UNIK4750 - Measurable Security for the Internet of Things

L5 – Service Implications on Functional Requirements

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

Josef Noll
UiO/UNIK
josef@unik.no

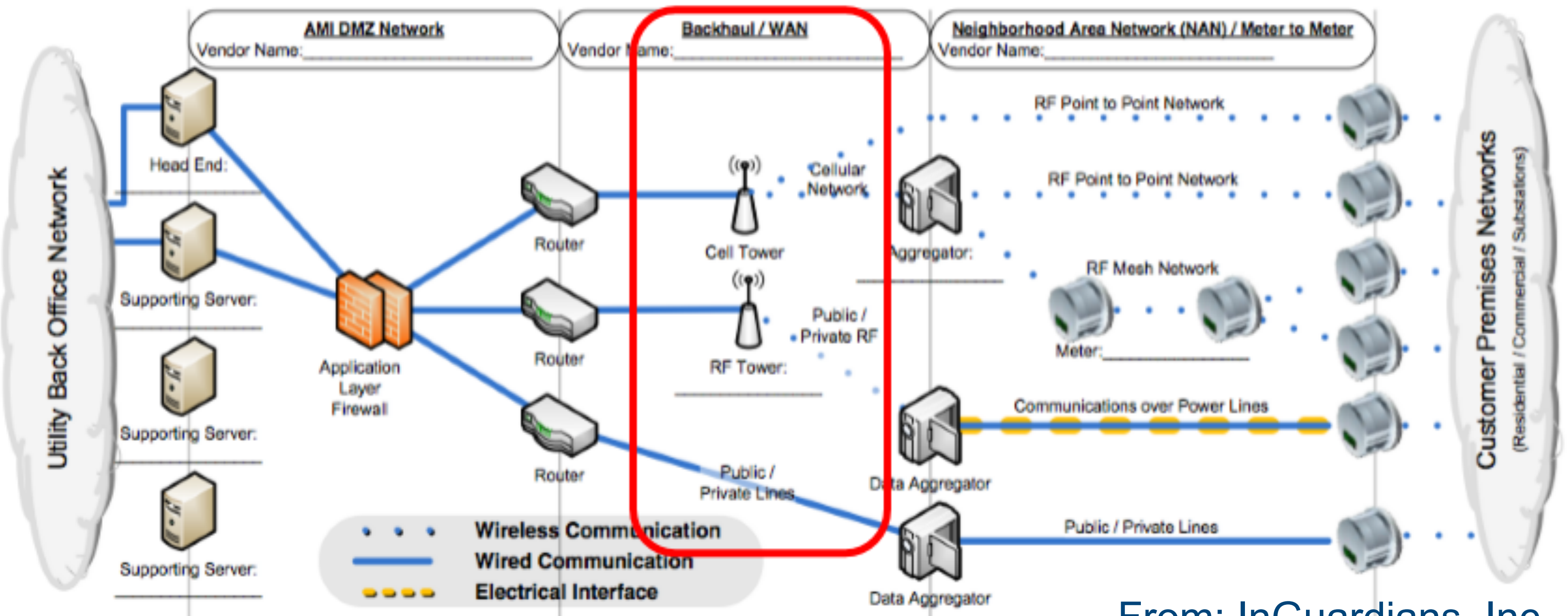
http://cwi.unik.no/wiki/UNIK4750, #IoTSec, #IoTSecNO

Overview

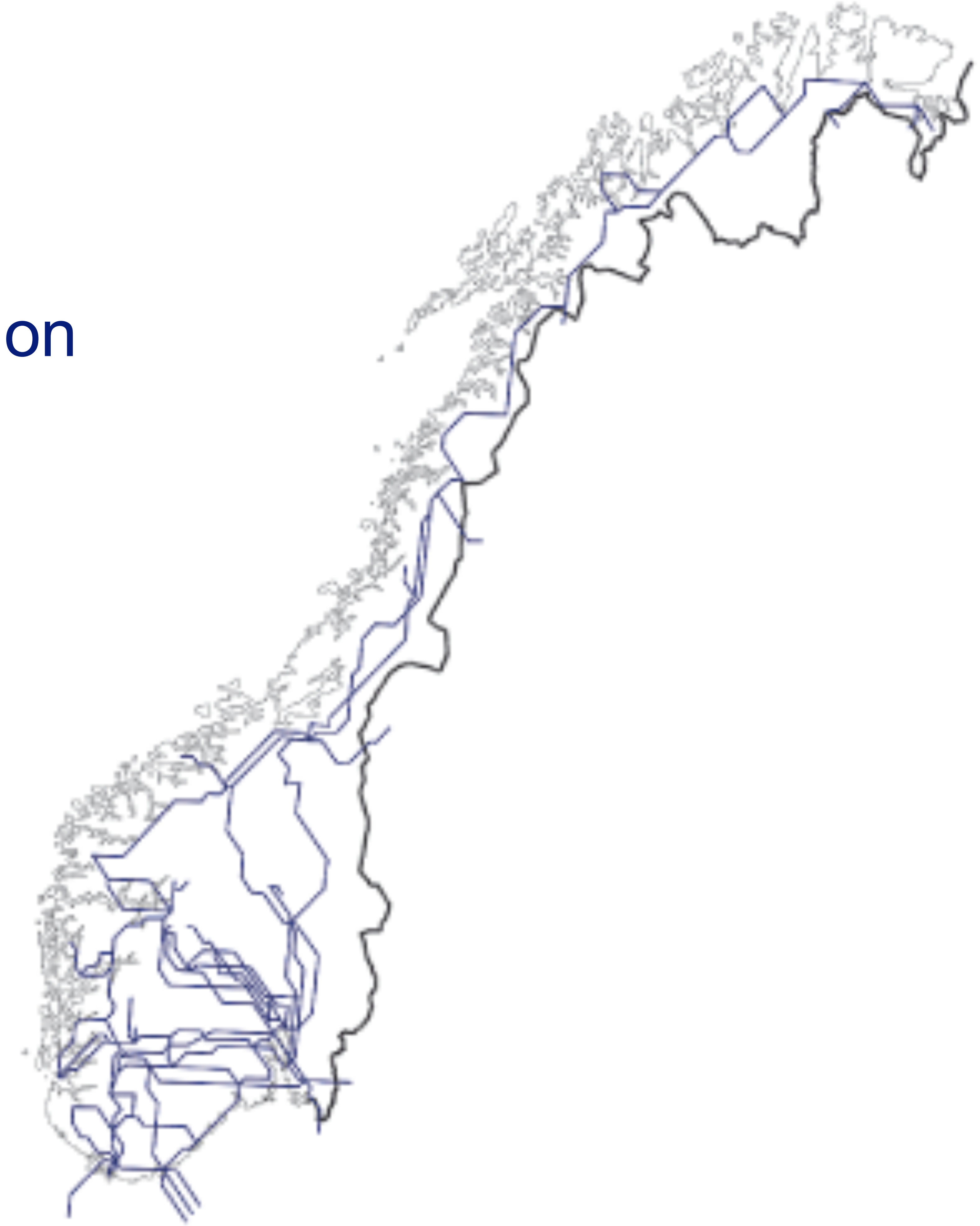
- Recap: the electric grid example
- The problem of QoS
- QoS in communication
- QoS in automation
- Intrinsic QoS
- Conversion, operating envelope
- Adaptation of the fault-tree to QoS requirements
- Applicability of Safety and the V-model
- Research efforts
- Conclusion

