TEK5530 - Measurable Security for the Internet of Things

L1 – Introduction

György Kálmán,
UiO
gyorgy.kalman@its.uio.no

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

https://its-wiki.no/wiki/TEK5530, #IoTSec, #IoTSecNO

Overview

- Expectations
- Lecture overview
- Exam
- Topic introduction

Expected outcome:

- Describe application-driven security and establish challenges of sensor-driven systems
- Provide industrial examples, e.g. Smart Grid and automatic meter readings
- Establish application-driven security goals as well as the semantics of your system
- Be able to describe the security impact of components and sub-systems
- Perform a multi-metrics analysis to measure the system security
- Analyse application goal versus system security, be able to describe differences and mitigation solutions
- Be able to analyse and present own thoughts on a scientific paper
- Group work with distribution of workload

TEK5530: Lecture plan

- **16.01**
  - **L1: Introduction (Josef Noll)**
  - **L2: Internet of Things (Gyorgy Kalman)**
- 23.01 (Gyorgy Kalman)
  - L3: Security of IoT + Paper list
  - L4: Smart Grid, Automatic Meter Readings
- 06.02 (Josef Noll)
  - L5: Practical implementation of ontologies
  - L6: Multi-Metrics Method for measurable Security
- 13.02 (Josef Noll)
  - L7: Multi-Metrics Weighting of an AMR sub-system
  - L8: System Security and Privacy analysis
- 20.02 --- Winter holiday
- 27.02 (Josef Noll)
  - L9-10: Paper analysis with 25 min presentation
- 05.03 (Gyorgy Kalman)
  - L11: Service implications on functional requirements
  - L12: Intrusion Detection
- 12.03 (Gyorgy Kalman)
  - L13: Technology mapping
  - L14: Communication and security in current industrial automation
- 19.03 (Gyorgy Kalman)
  - L15: Cloud basics and cloud architecture
  - L16: Cloud security, IoT and service examples from AWS
- 26.03 (Gyorgy Kalman)
  - L17: Selected recent topics from IoT security
  - L18: Wrap-up of the course
- 02.04 ---- No lecture, prepare for exam, consultation possibility
- 09.04 ---- Easter holiday, no lecture
- 16.04 ---- Exam

Department of Technolgy Systems

UiO : Institutt for teknologisystemer
Det matematisk-naturvitenskapelige fakultet

Long and nice history on communications and the birth of internet

Was home of the first ARPANET link to Europe made possible by internet-pioneer Pål Spilling, whom we lost a year ago.

Cooperation with the Kjeller-Institutes

First implementation of OLSR routing protocol

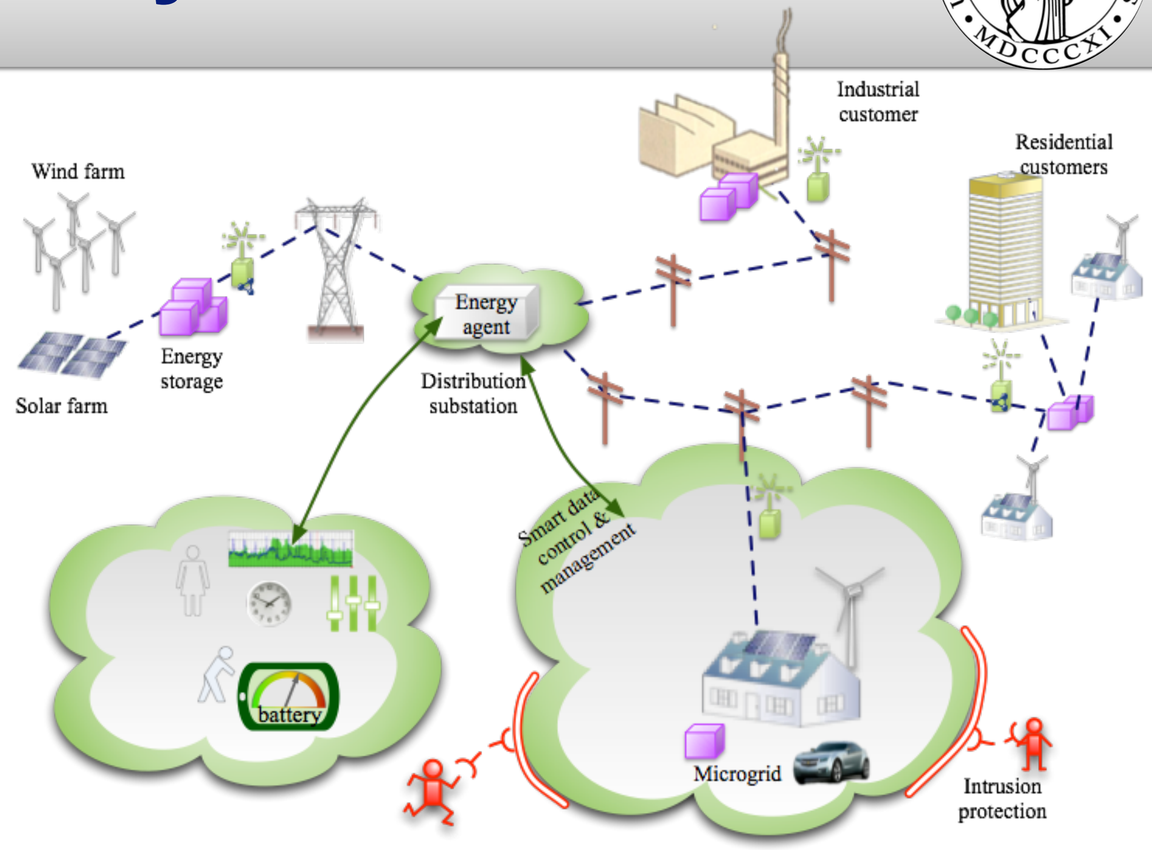
The threat dimension

- Ukraine blackout
- Surveillance camera DDoS
- AMS attack surface
- Exploiting cloud-elasticity
- Smart home – Always online
- Autonomous vehicles
- Ransomware
- Unauthorized resource usage (e.g. mining)

- Worth reading:
  - OWASP Internet of Things project
  https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
  - Amazon Web Services IoT
  https://aws.amazon.com/iot/

L1 - L3: Introduction to security

- This first part will provide the introduction into the Internet of Things (Lecture 1 - L2), with industrial examples
  - Smart Grid and automatic metering system (AMS)
  - Smart Homes with sensors
  - Wireless System upgrade of cars
- Lecture 3 will further address potential security threats, through the example of the smart electricity grid.



