Innovations & LiveLab

IT Digital Grids

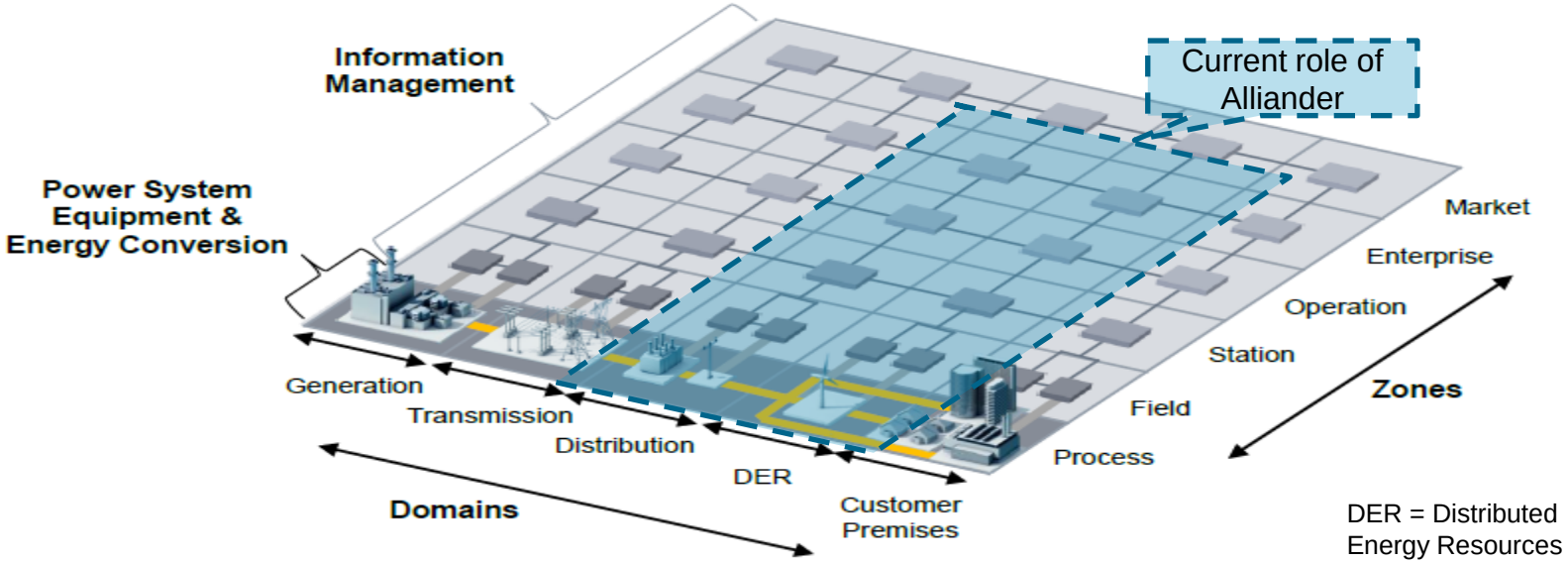
Roelof Klein

The connected utility

Liander LiveLab

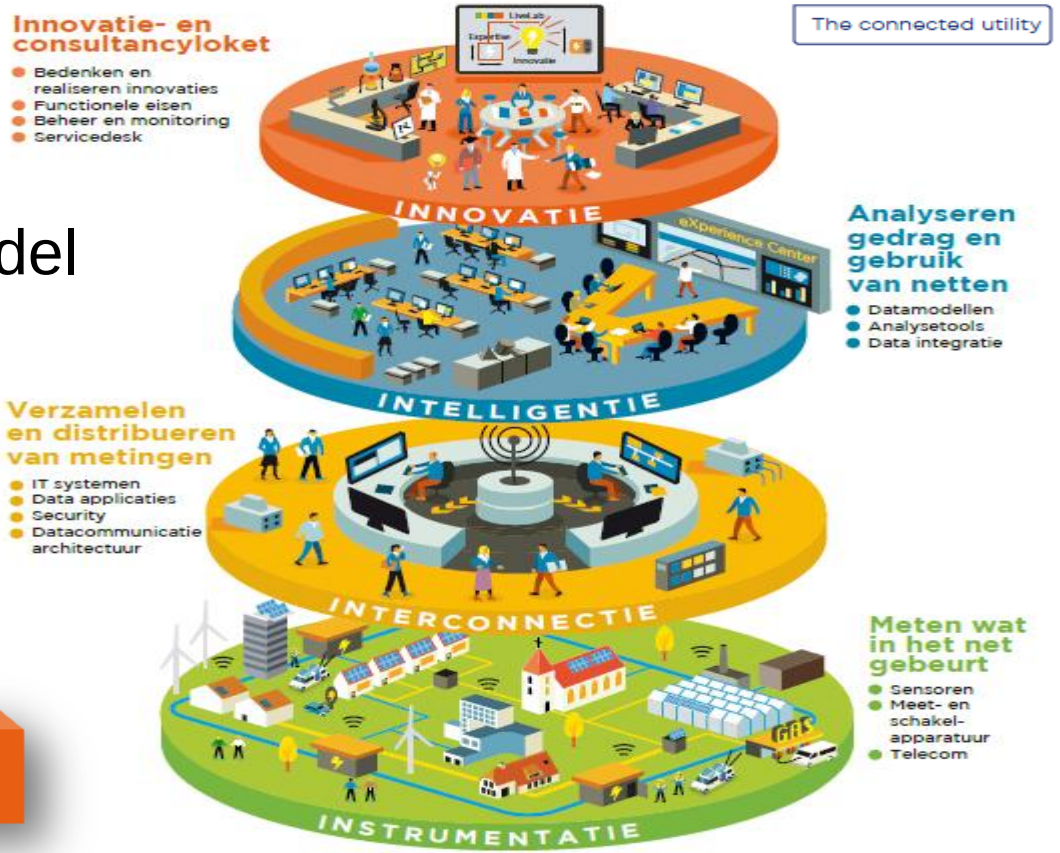
Overview Smart Grid & Alliander

Overview of the Smart Grid arena defined by IEC 62357 and the role of Liander as distribution grid operator. The previous role was a focus on transmission and customer meter reading.



