UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L13 – Technology Mapping

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

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

TEK5530: Lecture plan

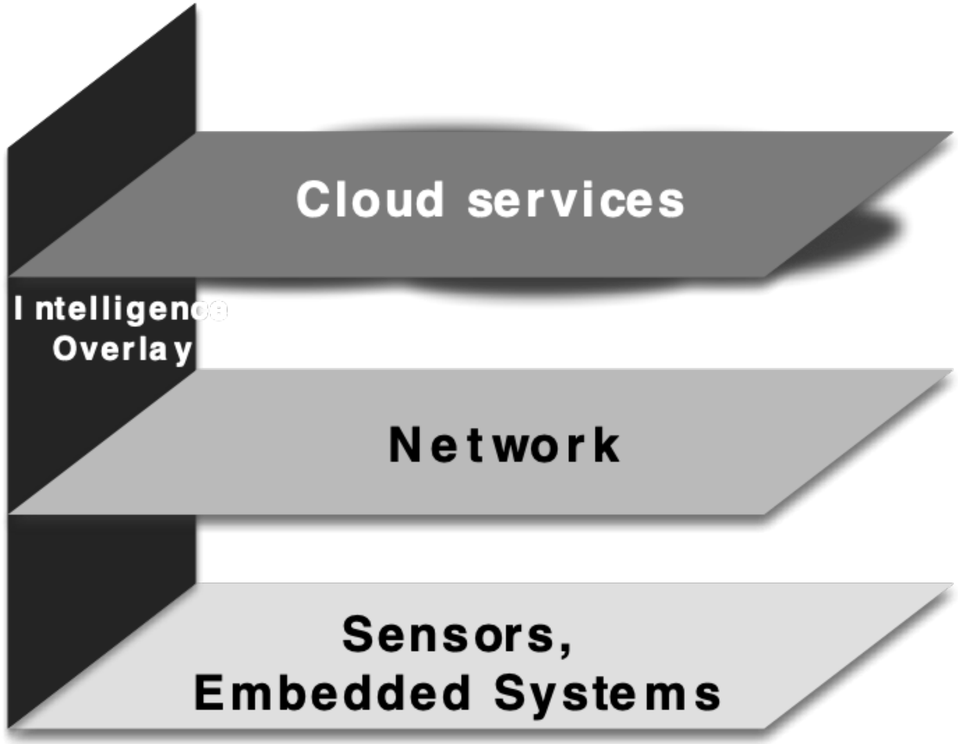
- 16Jan (Gyorgy Kalman & Josef Noll) 09:15-16:00h
- L1: Introduction (Josef Noll) Media:TEK5530-L1.pdf
- Tesla battery with high earnings when balancing the Australian grid
- Tesla battery paid back third of investment in a year
- eHealth predictions for 2019
- L2: Internet of Things (Gyorgy Kalman) Media:TEK5530-L2.pdf Media:TEK5530-L2-notes.pdf
- Paper used for the group work on the lecture: Atzori et al. Survey Internet of Things
- Video introduction: IBM introduction to IoT, TED talk of John Barrett Introduction to Amazon AWS IoT
- 23.01 (Gyorgy Kalman)
- L3: Security of IoT + Paper list Media:TEK5530-L3.pdf
- Advantech Internet Gateway Vulnerability
- ICS-CERT alerts
- OWASP IoT Project
- Data leakage from fitness tracker app reveals base locations
- L4: Smart Grid, Automatic Meter Readings Media:TEK5530-L4.pdf
- 06.02 (Josef Noll)
- L5: Semantic Technologies - Ontologies Media:TEK5530-L5.pdf - Whiteboard Notes: Media:TEK5530-L5-L6-Notes.pdf
- see: intro to semantics https://www.youtube.com/watch?v=4x_xzT5eF5Q
- enjoy: ordering a piza https://www.youtube.com/watch?v=RNJl9EEcsoE
- details on Ontologies: https://www.slideshare.net/marinasantini1/09-semantic-webontologies?qid=8b178746-ea3c-48db-b4f6-6bc9b0923d9b
- IoT Life-Cycle Security, see: IoTSec:Security_and_Privacy_Functionality with document IoT Security and Privacy Functionality Life Map (.pdf)
- L6: Multi-Metrics Method for measurable Security Media:TEK5530-L6_Multi-Metrics.pdf
- Security threats/attacks on IoT by Tom Gaffney, F-Secure https://eyenetworks.no/wp-content/uploads/2019-shared-insights-tom-gaffney-f-secure-1.pdf
- Mirai attack capabilities IoTSec:The_Denial_of_Service_Attack_from_IoT_devices
- Privacy label, see Privacy_Label
- **13.02 (Josef Noll)**
- **L7: Multi-Metrics Weighting of an AMR sub-system Media:TEK5530-L.pdf**
- **L8: System Security and Privacy analysis Media:TEK5530-L.pdf**
- 20.02 (Josef Noll) L9-10: Paper analysis with 25 min presentation
- 27.02 no lecture
- 05.03 (Gyorgy Kalman)
- L11: Service implications on functional requirements Media:TEK5530-L.pdf
- L12: Intrusion Detection Media:TEK5530-L.pdf
- 12.03 (Gyorgy Kalman)
- L13: Technology mapping Media:TEK5530-L.pdf
- L14: Communication and security in current industrial automation Media:TEK5530-L.pdf
- 19.03 (Gyorgy Kalman)
- L15: Cloud basics and cloud architecture Media:TEK5530-L.pdf
- L16: Cloud security, IoT and service examples from AWS Media:TEK5530-L.pdf
- Exam: to be decided - either 26Mar2020 or after Easter, e.g. 16Apr2020

