UNIK4750 - Measurable Security for the Internet of Things

L6 – Technology Mapping

György Kálmán,
Mnemonic/CCIS/UNIK
gyorgy@unik.no

Josef Noll
UiO/UNIK
josef@unik.no

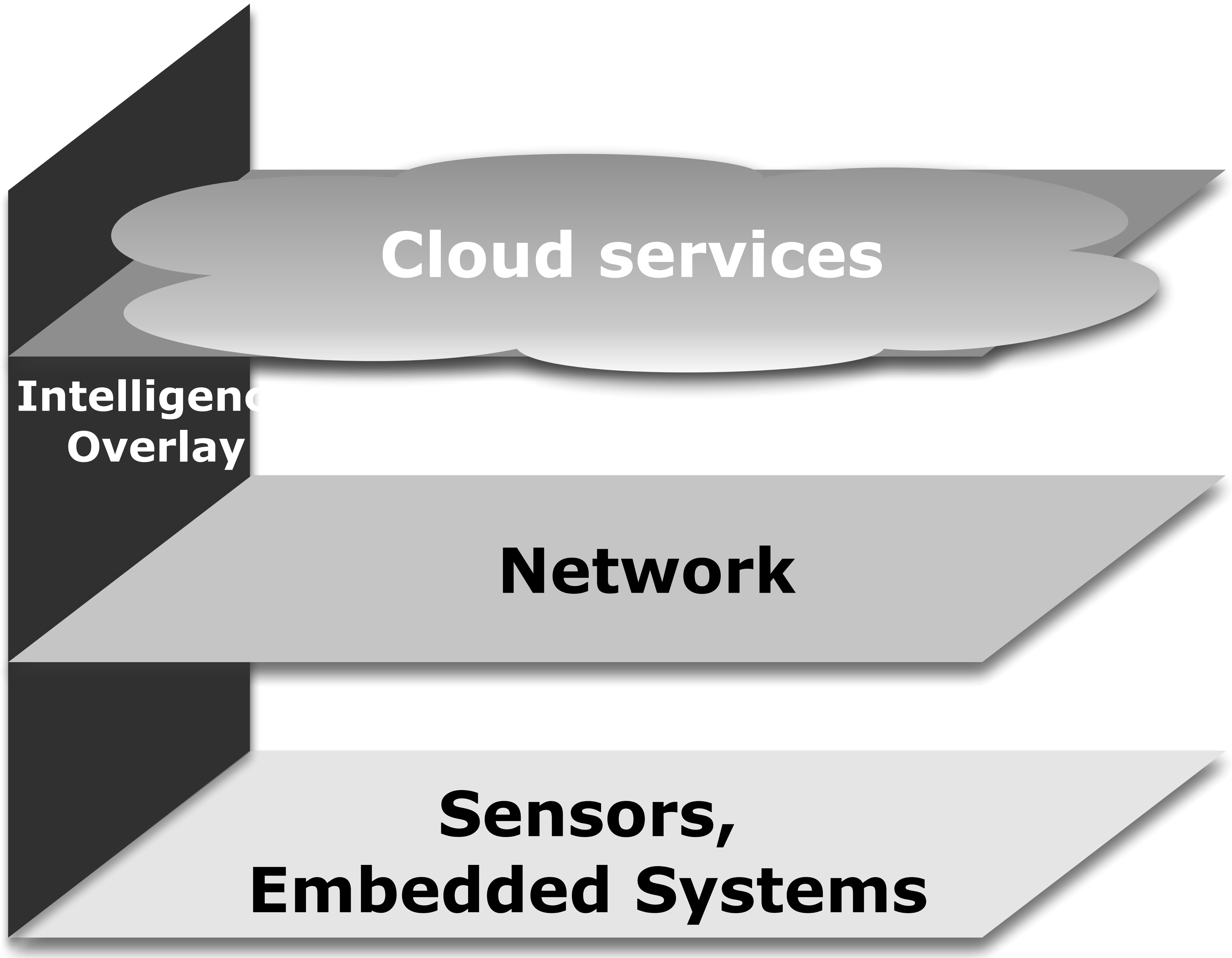
http://cwi.unik.no/wiki/UNIK4750, #IoTSec, #IoTSecNO

Overview

- Recap: two weeks ago 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)