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
- Spreads from ”atomic” sensors to big data and exchange of information
- Good QoS example because of protection and supply stability



From: InGuardians, Inc.



The problem of QoS

- 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
- Works quite well.

- Automation: has requirements because of the physical connection
- Many requirements are only heritage from old times
- Are very much ”nothing” for an acceptably modern GE network

- QoS for the control loop
- QoS over the internet

QoS in communication

- Long tradition with high QoS neworks (SDH, PDH, traditional circuit switching)
- ATM has failed because of excessive cost
- Carrier Ethernet is the current choice of technology
- Overprovisioning works
- Diffserv-intserv
- In a multi-provider path, it is problematic to quarantee QoS
- Technologies are available, like MPLS – industrial problems are either related to cost or inability to identify requirements (and have higher cost because of that)

- Current status: we are trying to implement services, which made ATM expensive and fail, maybe this time it will be OK
- IEEE 802.1 TSN
- Typical metrics: bandwidth, delay, jitter, burstiness, redundancy

QoS in industry

- Connectivity
  - ➡ Direct wiring
  - ➡ Low speed serial buses
  - ➡ Ethernet
- Key in the local automation network
- Very fast reaction times
  - ➡ Motion control
  - ➡ Robotics
  - ➡ Substation automation
- Fast reaction times
  - ➡ Factory automation
- Slow reaction times
  - ➡ Process automation
- Upper levels are more a telco question
- Ethernet is everywhere
- Typical metrics: sampling frequency, delay, jitter, redundancy
- Time synchronization

! This is when engineering tries to convert their requirements into networking terms!