- Smart grid with prosumers
- Various control mechanisms
- Attack scenarios
- Critical infrastructure

Internet of Things Security

Energy sector tops list of US industries under cyber attack, says Homeland Security report

12 March, 2015 at 6:38 PM Posted by: Jeremy Cowan

Washington, DC. March 12, 2015 — A report issued today by the US Department for Homeland Security says that in 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents reported by asset owners and industry partners.

The energy sector, says *Jeremy Cowan*, led all others again in 2014 with 79 reported incidents, followed by manufacturing at 65 and worryingly healthcare at 15 reported incidents. ICS-CERT's continuing partnership with the Energy sector reportedly provides many opportunities to share collaborate on incident response efforts.

Power Grid Cyber Attacks Keep the Pentagon Up at Night

A detailed look at why computers running the U.S. electrical infrastructure are so vulnerable to digital threats

By Michael McElfresh and The Conversation | June 8, 2015

The following essay is reprinted with permission from The Conversation, an online publication covering the latest research.

It's very hard to overstate how important the US power grid is to American society and its economy. Every critical infrastructure, from communications to water, is built on it and every important business function from banking to milking cows is completely dependent on it.

Scott Wylie/Flickr

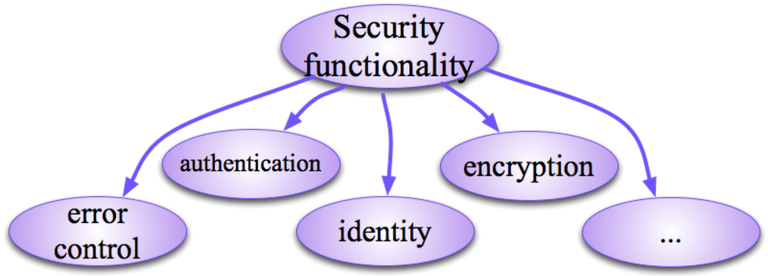
Security and Privacy challenges

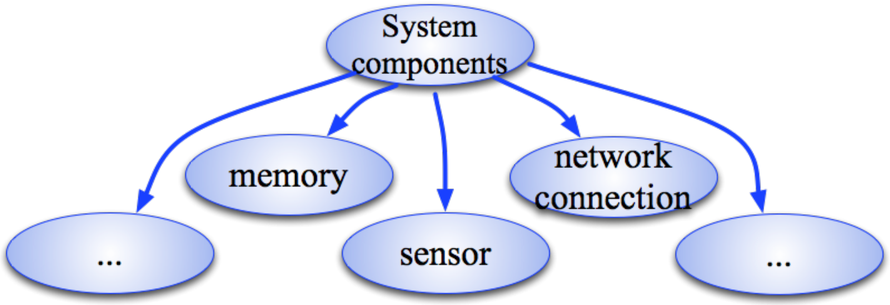
- Example: automatic meter reading (AMR) and -system (AMS) - Insurance
- Mapping from functional requirements towards mapping into technology.
- Example: translation of privacy requirements - can somebody see from my meter reading if I'm at home
- Legislation questions – GDPR and others

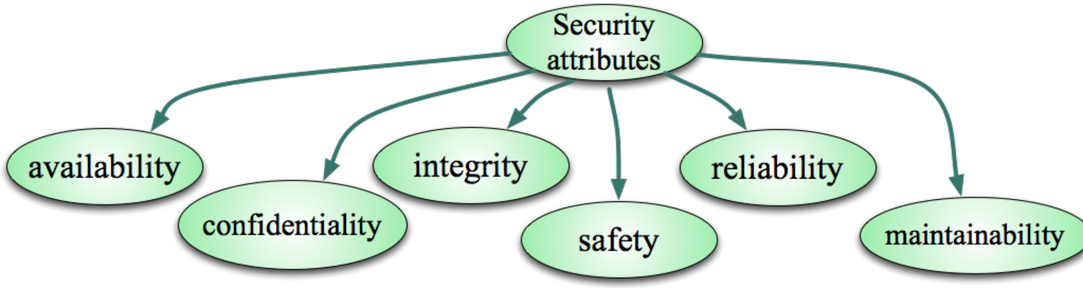
[source: seminarsonly.com]

Machine-readable descriptions

- Describe a system based on security attributes
- Introduction to the Semantic Web
  - Ontologies
- Rules & Reasoning
  - make decisions