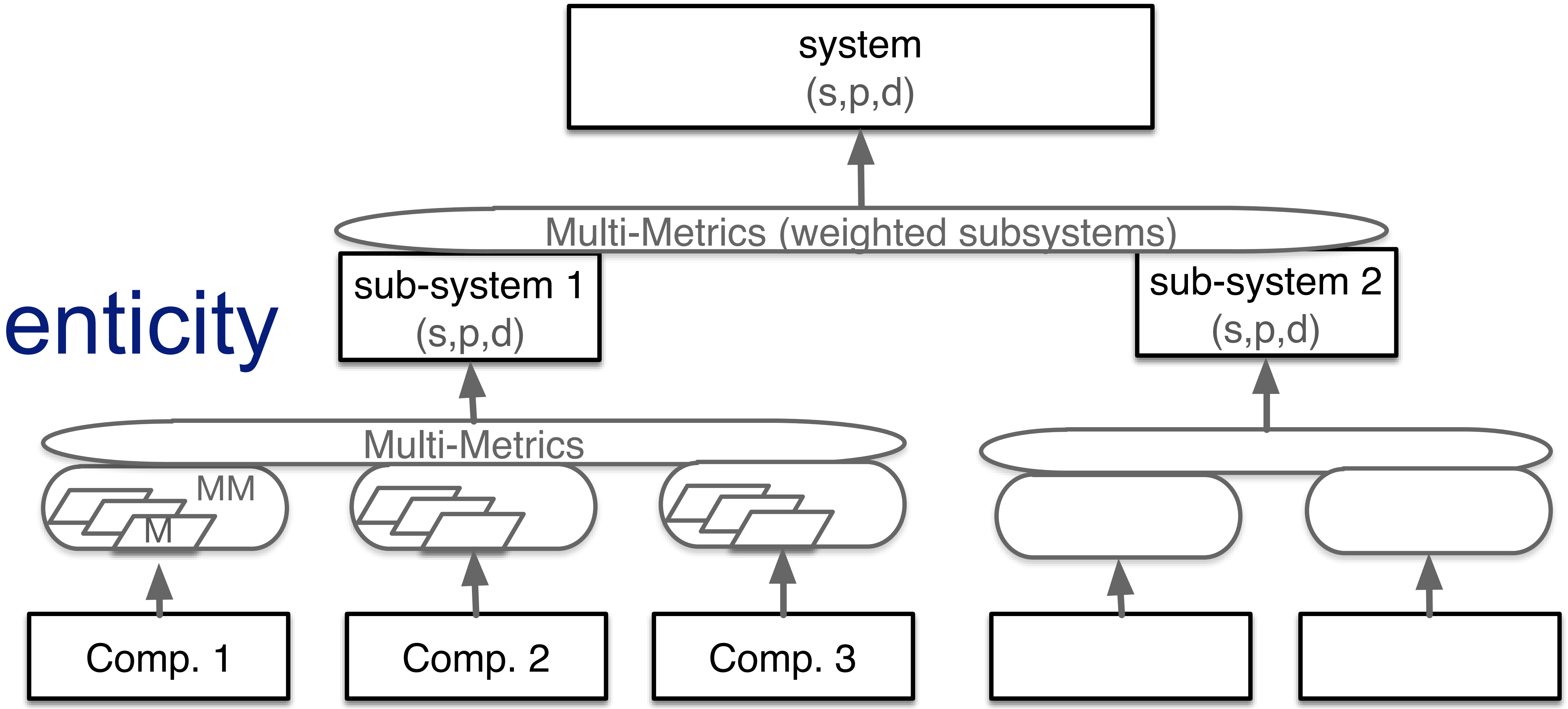
- Match between components and Architecture?