Overview

- Recap: last time we talked about QoS Security is also part of QoS
- System components
- QoS in LAN and WAN
- Challenges
  - Performance monitoring
  - Forwarding control
  - Security measures
- Examples
- Conversion, operating envelope
- Conclusion

System components

- Functional components
  - ➡ input component (sensors, keyboard, mouse,..)
  - ➡ output component (alarm, screen, actuator,..)
  - ➡ processing component
  - ➡ Storing component (data base, files,)
  - ➡ Connection (wireless connection, wired connection)
- Security, Privacy, Dependability (SPD) components:
  - ➡ Encryption: Encryption algorithm, keys,..
  - ➡ Protocols
  - ➡ Authentication(mechanism (fingerprint, password, password complexity,.....) .
  - ➡ Authorization (privileges, ..)
- Management components (OS, Web server, data server)
- Human component (admin, user, ..).
- Physical component, car being a component in a car factory. (if treated as “sub-system)

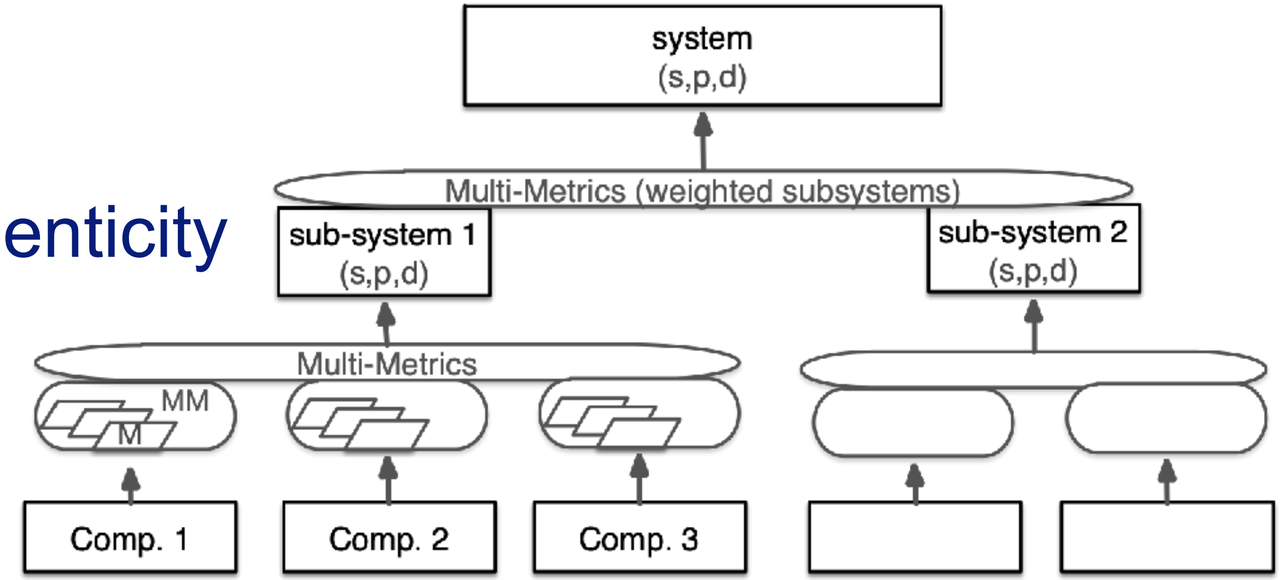


QoS in LAN and WAN

- Communication metrics: bandwidth, delay, jitter, burstiness, redundancy
- Automation metrics: sampling frequency, delay, jitter, redundancy