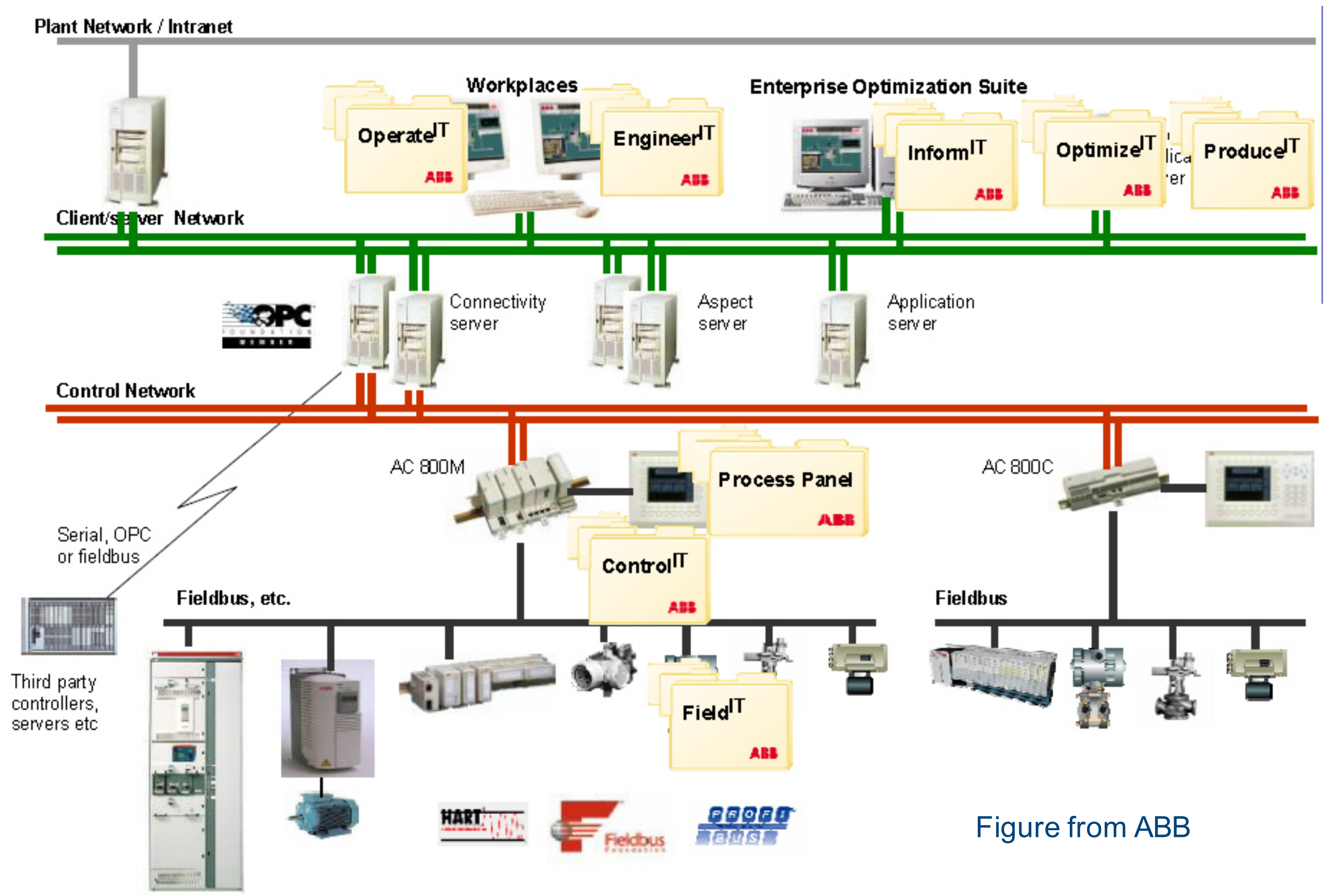
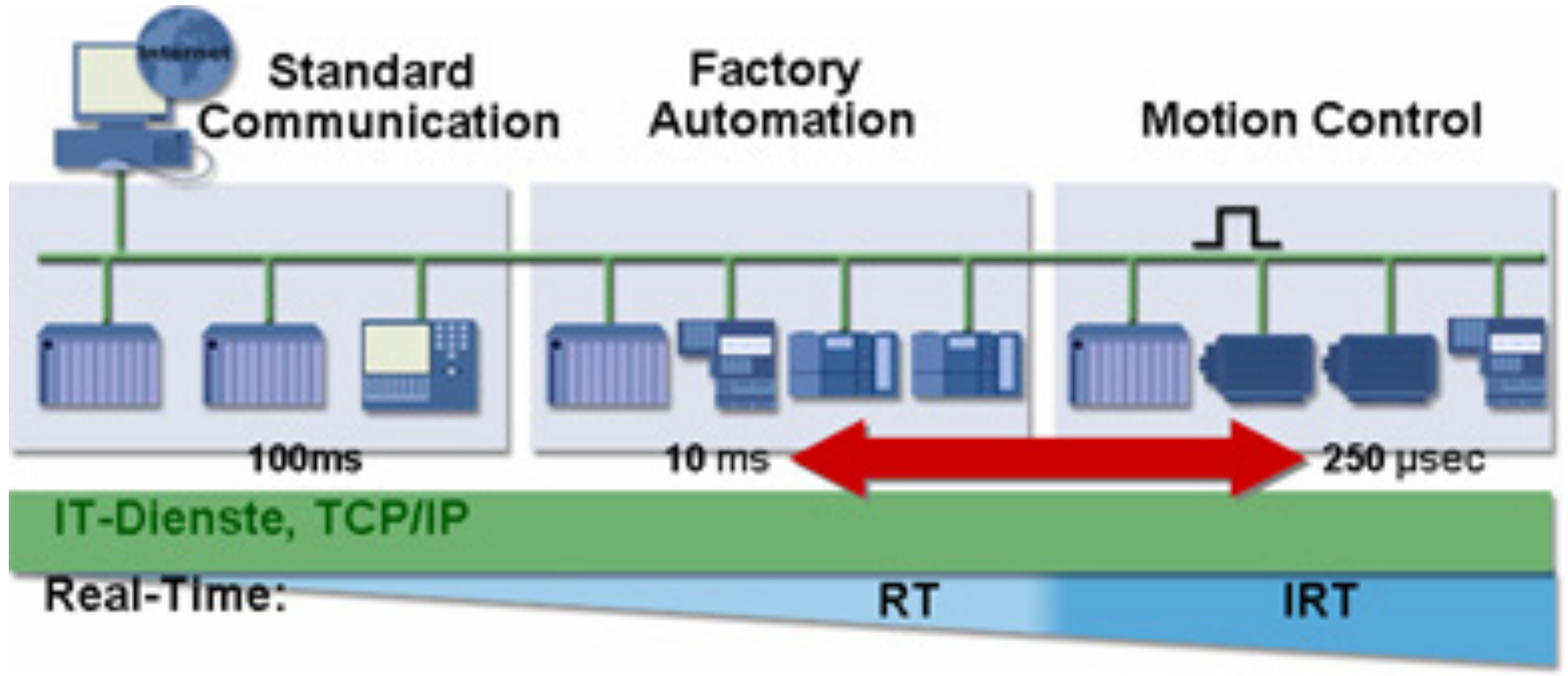