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



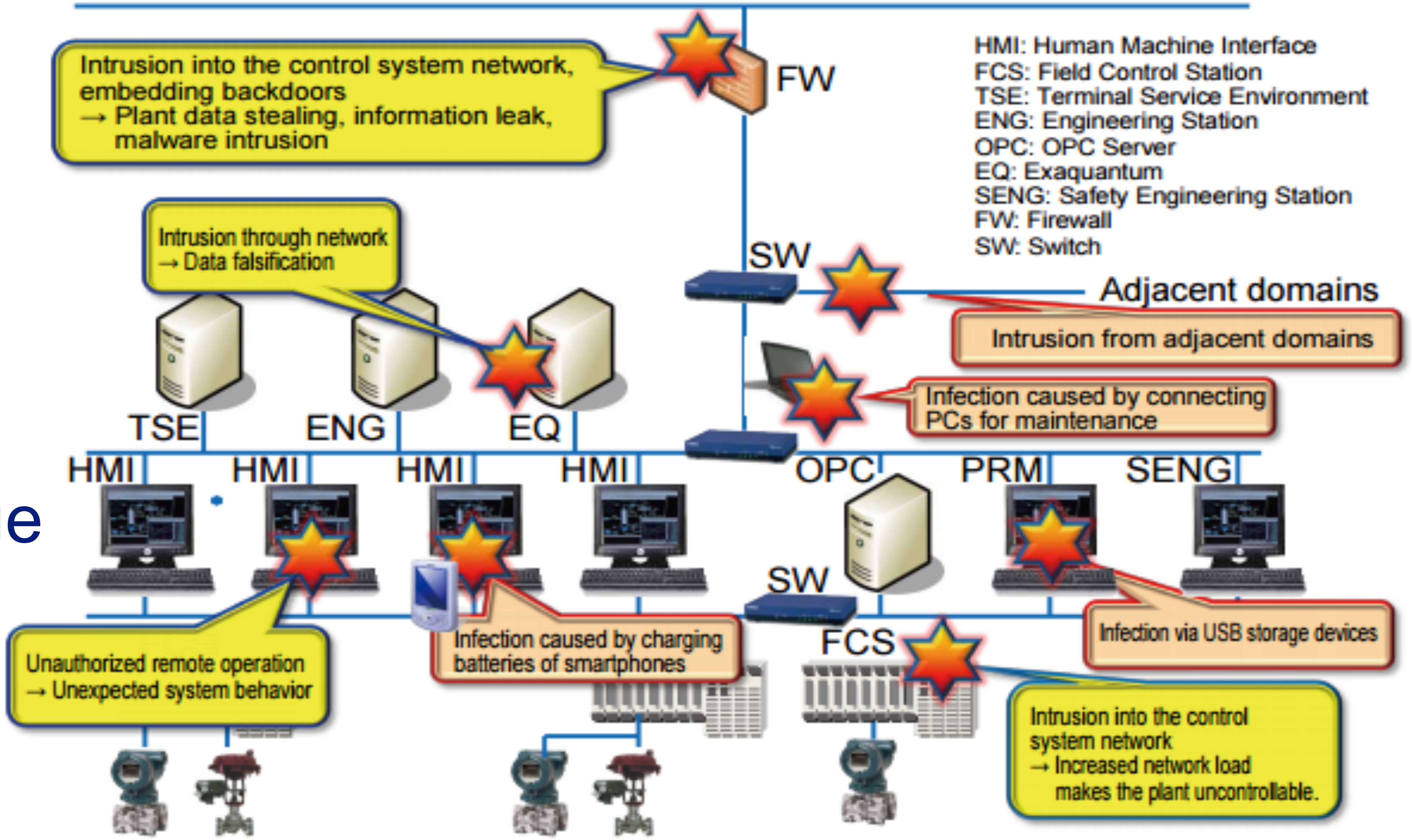
Performance monitoring and forwarding control

- 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



HMI: Human Machine Interface
FCS: Field Control Station
TSE: Terminal Service Environment
ENG: Engineering Station
OPC: OPC Server
EQ: Exaquantum
SENG: Safety Engineering Station
FW: Firewall
SW: Switch

Intrusion into the control system network, embedding backdoors
→ Plant data stealing, information leak, malware intrusion