- LAN-WAN

- Time synchronization
- Security focus on integrity and authenticity
- Availability



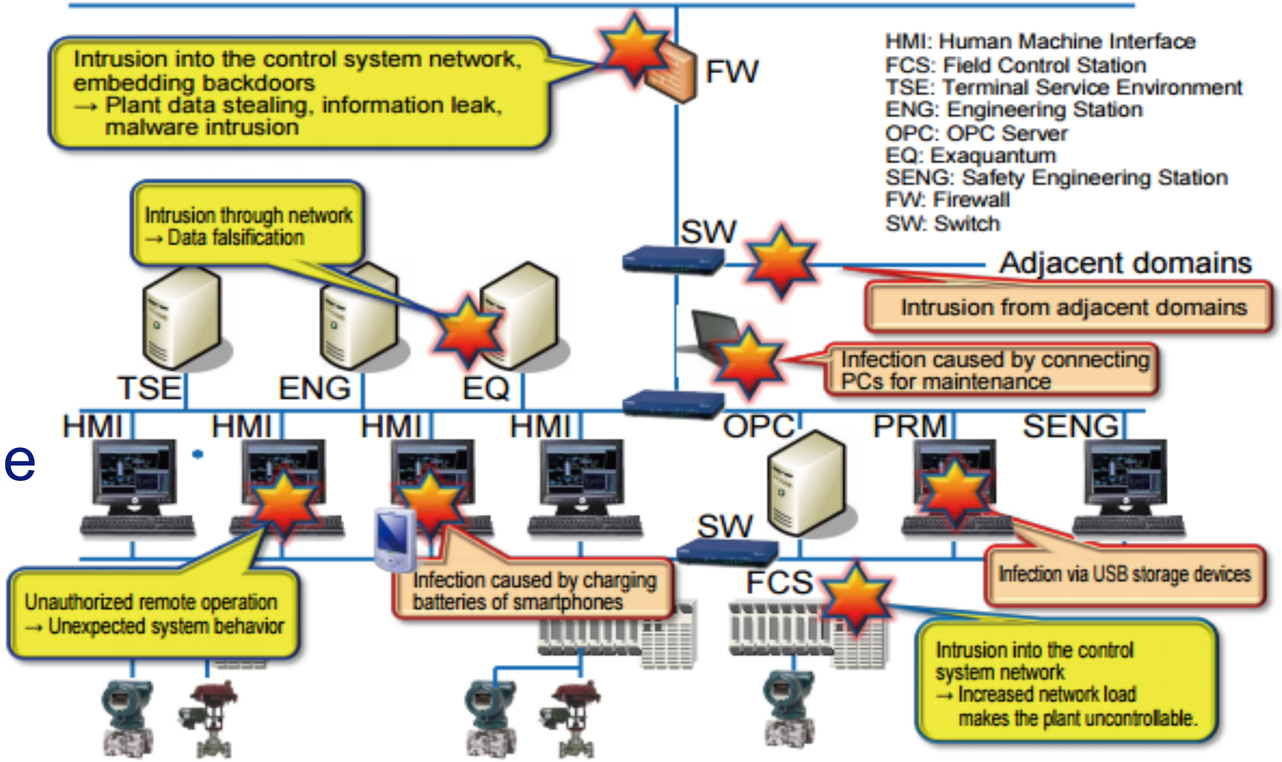
Performance monitoring and forwarding control

- Performance monitoring
  - Life-cycle support
  - More important in the WAN case

- Forwarding control
  - IEEE 802.1 TSN - SPB

Integrity – Authenticity – (Confidentiality)