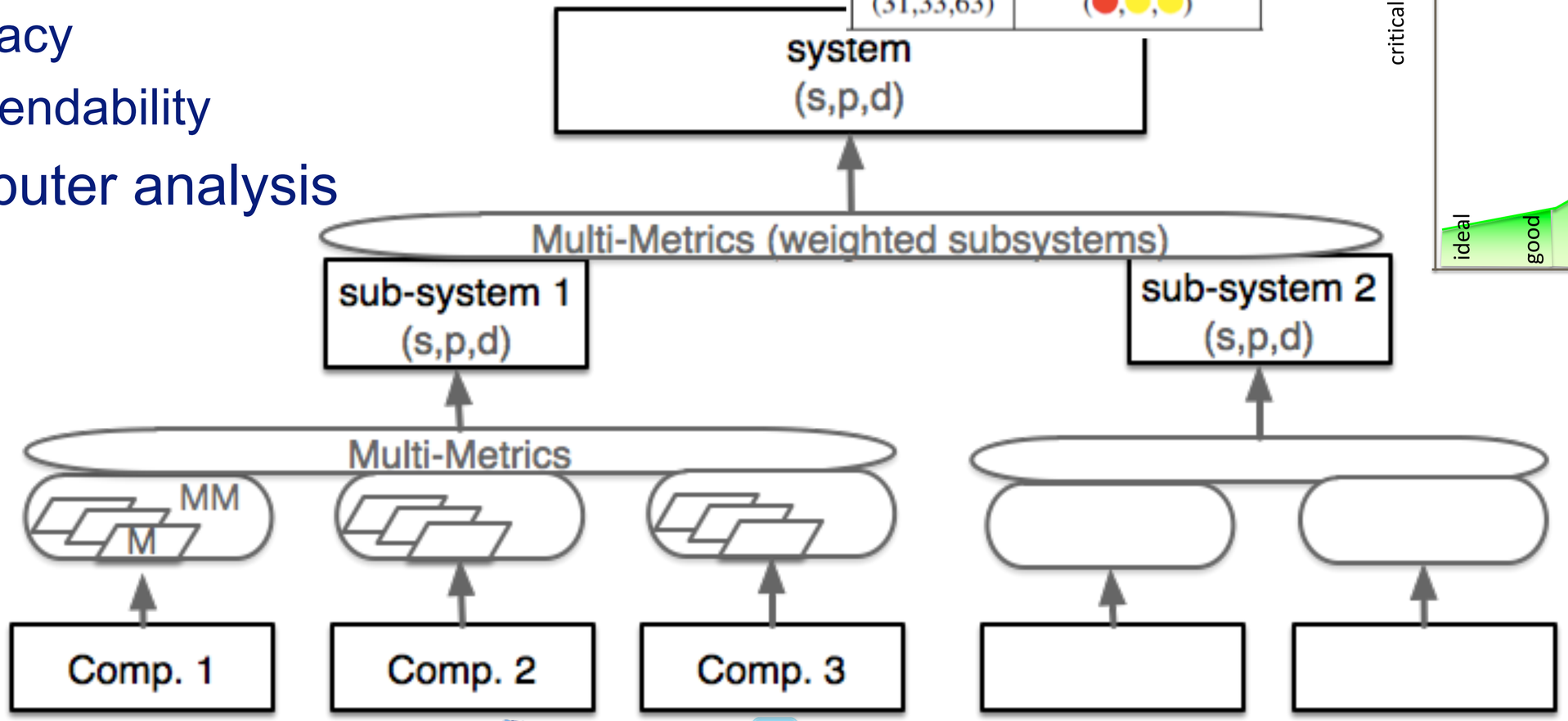


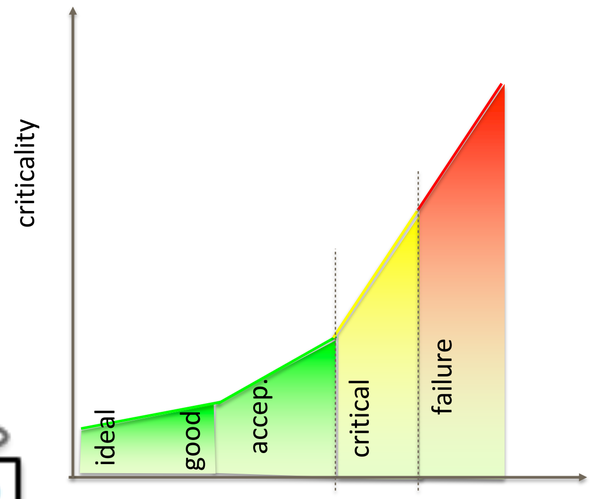


Multi-Metrics method

- System consists of sub-systems consists of components
  - security
  - privacy
  - dependability
- Computer analysis

SPD level	SPD vs SPD_{Goal}
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)





Paper presentation

- Methodology:

  Select (or search) for scientific papers

  Present the paper

  Discuss issues which you find interesting

- Outcome

  Personal:

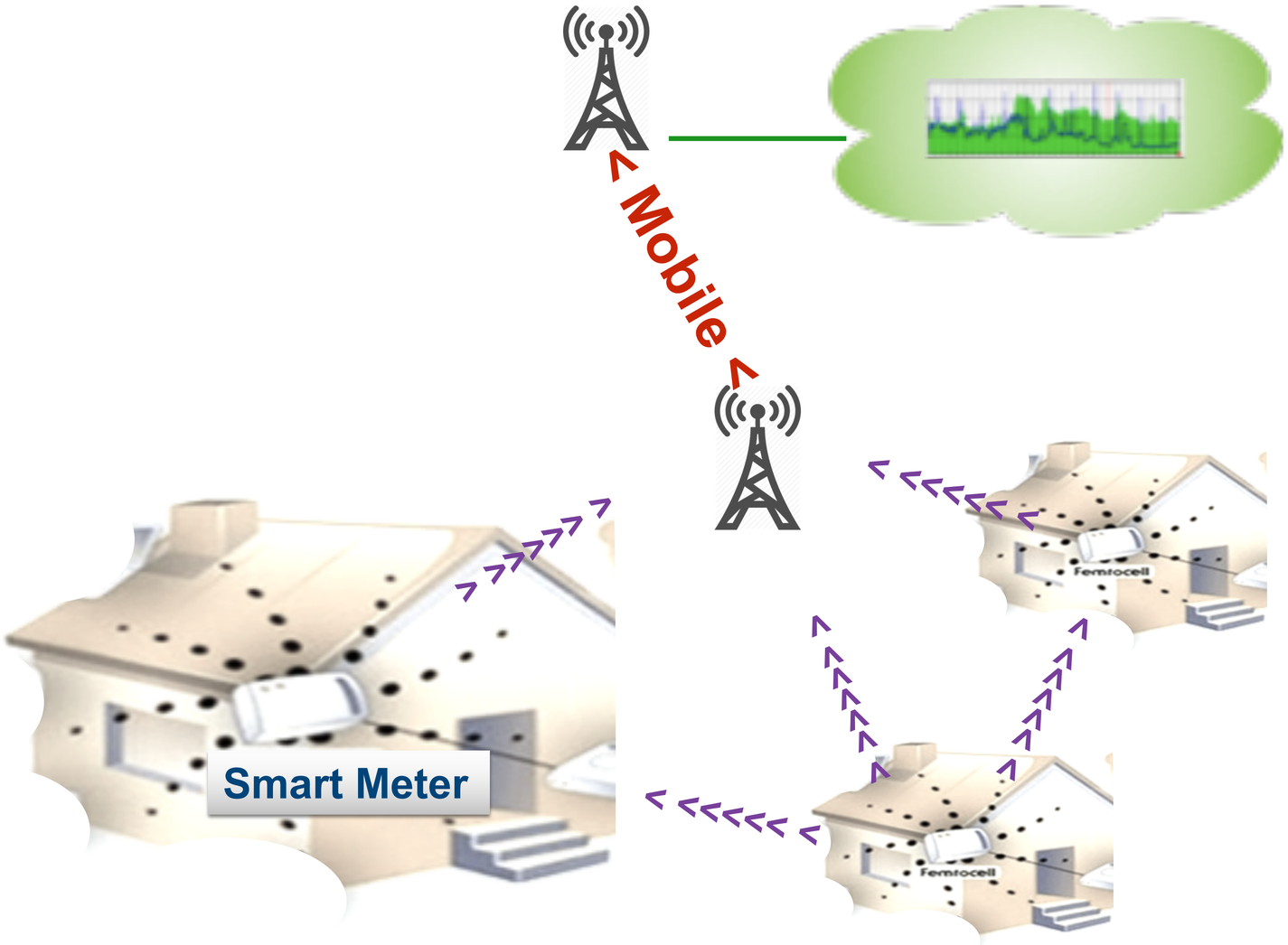
  - Learn to read and present scientific literature with own thoughts
  - Be able to hold a presentation with time limits and active audience

  Course

  - Get a fresh overview of the newest available research challenges and selected surveys of the field of the course
  - Learn from how others are making their presentations
  - Learn to ask questions

Real World Examples

- Real world examples
  - taken from industry, e.g. Smart Meter
  - billing,
  - Controlling
- Service implications on requirements
- Technology mapping
- Intrusion detection
- Communication in automation networks



[source: seminarsonly.com]

Cloud security

- An introduction to cloud and specifically, to AWS
- Cloud security, IoT and IoT support services from AWS

György Kálmán, Josef Noll

Recent news and Wrap-up

- L18: what has happened since we started in January
- L19: Wrap-up, what you can expect on the exam

TEK5530 exam

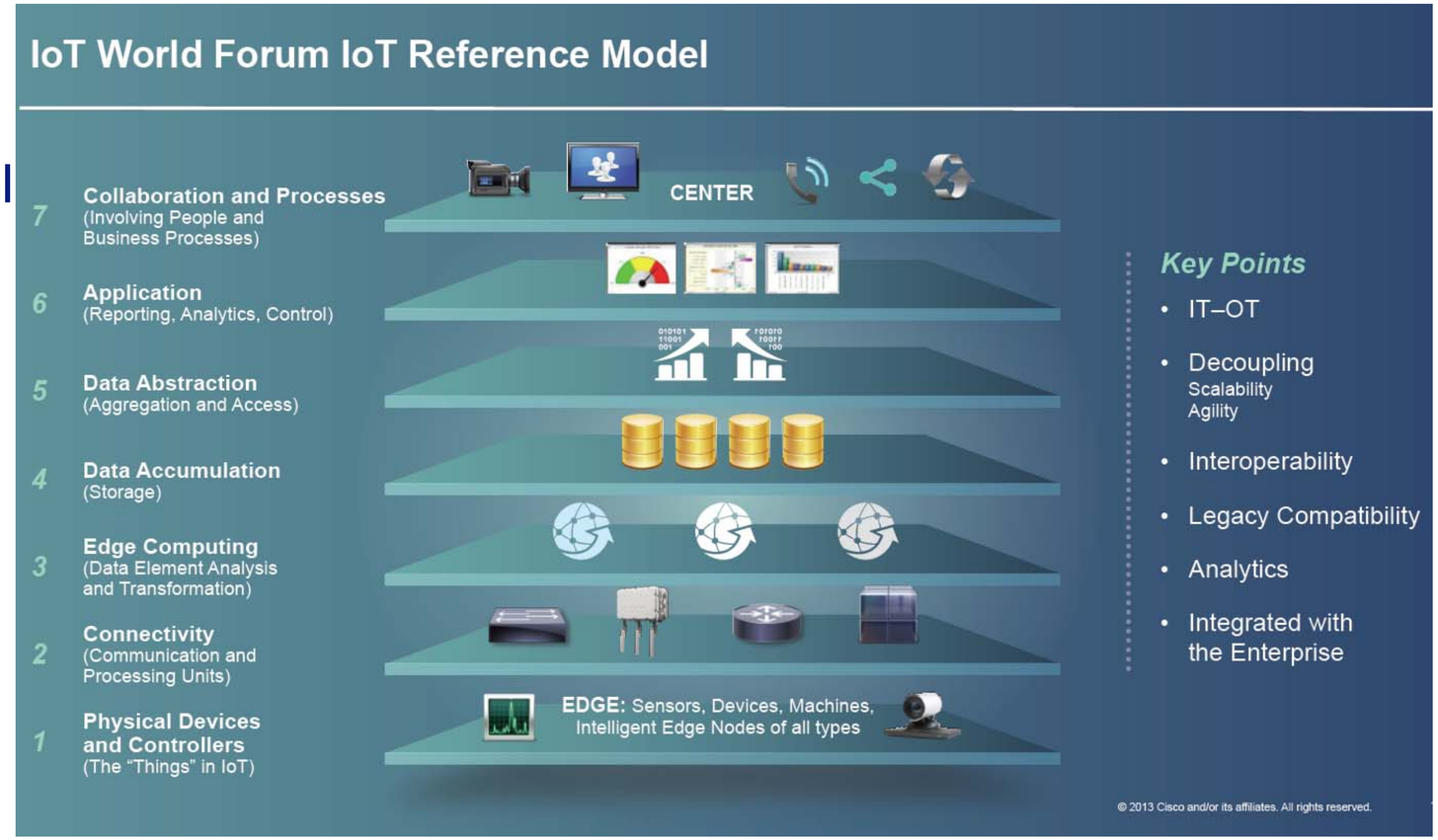
- The final grade is based on
  - a paper presentation (40%)
  - an oral exam (60%).