Figure from ABB

Intrinsic QoS

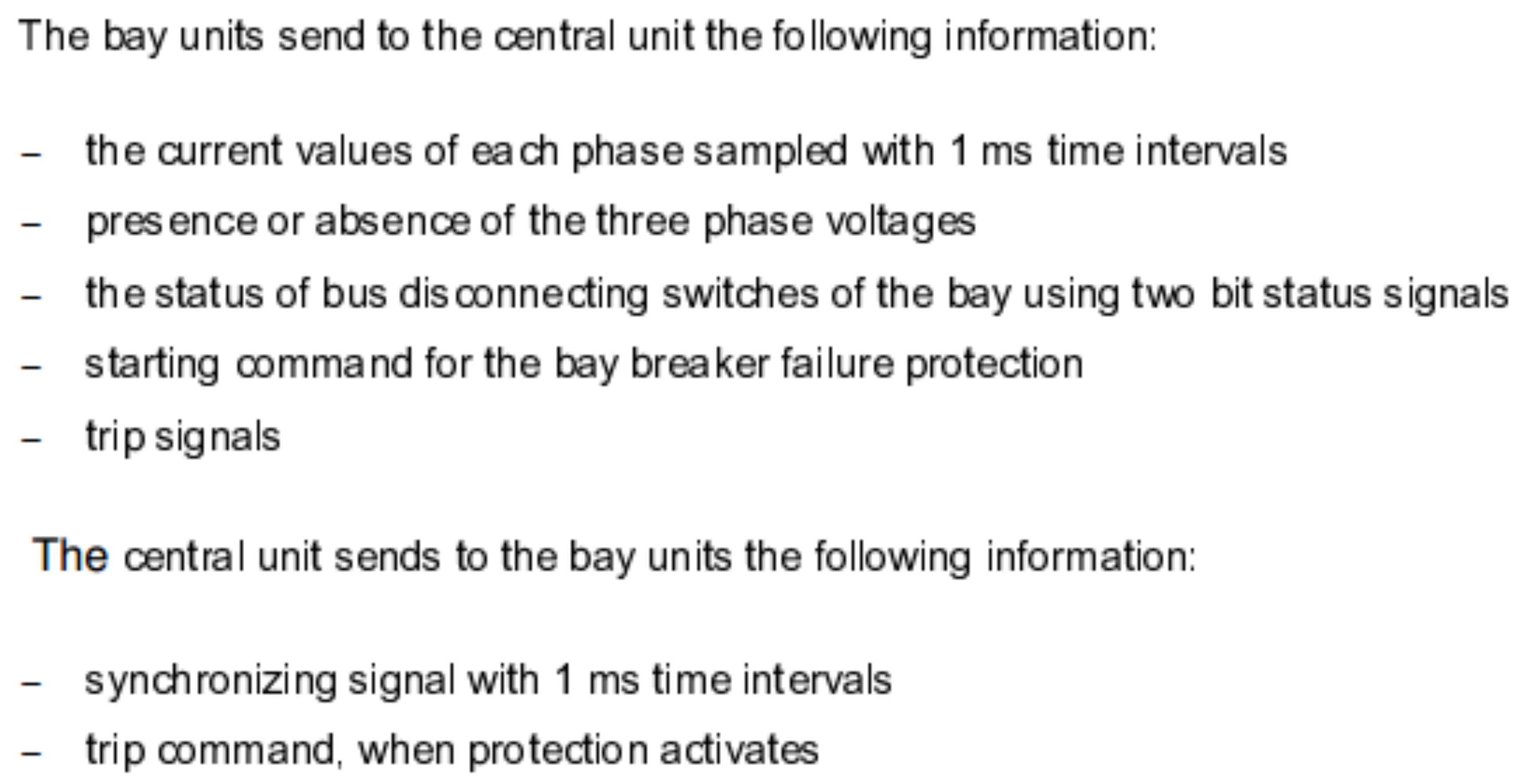
- Taking the most problematic part of the automation QoS
  - ➡ E.g. Profinet IRT or EtherCAT
- Relaxed QoS
  - ➡ Supervisory Control and Data Aquisition
  - ➡ Remote management
- High QoS
  - ➡ Electric grid
  - ➡ Electrified production platforms

High Performance for Harsh Environments.
The EtherCAT Box with IP 67 protection.
EtherCAT



Identifying QoS metrics in automation

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

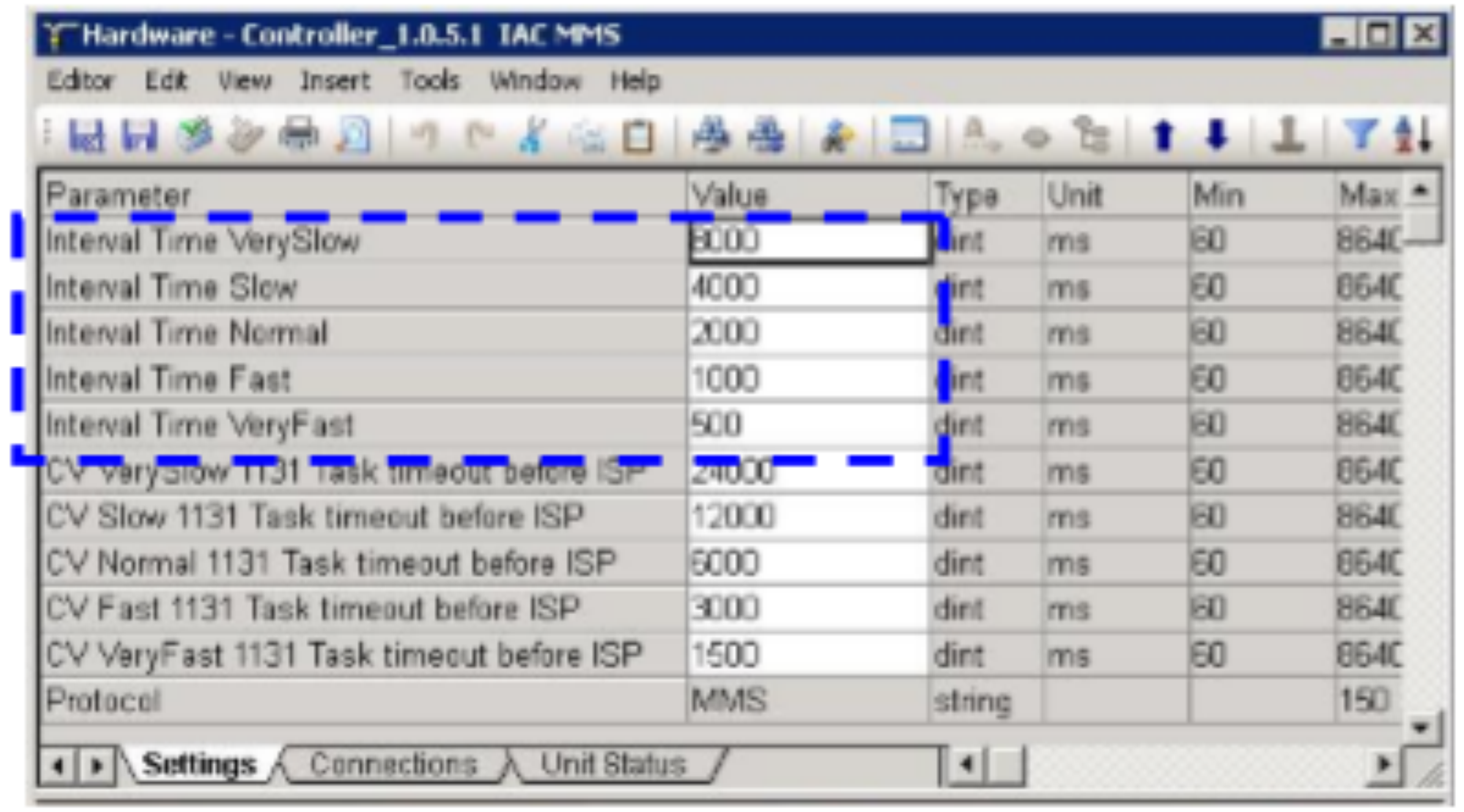


The bay units send to the central unit the following information:

- 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

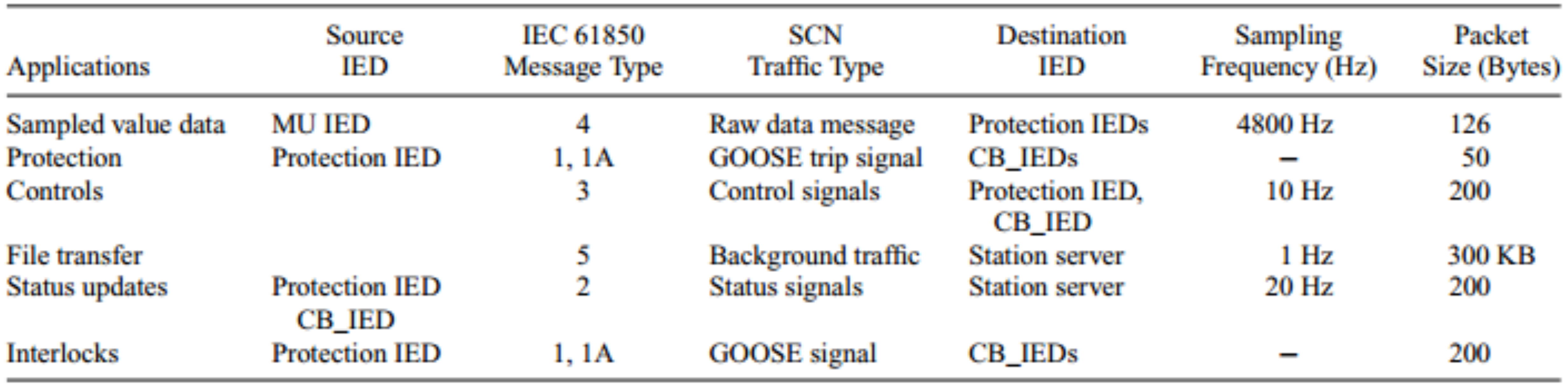
The central unit sends to the bay units the following information:

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



Hardware - Controller_1.0.5.1 IAC MMS
Editor Edit View Insert Tools Window Help
Settings
Connections
Unit Status

Parameter	Value	Type	Unit	Min	Max
Interval Time VerySlow	8000	dint	ms	60	8640
Interval Time Slow	4000	dint	ms	60	8640
Interval Time Normal	2000	dint	ms	60	8640
Interval Time Fast	1000	dint	ms	60	8640
Interval Time VeryFast	500	dint	ms	60	8640
CV VerySlow 1131 Task timeout before ISP	24000	dint	ms	60	8640
CV Slow 1131 Task timeout before ISP	12000	dint	ms	60	8640
CV Normal 1131 Task timeout before ISP	6000	dint	ms	60	8640
CV Fast 1131 Task timeout before ISP	3000	dint	ms	60	8640
CV VeryFast 1131 Task timeout before ISP	1500	dint	ms	60	8640
Protocol	MMS	string			150