Intrusion through network
→ Data falsification

Intrusion from adjacent domains

Infection caused by connecting PCs for maintenance

Unauthorized remote operation
→ Unexpected system behavior

Infection caused by charging batteries of smartphones

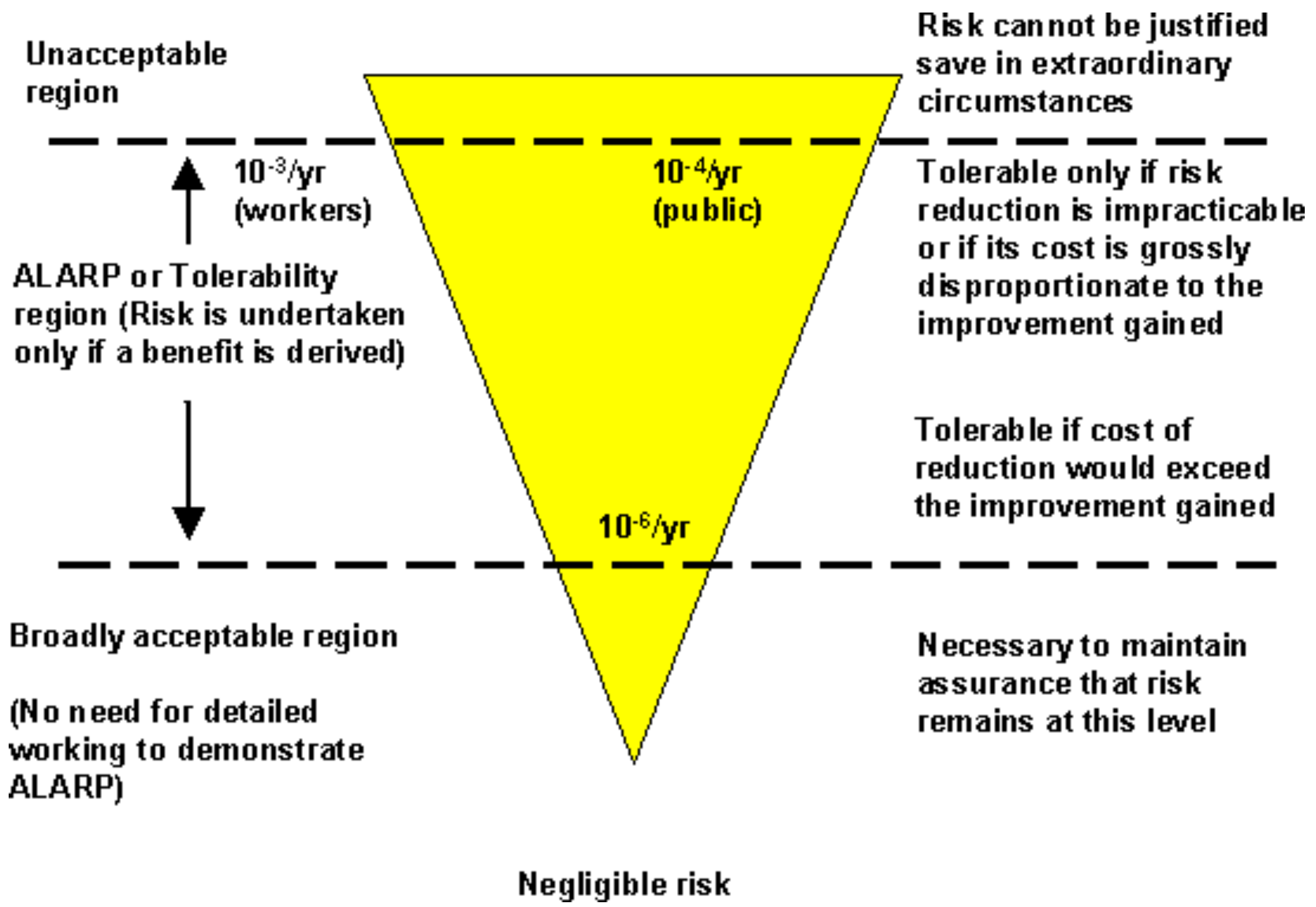
Infection via USB storage devices

Intrusion into the control system network
→ Increased network load makes the plant uncontrollable.

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 browser IoT



Unacceptable region

Risk cannot be justified save in extraordinary circumstances

10^{-3}/yr (workers)

10^{-4}/yr (public)

ALARP or Tolerability region (Risk is undertaken only if a benefit is derived)

Tolerable only if risk reduction is impractical or if its cost is grossly disproportionate to the improvement gained

Tolerable if cost of reduction would exceed the improvement gained

10^{-6}/yr

Broadly acceptable region

(No need for detailed working to demonstrate ALARP)