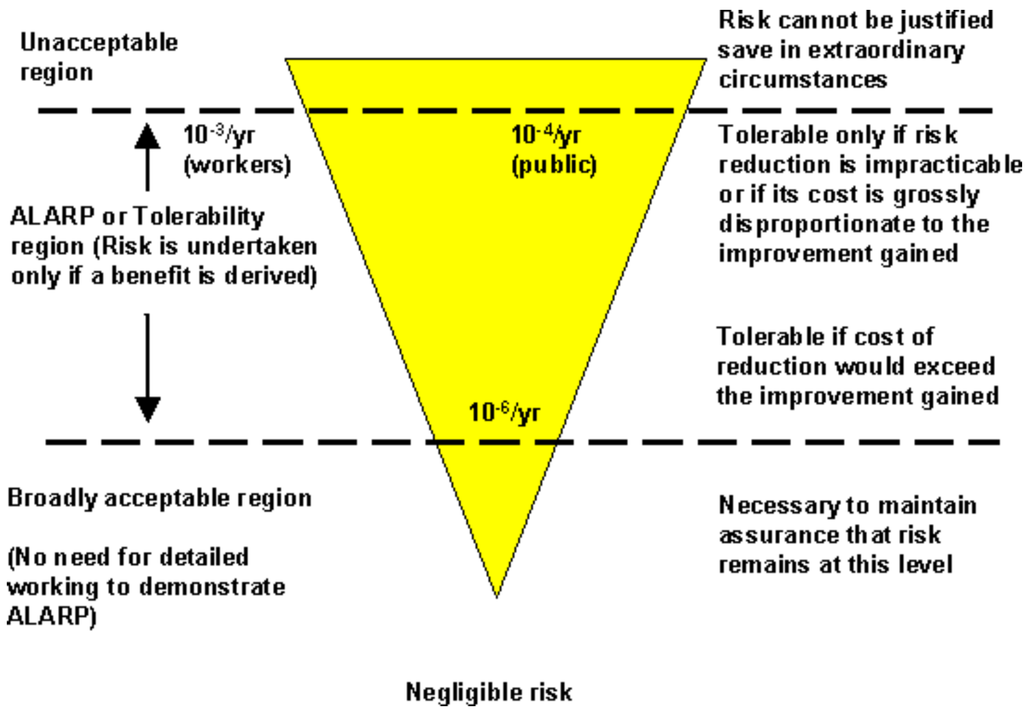
- Endpoint security in control systems
- Identifying security risks in automation networks
- Countermeasures:
  - ➡ IDS/IPS
  - ➡ Firewall
  - ➡ Automatic updates
  - ➡ Application black/whitelisting
  - ➡ Backup
- Integrity
  - ➡ Safety is not protecting from sabotage
  - ➡ In general, no sabotage protection
- Availability
  - ➡ Alarms



https://www.yokogawa.com/rd/pdf/TR/rd-te-r05702-008.pdf

Availability

- Main objective of Control System security:
  To maintain the integrity of its production process and the availability of its components
- Maps to:
  - ➡ Network redundancy
  - ➡ Software and hardware requirements
  - ➡ Device redundancy



- Shodan

Example

- IEC 61850 in smart grid scenario
- AMS consists of reader (AMR), aggregator, communications, storage, user access
- AMR consists of power monitor, processing unit, communication unit
- AMR communication contains of a baseband processing, antenna, wireless link

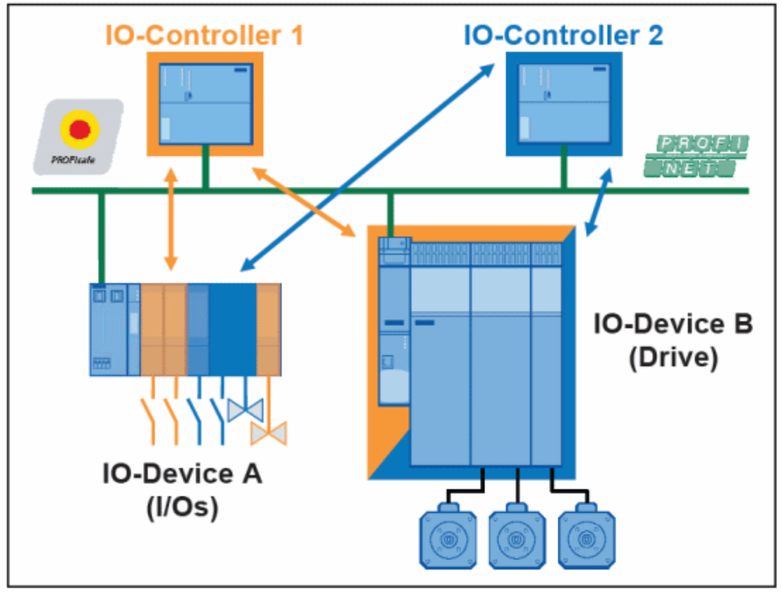
- Requirements traceability
- Relevance for the whole communication path