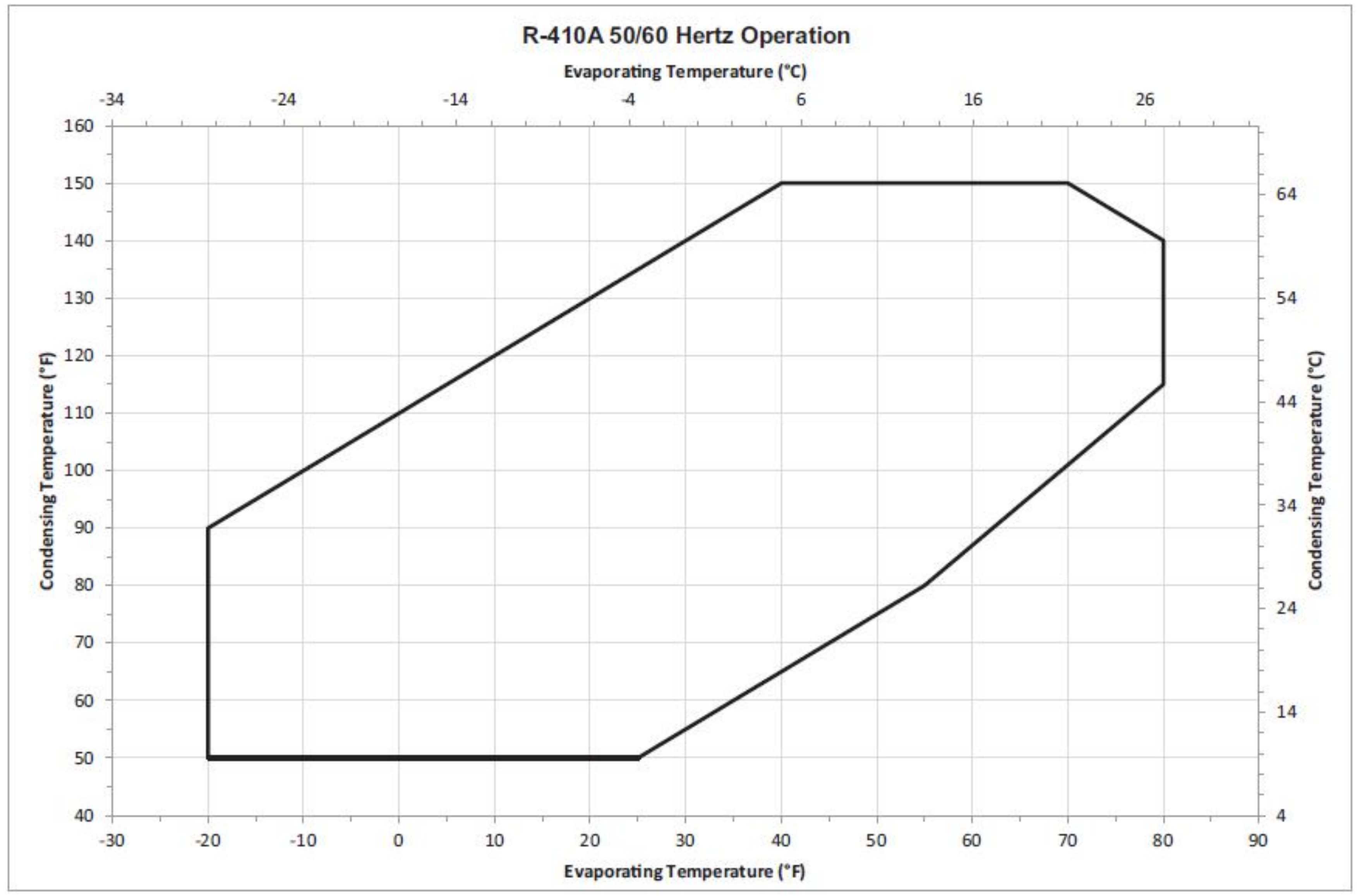


Applications	Source IED	IEC 61850 Message Type	SCN Traffic Type	Destination IED	Sampling Frequency (Hz)	Packet Size (Bytes)
Sampled value data	MU IED	4	Raw data message	Protection IEDs	4800 Hz	126
Protection	Protection IED	1, 1A	GOOSE trip signal	CB_IEDs	–	50
Controls		3	Control signals	Protection IED,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

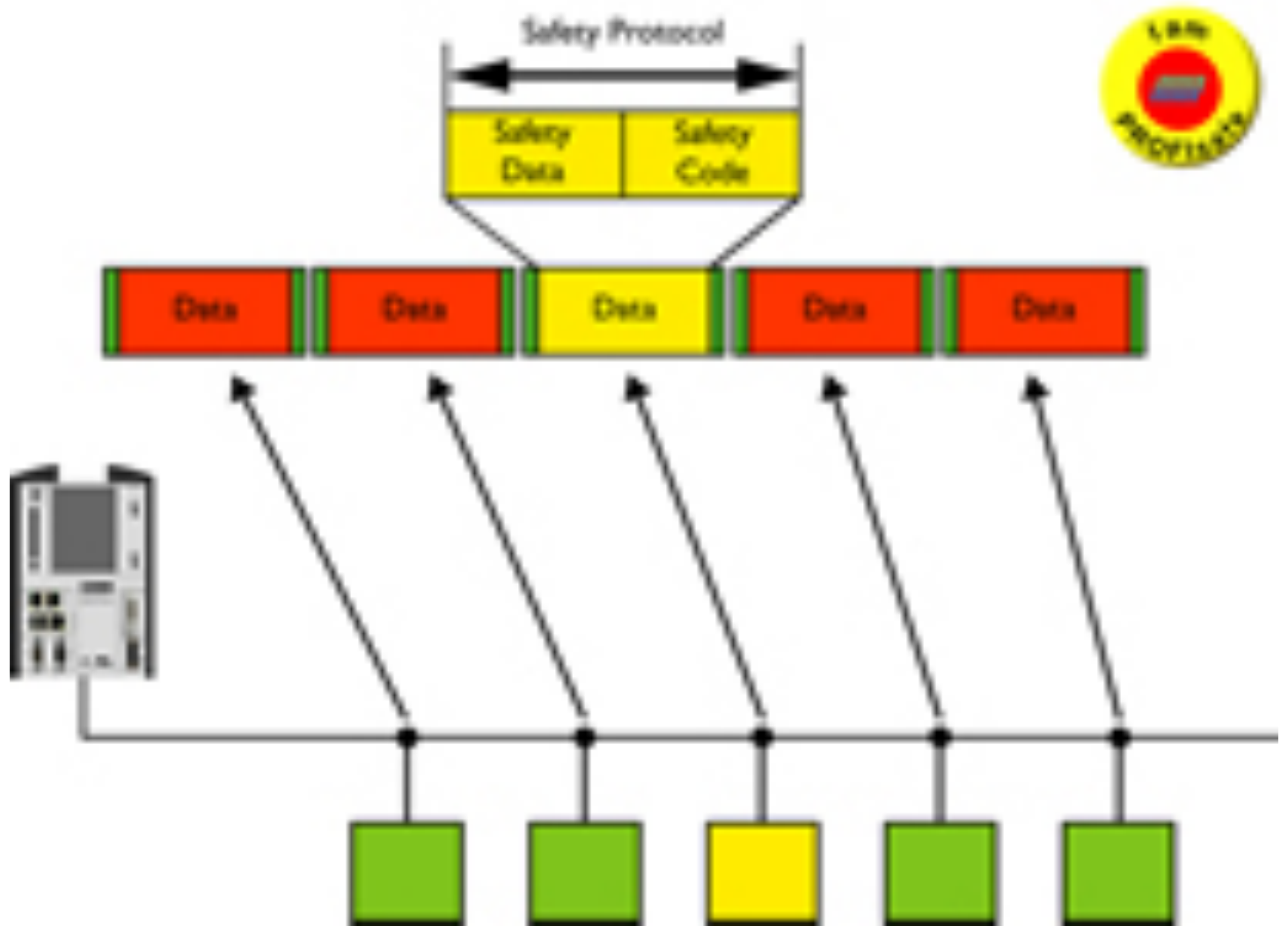
Conversion and operating envelope

- Operating envelope: the operational parameters where our network can work “well”, depends on the technology and on the task
- For traffic estimation we need it in ”communication” QoS
  - ➡ Bandwidth, delay, jitter, (redundancy)
- Often can be done with simple arithmetic with a certain confidence level