Necessary to maintain assurance that risk remains at this level

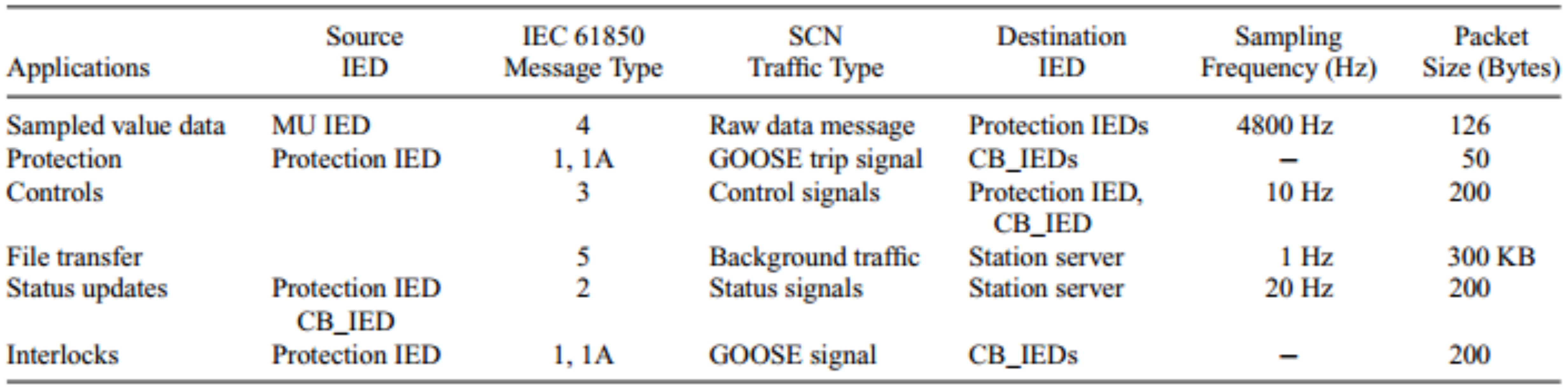
Negligible risk

http://www2.emersonprocess.com/siteadmincenter/PM%20Articles/InTech_MayJune2014_TopTenDiff.pdf

Example

- IEC 61850 in smart grid scenario
- AMS consists of reader (AMR), aggregator, communications, storage, user acces
- 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