- Paper presentation
  - Keeping the time limits
  - Clear presentation of the topic
  - Own evaluation of the work

- Oral exam
  - Questions to your paper presentation
  - Topics of the course

Internet of Things

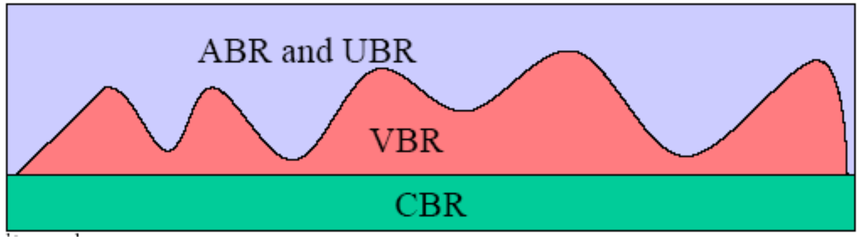
- Heading toward a fully connected world
- In a more focused way, in this course we speak about industrial internet of things
- The substantial difference is, that these systems have a physical dimension
- Considered as the next industrial revolution
- Automation to a new connectivity level – the internet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



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)
- High availability allows switchover in seconds



Automation as we know it

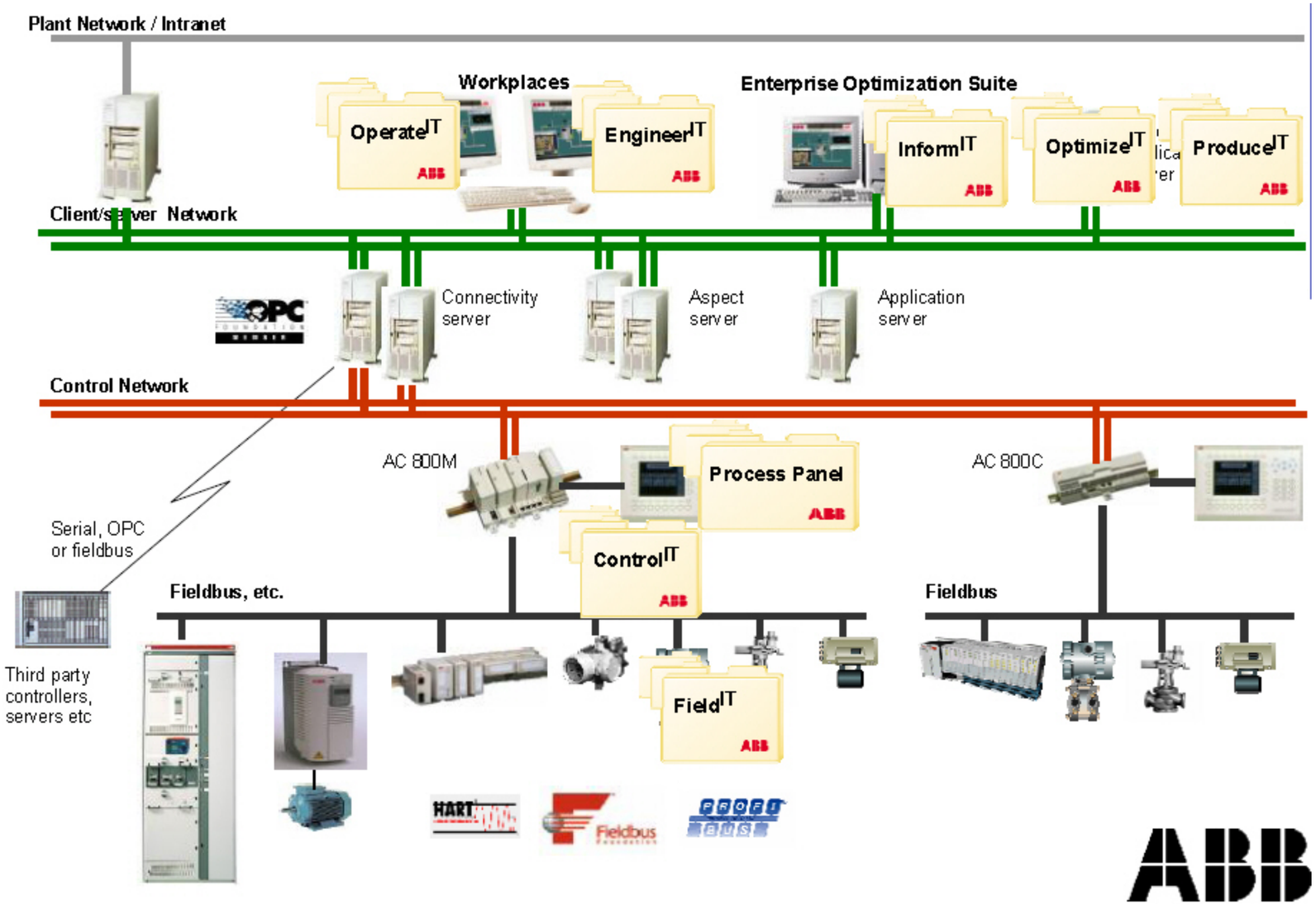
- Centralized intelligence
- Traditionally operated as islands by operations
- Direct connection with the physical world
- Is made for information gathering and processing by machines
- Has a lag of approx. 15-20 years, but cost pressure is reducing it
- Still current questions: what happens if one has to share infrastructure with others, how to operate a link with long step-out distance, use of Java
- Economic press leads to adoption of internet-based services which *require* a paradigm change

