusion

Internet of Things

- Heading toward a fully connected world
- In a more focused way, in this course we speak about industrial internet of things
- The substantial difference is, that these systems have a physical dimension
- Considered as the next industrial revolution
- Automation to a new connectivity level – the internet is coming to automation
- Main challenges: how to join the physical and the logical world, how to achieve interoperability in a heterogenous and conservative industry?


IoT World Forum IoT Reference Model
7
Collaboration and Processes
(Involving People and Business Processes)
6
Application
(Reporting, Analytics, Control)
5
Data Abstraction
(Aggregation and Access)
4
Data Accumulation
(Storage)
3
Edge Computing
(Data Element Analysis and Transformation)
2
Connectivity
(Communication and Processing Units)
1
Physical Devices and Controllers
(The "Things" in IoT)
CENTER
EDGE: Sensors, Devices, Machines, Intelligent Edge Nodes of all types
Key Points
• IT–OT
• Decoupling
Scalability
Agility
• Interoperability
• Legacy Compatibility
• Analytics
• Integrated with the Enterprise
© 2013 Cisco and/or its affiliates. All rights reserved.

Internet as we know it

- Intelligence in the end nodes
- Best effort traffic
- Infrastructure = network equipment
- Operated by IT or telecom
- No direct physical dimension
- Mostly built to serve human-generated traffic
- QoS: best effort, adopted to the human consumer: 10s of ms of drop is not a problem, stable delay is accepted, majority of applications are bursty
- Reaction time in 0.5-1s range
- Stochastic → services do exploit this (like Erlang-B formula for capacity estimation or lossy compression in nearly everything)

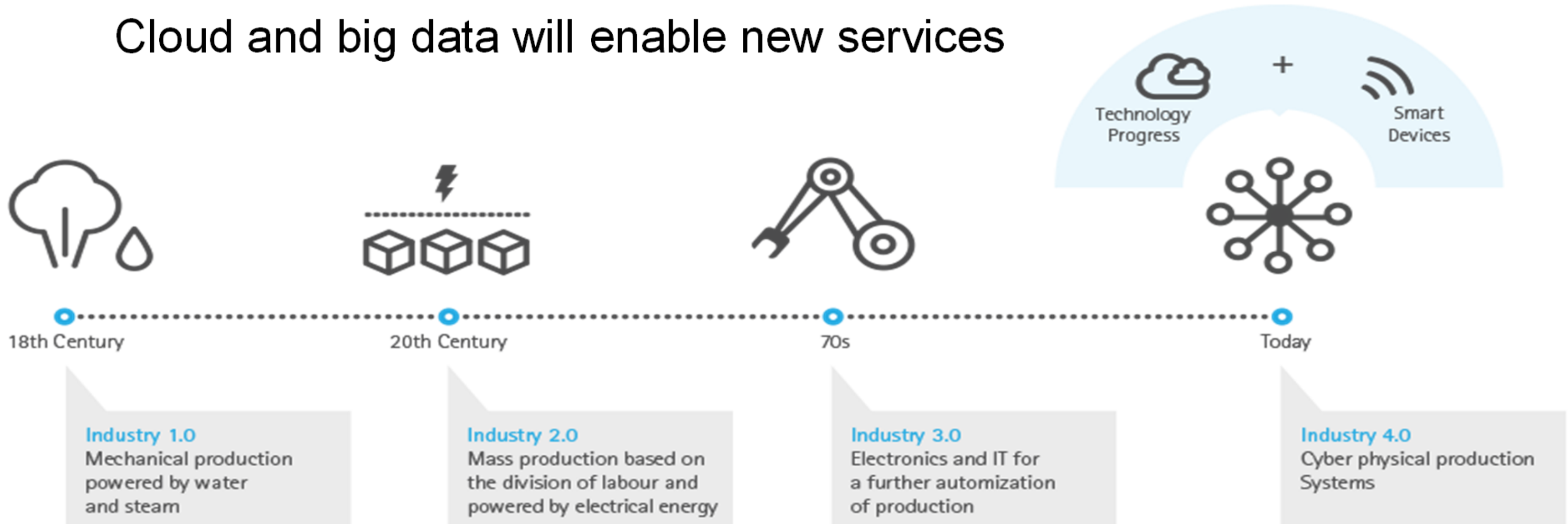
Automation as we know it

- Centralized intelligence
- Traditionally operated as islands by operations
- Direct connection with the physical world
- Is made for information gathering and processing by machines
- Has a lag of approx. 15-20 years (one generation of devices)
- Still a current question: collisions on Ethernet, what happens if one has to share infrastructure with others, how to operate a link with long step-out distance
- Economic press leads to adoption of internet-based services which *require* a paradigm change

ABB robots

Merging this two

- ”dissolves” the automation system in the internet
- Network communication gets physical impact
- Automation meets real internet-type deployment
- Already happening
- The real value of IoT: data.
  Cloud and big data will enable new services



http://prd.accenture.com/microsites/digital-industry/images/digital/industrial-infographic-large.png

The power grid

- Nation/continent-wide critical infrastructure
- Reaches in practice every home and installation
- Was always kind of smart, the difference is in:
  - Resolution and timeliness of data
  - Use of IT
  - Ratio between consumers and producers
- Motivation to build a smart grid:
  save on investments, higher profit rate,
  better stability, renewables, some cost reduction
- Possible new services based on acquired data
- Synchrophasor operations
- Microgrids – possibility for island operation