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

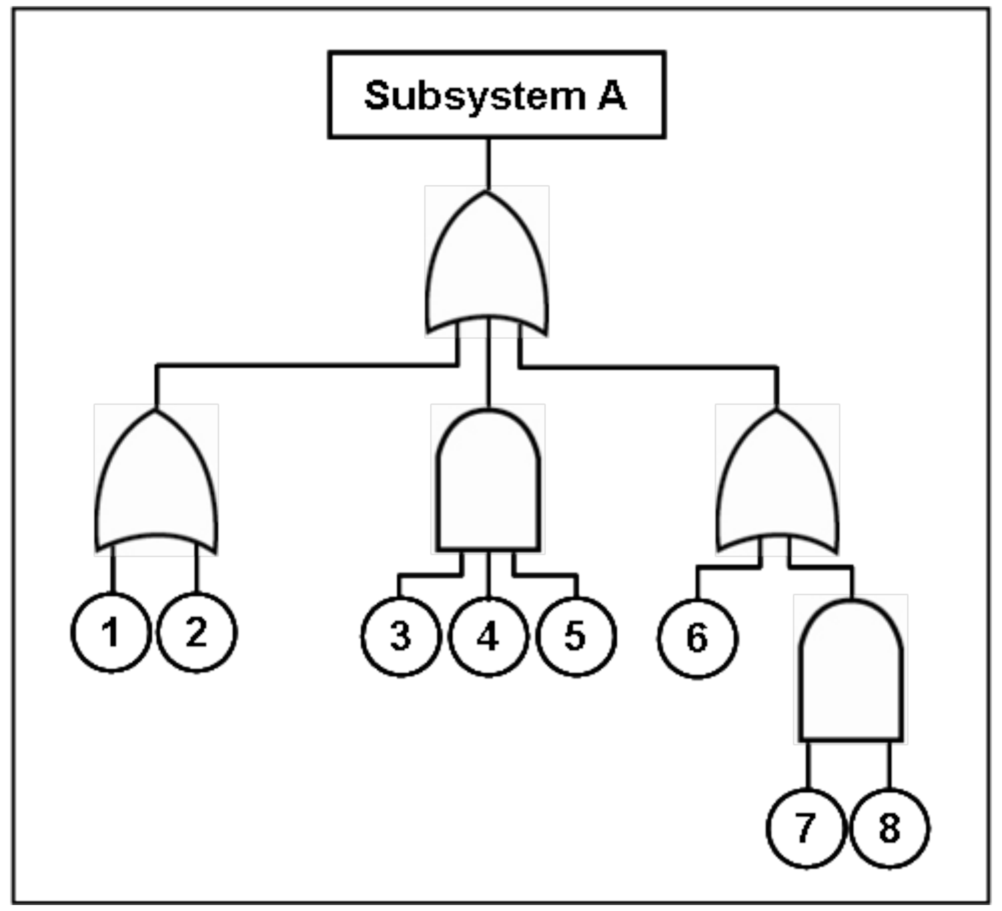
- Connected because security threats are resulting in safety threats, which have to be mitigated
- Different fields but approaching similar problems
- The process behind is completely different: safety deals with a static statistical process, while security problems are the result of an active, changing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

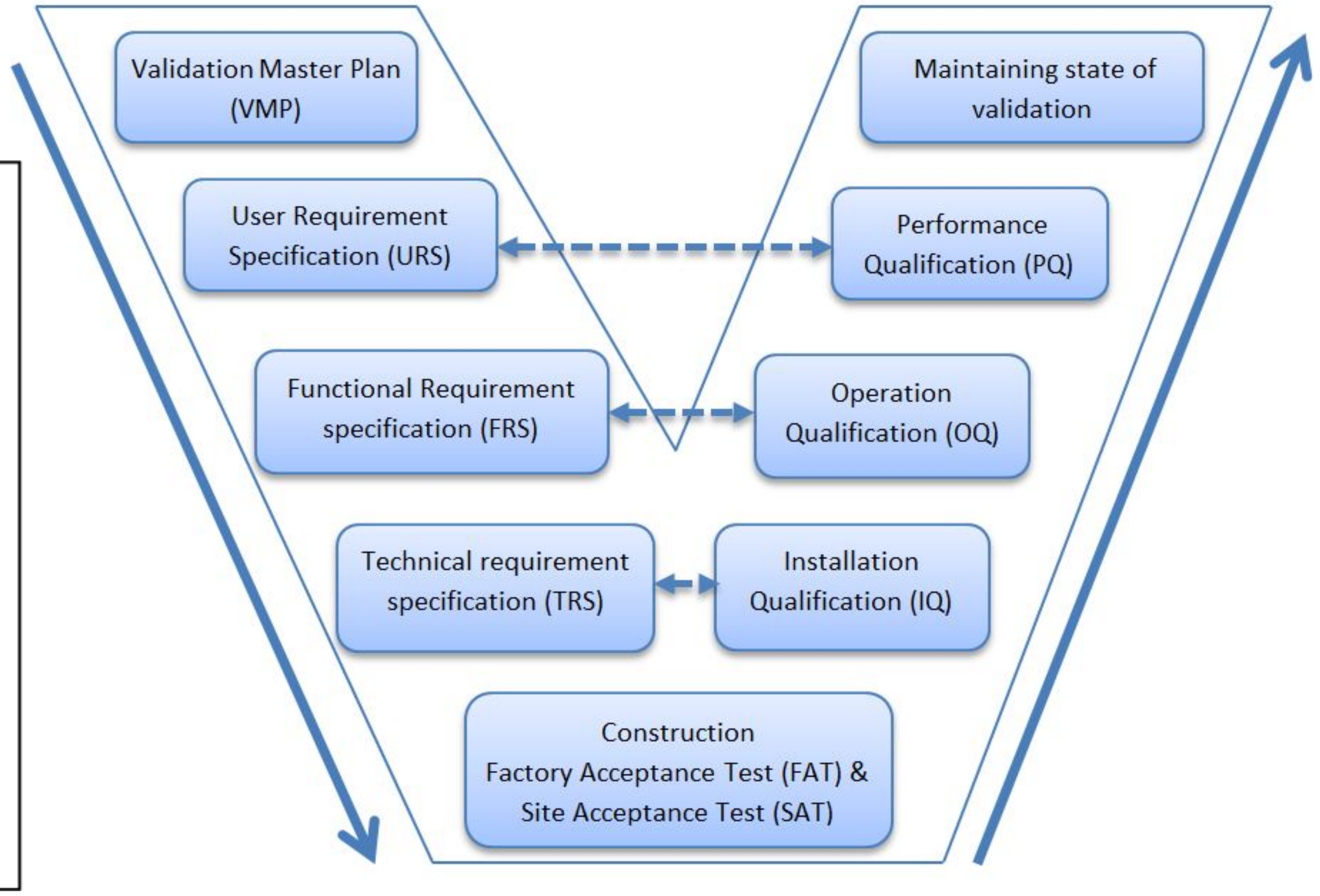
- Stopping somebody to do something to avoid damage
- Even if something has happened, avoid or limit damage