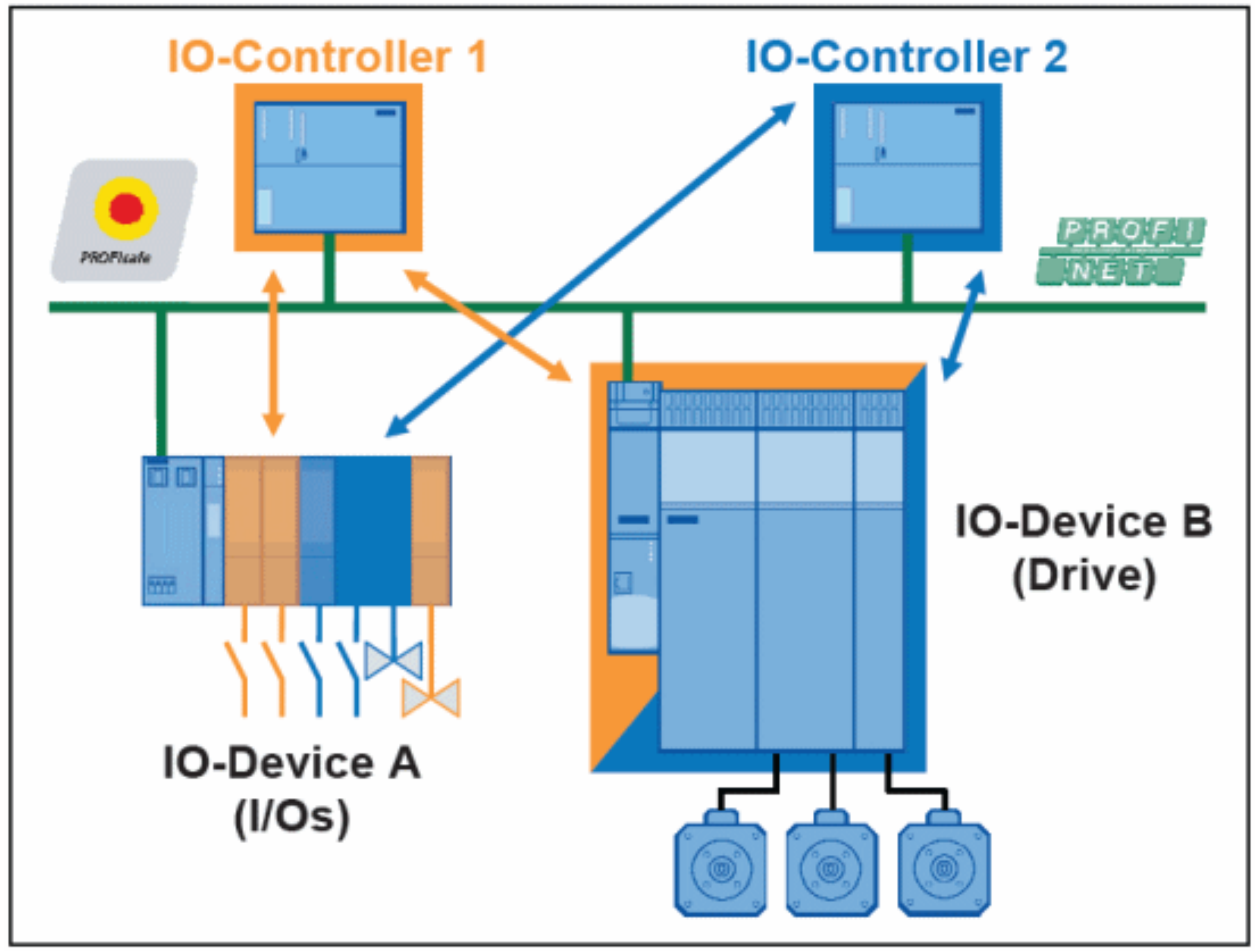


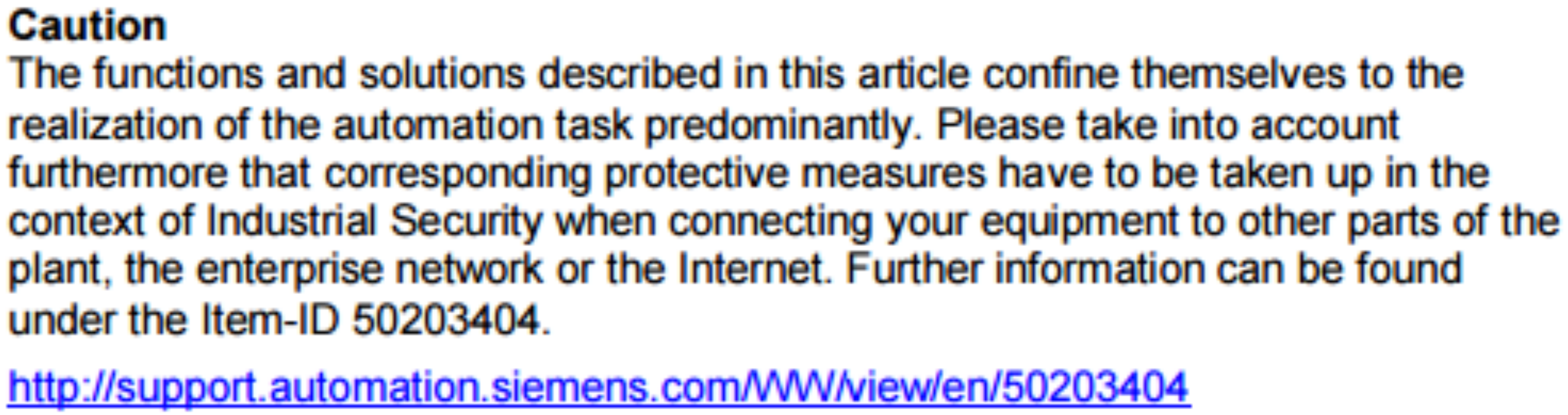
Applications	Source IED	IEC 61850 Message Type	SCN Traffic Type	Destination IED	Sampling Frequency (Hz)	Packet Size (Bytes)
Sampled value data	MU IED	4	Raw data message	Protection IEDs	4800 Hz	126
Protection	Protection IED	1, 1A	GOOSE trip signal	CB_IEDs	–	50
Controls		3	Control signals	Protection IED, 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.