What’s new with the smart grid

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
- Availability has priority over confidentiality

Attack surface in smart grid

- 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

Security needs of the IoT

- User identification
- Identity management
- Tamper resistance
- Secure storage
- Secure content
- Secure software execution
- Secure communication
- Secure network access

- Gateway as a key customer component: edge device for the LAN, concentrator
- Over-the-air updates

Risk assessment

- risk = probability x impact
- Special with the smart grid:
- long value chain,
- cascading effects: e.g. supporting infrastructure fails because of blackout and blocks reactivation of the grid
- Safety: established methods (fault-tree, Hazard and operability study HAZOP) – by default against natural causes
- Cyber-phyisical risks: the smart grid and the risks associated have a physical dimension – the phyisical process must be part of the eval.
- Legacy systems: see «SCADA» options in security testing software: fragile, not prepared to meet unexpected/malformed data

The (SG)^2 project's risk catalogue

Attacks on the WAN through smart grid gateway

Attacks through remote maintenance access

Cluster / Threat to...	Smart Buildings	E-Mobility	Customer Premises	Low Volt. Gen.	Med. Volt. Gen.	Grid Testpoints	Primary Substation	Secondary Substation	Grid Operation	Metering	*Threat Category Avg.*
Authentication & Authorisation	3,50	4,00	3,00	6,00	6,00	6,25	5,25	8,25	7,00	5,00	5,43
Applied Security Mechanisms	9,50	4,15	7,50	6,40	4,60	4,70	5,05	5,90	7,05	3,00	5,79
Integrity & Availability	2,71	4,46	4,69	4,00	3,13	3,07	3,64	4,72	3,97	4,50	3,89
Internal & ext. Interfaces	2,67	3,50	6,33	6,67	4,00	3,33	5,00	4,00	5,83	2,33	4,37
Confidentiality & Data Protection	5,67	4,67	4,67	8,67	4,33	4,00	3,67	5,63	7,50	3,75	5,25
Maintenance of Equipment	4,43	3,50	4,60	3,75	4,15	3,31	3,94	5,33	5,83	3,60	4,24
Component Cluster Avg.	4,75	4,05	5,13	5,91	4,37	4,11	4,42	5,64	6,20	3,70	

Privacy issues of customer production data

http://energyit.ict.tuwien.ac.at/wp-content/uploads/2014/10/ComForEn14_Langer.pdf

Attack vectors

- Gateway:
  - physical access,
  - authenticated attacks,
  - Unauthenticated attacks,
  - Trivial access
  - Other problems from the fact, that the gateway has at least two interfaces, one LAN and one WAN.

- Security features for embedded devices (more or less true for the whole LAN ecosystem
  - Integrated crypto hardware
  - Firmware protection,
  - Tamper resistance
  - Vertical integration of security functions
  - Trivial access throughout the vertical

A typical industrial device

- A gateway/vpn router:
  - http basic authentication without TLS
  - Cross-side scripting vulnerability on the admin interface
  - Loading scripts from internet
  - Autocomplete for password in web gui
  - Sends all previous passwords in plain text for form in the web gui
  - HTML 5 cross origin resource sharing (opens possibility to circumvent origin checking)
  - Tunneling for serial interface

Attacks

- Computational capabilities and permanent internet connectivity
- Can be used to:
  - Send spam
  - Coordinated attack against e.g. Critical infrastructure
  - Act as server for malware
  - Entry point into an other network (e.g. Corporate)
- Example:
  - Spike botnet: DDoS attacks, ARM platform, infected devices included routers, smart thermostats, dryers, freezers, raspberry pi appliances.
  - Critical infrastructure damage
  - Safety-critical information such as warnings of a broken gas line can go unnoticed

Smart Metering (AMI)

- smart metering is present for big consumers since more than a decade
- Now moving to the household, required by law in Norway and in the EU
- Adds new possibility for load control: consumer, 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]
- Assumes IPv6
- 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?

Smart Metering (AMI) – contd.

- 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 – nothing what a student can't have at home
- 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
- Services (maybe the main point for customer satisfaction):
  - Opens communication with the AMI through the internet
  - Maybe also third party
  - Breaches here _will have_ a physical dimension

Smart Metering (AMI) – contd.

- Potentially millions of devices of same type
- Utility and consumer can’t trust eachother
- Communication policies and configuration – segmentation, firewalling, patching
- Who owns the network?
- How to run an IDS/IPS in this infrastructure?
- How to monitor the whole system?
- Incident handling with heuristics
- Trusted external provider and/or detailed SLAs
- Attack surface again: CLI, webif, remote management, home automation, consumer services, data history
- Vendors form the metering industry: tamper resistance, protocol design, securing communication interfaces are typically not core competence

Conclusion

- Millions of devices with relatively simple communication interfaces
- Risk analysis shall be extended with respect to the whole value chain, the possible phyisical impact and the expected lifetime of the system
- Focus on availability and safety rather than security
- Typical vulnerability testing toolbox fits in most cases
- Tamper resistance seems to focus on the metering function
- Problematic around multi-interface device needs to be solved
- Easy and secure configuration is a challenge
- Regulatory tasks related to privacy protection