Mine (Boliden)

ABB robots

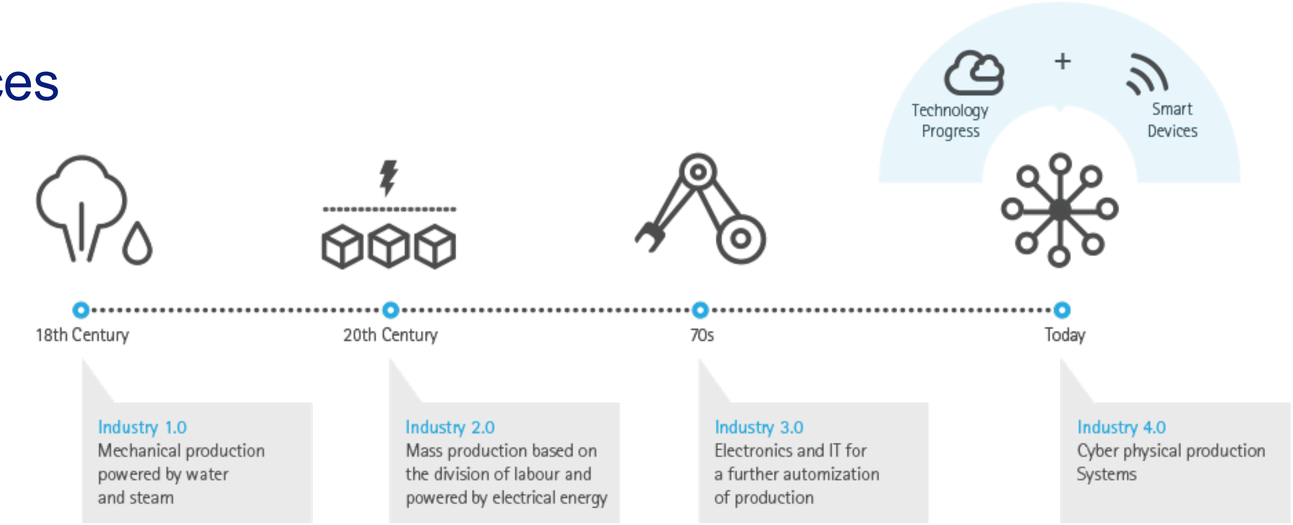
http://www07.abb.com/images/librariesprovider104/Extended-Automation/control-room-consolidation-by-abb.png?sfvrsn=1

Typical traditional industrial network



Merging these two

- Internet is the infrastructure – sensor, actuator, controller not on the same physical network any more
- ”dissolves” the automation system in the internet
- Automation processes run over an unknown communication infrastructure
- 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
- Challenges of security related to cloud services



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

Interesting challenges

- Architecture: physical impact, end-to-end resource reservation, discovery, safety, security and privacy
- Governance, interoperability, standardization
- Managing risk in a system with impact on both logical and physical level
- Provide QoS over a best effort infrastructure – with a price pressure

- Aggregation of data: here lies the added value, enables novel services and higher efficiency
- Distribution of intelligence: make the automation system more internet-like: intelligence in the end-nodes. Support it with the recent it trends of cloud and big data. Challenge for traditional automation mindset.
- Open architectural model
- Security concerns are a critical barrier for wide scale adoption of IoT
- Cloud and IoT

- See when IT has arrived to the phone industry. Or when IT has arrived into telco backhaul. IT is arriving to automation.

IoT services

- Enabled by wide scale data gathering
- Monitoring of massive systems
- Real-time insight to processes
- Observation of systems
- Performance measurement and optimization
- Proactive and predictive methods
- To serve the automation goals, the services provided must be: scalable, distributed, have a real reference to the physical world (e.g. time), must ensure security and privacy of the users
- Just using existing security solutions is not leading to secure IoT deployments
- Composed by IT, operations and the IoT enabled objects

- * Following slides are from the presentation of Mikhail Kader, DSE, Cisco, presented on the ITU Workshop on “ICT Security Standardization for Developing Countries”

Connected Rail Operations *

PASSENGER SECURITY
- In-station and onboard safety
- Visibility into key events

ROUTE OPTIMIZATION
- Enhanced Customer Service
- Increased efficiency
- Collision avoidance
- Fuel savings

CRITICAL SENSING
- Transform “data” to “actionable intelligence”
- Proactive maintenance
- Accident avoidance