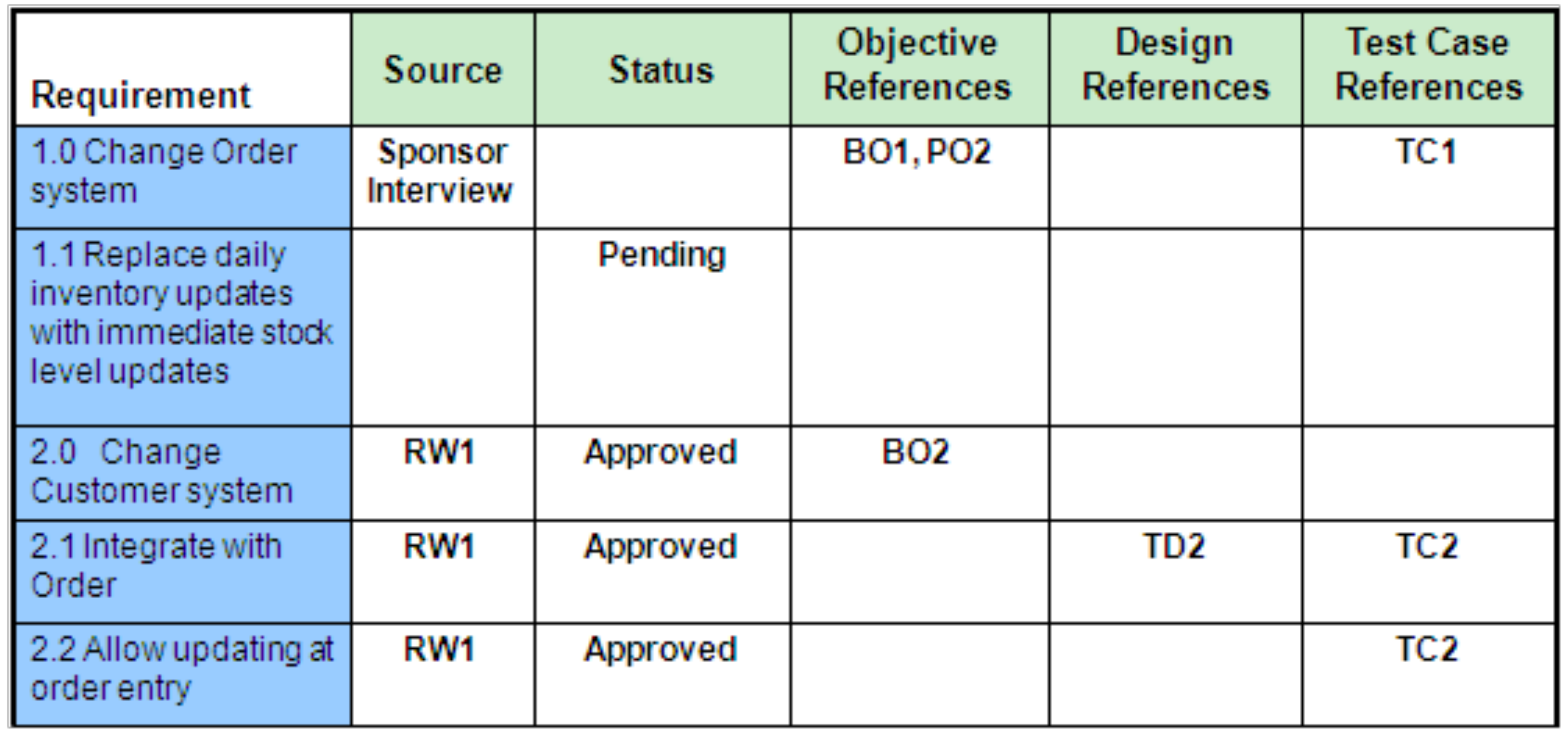
- Cyber-physical interactions
- IT security is not covering this field
- Safety is focusing on the physical interactions
- Safety is using extensive diagnostics to check itself
- Timescale of protection and data validity

Following up requirements

- One of the steps which typically are left out
- Results in: ”time sync precision requirement of 10us” Why? – nobody knows.
- I see (again) the safety workflow as the one where we could get some inspiration from:




Validation Master Plan (VMP)
Maintaining state of validation
User Requirement Specification (URS)
Performance Qualification (PQ)
Functional Requirement specification (FRS)
Operation Qualification (OQ)
Technical requirement specification (TRS)
Installation Qualification (IQ)
Construction
Factory Acceptance Test (FAT) &
Site Acceptance Test (SAT)



Requirement	Source	Status	Objective References	Design References	Test Case References
1.0 Change Order system	Sponsor Interview		BO1, PO2		TC1
1.1 Replace daily inventory updates with immediate stock level updates		Pending			
2.0 Change Customer system	RW1	Approved	BO2		
2.1 Integrate with Order	RW1	Approved		TD2	TC2
2.2 Allow updating at order entry	RW1	Approved			TC2

http://www.kaboomlatam.com/novosite/requirements-traceability-matrix-examples-815.png

L5 Conclusions

- Services in IoT have an implication typically in the communication and security domain of IT
- The QoS requirements are more ”hard” than in non-automation cases
- The metrics used at OT and at IT do differ, but with some reason we can convert them
- Big systems require a standardized, structured approach for planning infrastructure services
- Following up requirements is important as:
  - Unnecessary requirements might lead to either not feasible projects or higher cost
  - Necessary requirements shall be taken into account (and only those)
  - Following aggregated resource usage in the infrastructure is important
- Non-functional requirements are less typical in M2M systems