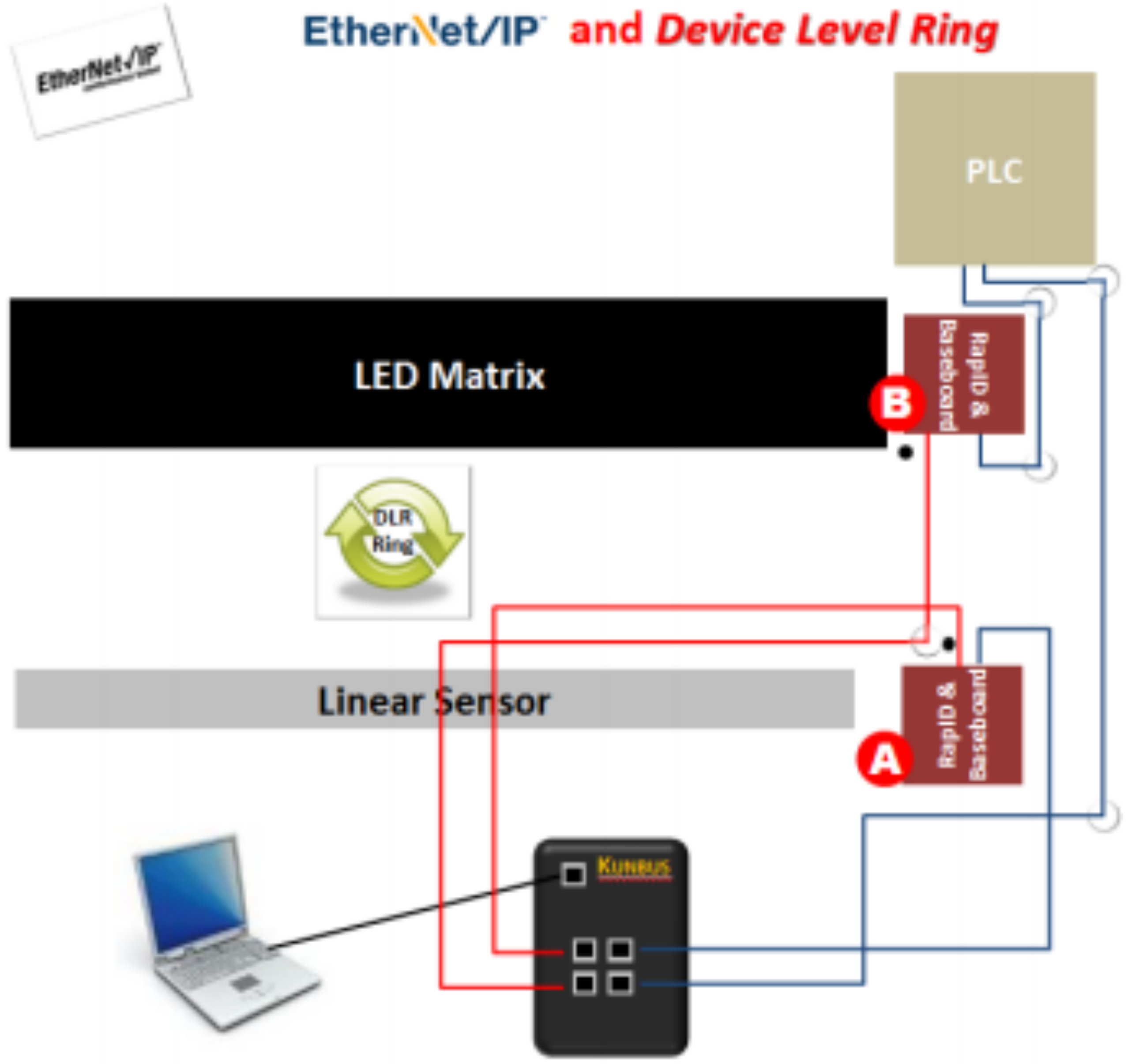
http://support.automation.siemens.com/WW/view/en/50203404