Cost savings, improved safety, superior service

Smart City *

CONNECTED TRAFFIC SIGNALS

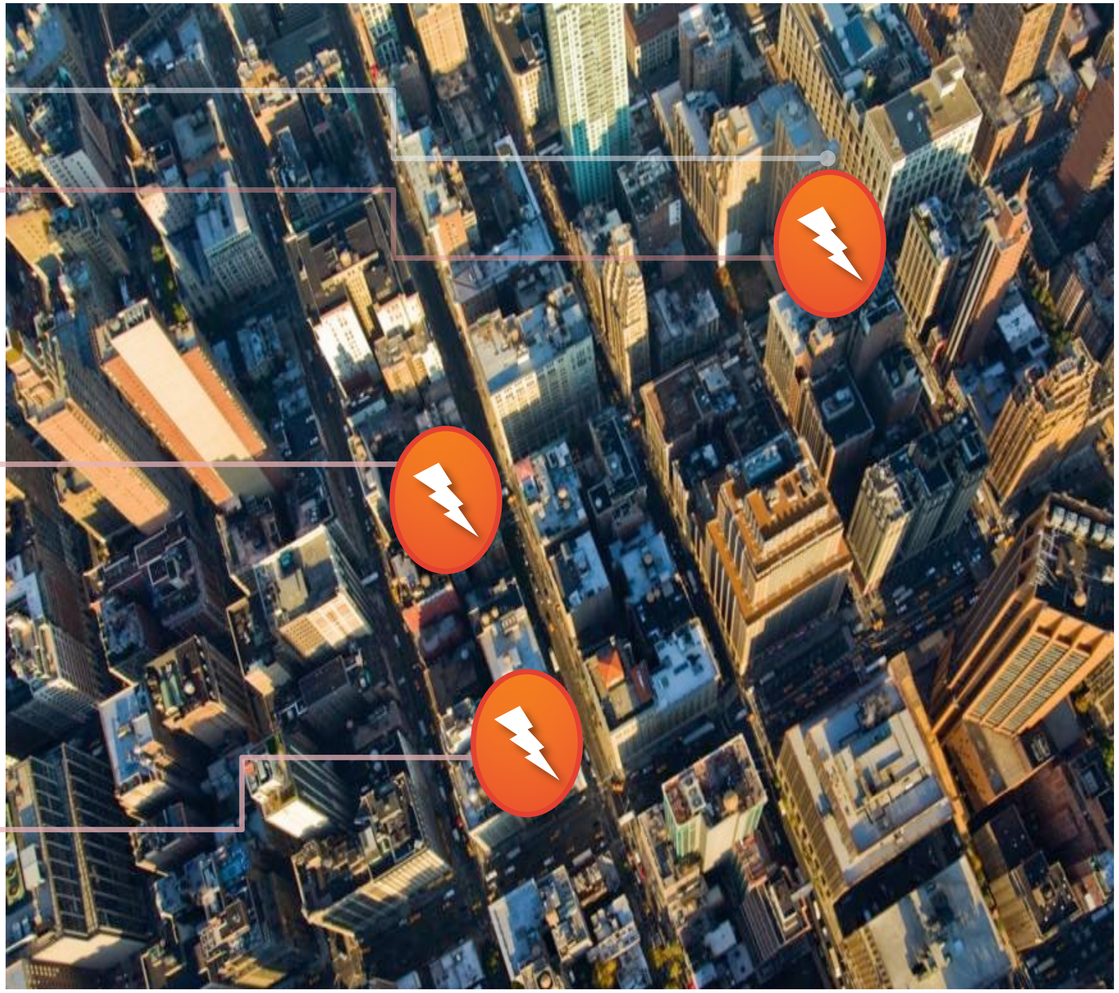
- Reduced congestion
- Improved emergency services response times
- Lower fuel usage

PARKING AND LIGHTING

- Increased efficiency
- Power and cost savings
- New revenue opportunities

CITY SERVICES

- Efficient service delivery
- Increased revenues
- Enhanced environmental monitoring capabilities

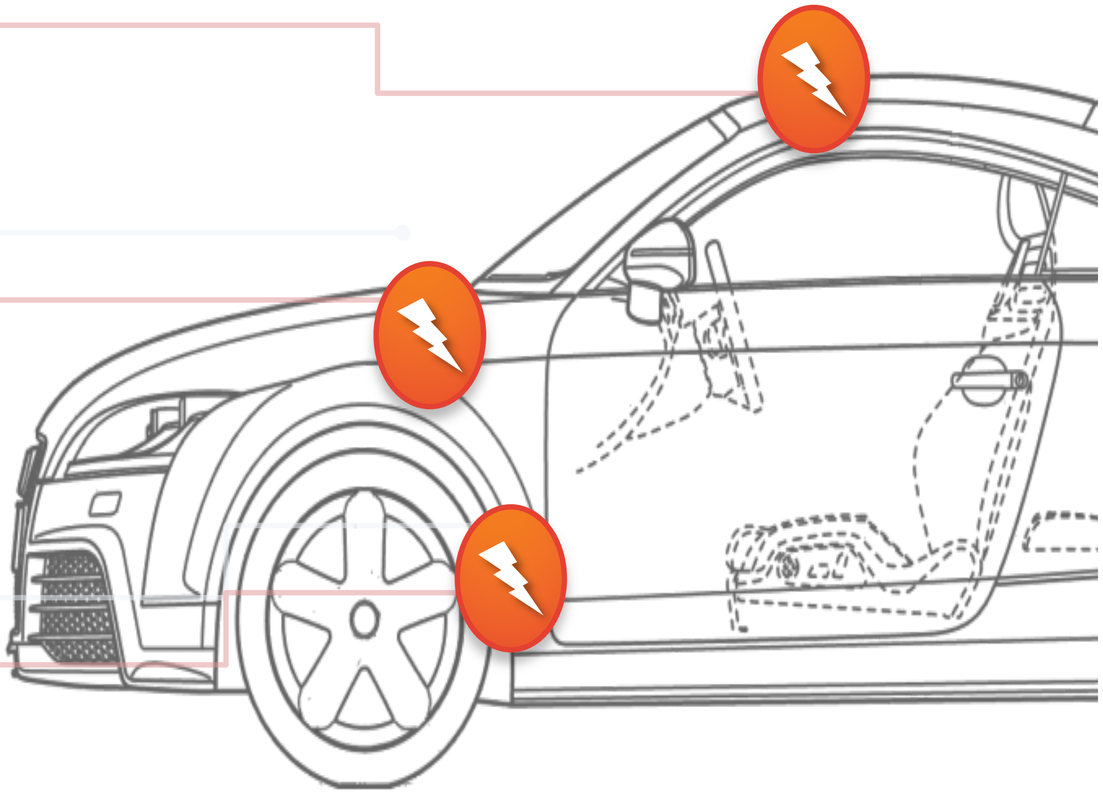


The Connected Car *

WIRELESS ROUTER
- Online entertainment
- Mapping, dynamic re-routing, safety and security