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

Example

- From the Siemens SINAMIC example library:
- **SINAMICS S: Safety-control of a S120 using S7-300/400 (STEP 7 V5) with PROFINET (Shared Device) and Safety Integrated (via PROFIsafe)**



Caution
The functions and solutions described in this article confine themselves to the realization of the automation task predominantly. Please take into account furthermore that corresponding protective measures have to be taken up in the context of Industrial Security when connecting your equipment to other parts of the plant, the enterprise network or the Internet. Further information can be found under the Item-ID 50203404.

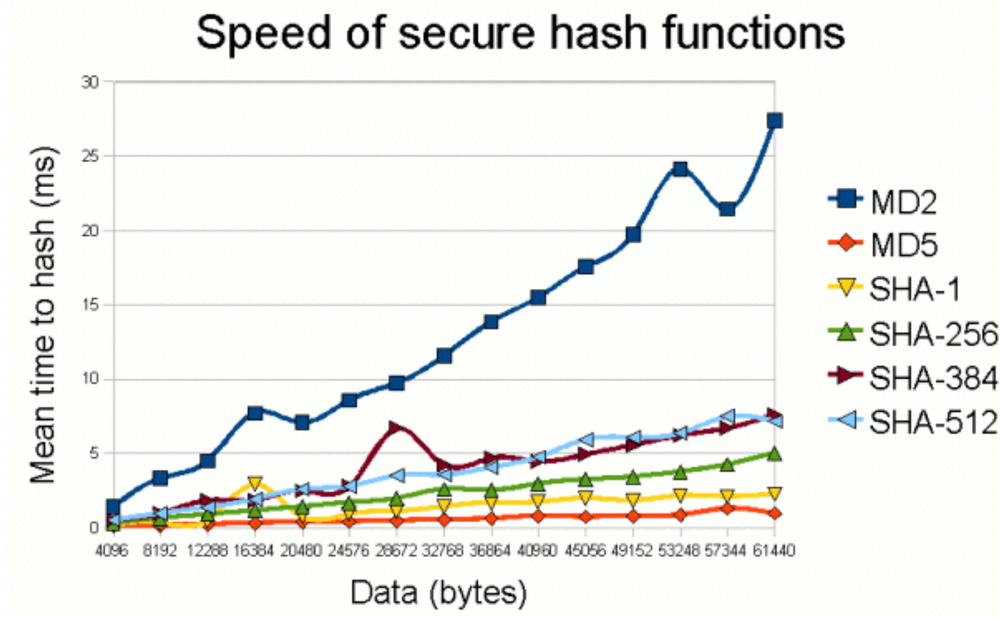
http://support.automation.siemens.com/WW/view/en/50203404

Identifying QoS metrics for security

- Risk analysis to identify attack surface
- Integrity – Authenticity – Confidentiality
- Data validity and reaction possibilities
- Physical security
- Whole communication path should be evaluated

Selecting technologies

- Select by mapping requirements to technology properties:
  - Hash: integrity requirement, stream speed, latency, size
  - Cipher: security requirement (includes already data validity and generic risk evaluation), delay, size – optimized ciper suites are available



http://www.javamex.com/tutorials/cryptography/hash_functions_algorithms.shtml

L6 Conclusions

- Services in IoT have an implication typically in the communication and security domain of IT
- Main challenge is the lack of understanding
- Sub-challenges are life-cycle management, status monitoring, continous evaluation of QoS
- Don't believe in the IoT explosion?
  Consider this: – How many MAC Addresses did you use in 1998?
  Typically less than 5: • Work computer, home computer, a laptop. . .
  Move to 2017. Now how many MAC Addresses do you use?
  Typically 15 to 20: • Cell phone, IP phone, laptop (2 – 1 for wired, 1 for wireless), laser printer (2 – same reason), set top box (2), TV, tablet, computer at home (2), gaming console, thermometer, weather station, wireless AP