Identifying QoS metrics for security

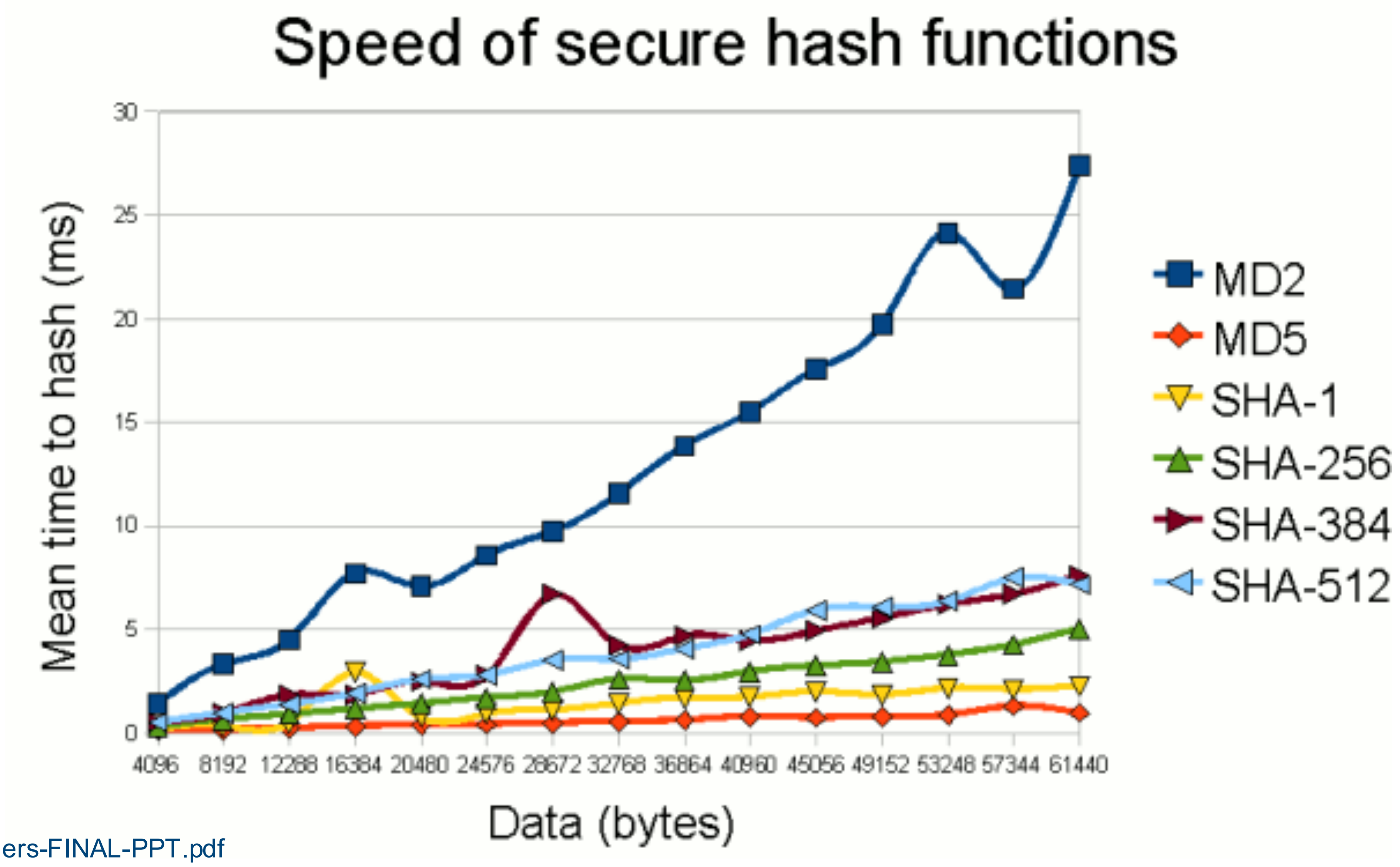
- Risk analysis to identify attack surface
- Integrity – Authenticity – Confidentiality
- Data validity and reaction possibilities
- Phyisical security
- Whole communication path should be evaluated

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



https://www.odva.org/Portals/0/Library/Conference/2015_ODVA_Conference_Woods_Practical-applications-of-Lightweight-Block%20Ciphers-FINAL-PPT.pdf



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 2014. Now how many MAC Addresses do you use?
  Typically 10 to 15: • Cell phone, IP phone, laptop (2 – 1 for wired, 1 for wireless), laser printer (2 – same reason), set top box (2), TV, BluRay player, tablet, computer at home (2), wireless AP

https://www.odva.org/Portals/0/Library/Conference/2015_ODVA_Conference_Woods_Practical-applications-of-Lightweight-Block%20Ciphers-FINAL-PPT.pdf