CONNECTED SENSORS
- Transform “data” to “actionable intelligence”
- Enable proactive maintenance
- Collision avoidance
- Fuel efficiency

URBAN CONNECTIVITY
- Reduced congestion
- Increased efficiency
- Safety (hazard avoidance)



IoT Expands Security Needs *

Increased Attack Surface

Threat Diversity

Impact and Risk

Remediation

Protocols

Compliance and Regulation

Converged, Managed Network

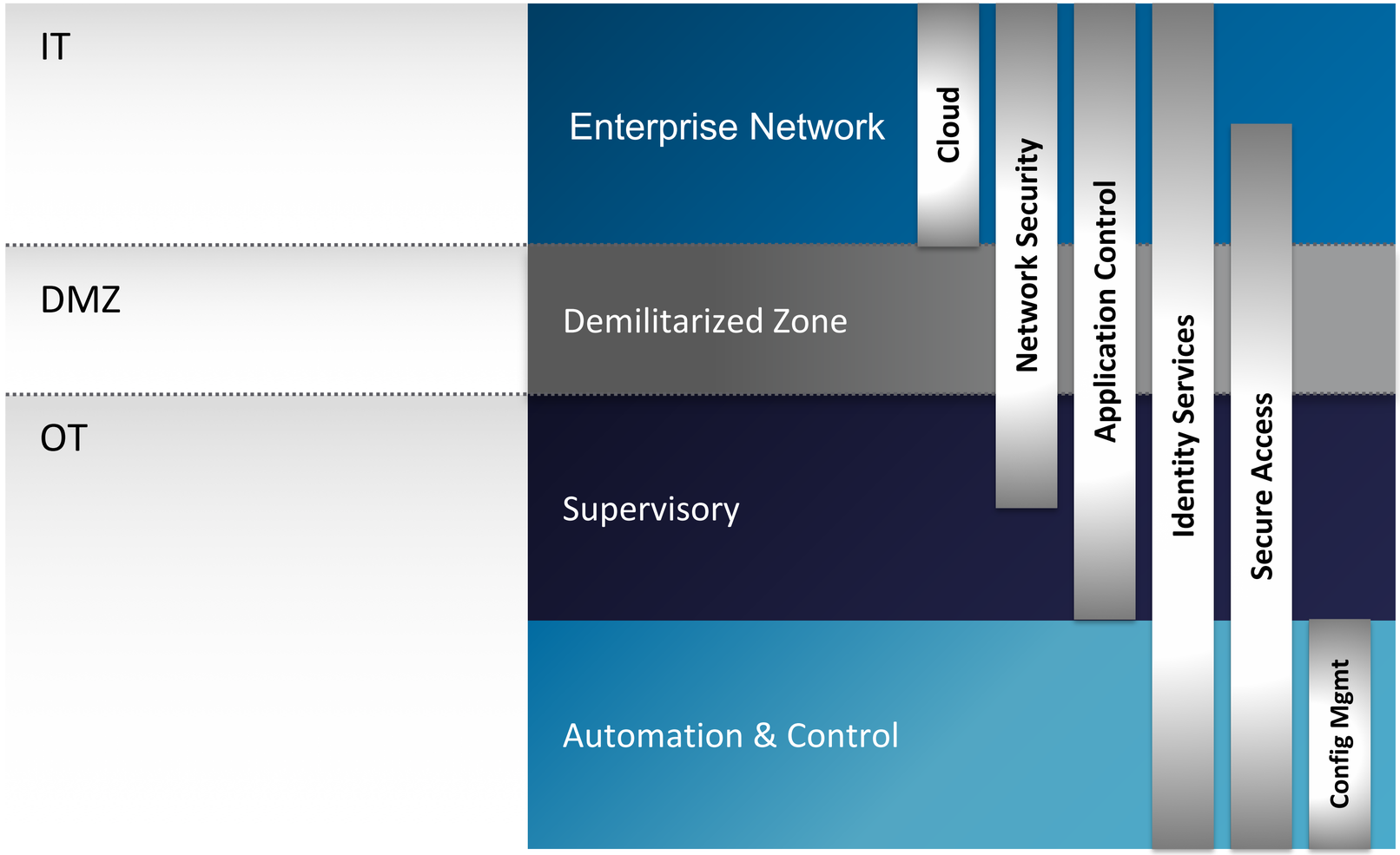
Resilience at Scale

Security

Distributed Intelligence

Application Enablement

IT/OT Converged Security Model *



IT and OT are Inherently Different *

- IT
  - Connectivity: “Any-to-Any”
  - Network Posture: Confidentiality, Integrity, Availability (CIA)
  - Security Solutions: Cybersecurity; Data Protection
  - Response to Attacks: Quarantine/Shutdown to Mitigate
- OT
  - Connectivity: Hierarchical
  - Network Posture: Availability, Integrity, Confidentiality (AIC)
  - Security Solutions: Physical Access Control; Safety
  - Response to Attacks: Non-stop Operations/Mission Critical – Never Stop, Even if Breached

What Can Lead to Breach in IoT Networks?

- What can't?
  - Billions of connected devices
  - Secure and insecure locations
  - Security may or may not be built in
  - Life cycle mismatch between IT and automation devices
  - Installed base
  - Clash between IT and OT, IT has to accept the traffic

- Any node on your network can potentially provide access to the core

L1 Conclusions

- Overview over lectures
- Explanation of portfolio and exam
- Introduction to topic blocks
- Discussion

[Source of starred slides: Monique Morrow, Cisco]