The LiveLab platform

LiveLab Innovation model
Digital Grids

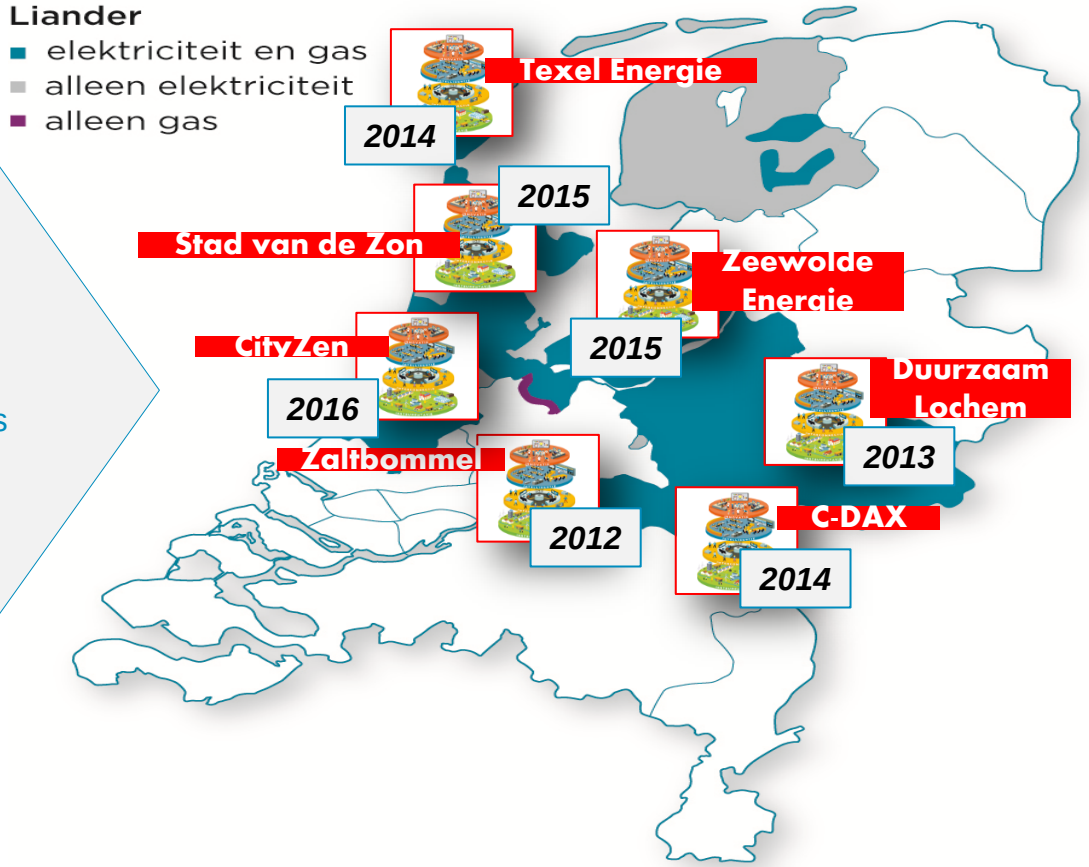


Liander LiveLab

LiveLab platform for testing new energy concepts

Added Value

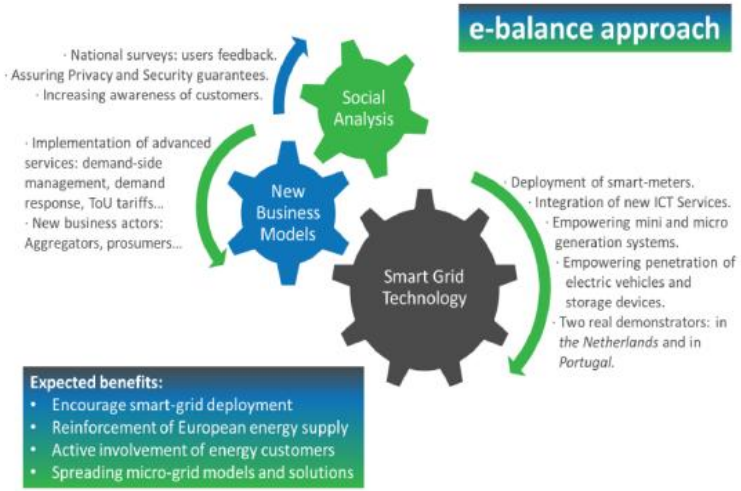
- Applicable and scalable to operational processes
- Asset management & IT Policies
- Standardization & security data chains
- Fast & Efficient implements of data chains
- Strong base of expertise, infrastructure and organization
- Gathering functional requirements for testing & acceptation
- Synergy in projects



E-Balance (as an example)

http://www.e-balance-project.eu/

- ICT solutions
- In order to achieve the project goals it is necessary to develop new ICT solutions and to integrate them with those already existing in the energy grid area. The e-balance approach is a hierarchic distributed system consisting of multiple computing units (energy management units) deployed within the energy grid to monitor the parameters of the grid and to trigger actions that influence its working. Our solution covers:
- Reliable communication technologies
- Reliable data exchange middleware
- Efficient data processing algorithms
- Support for security and privacy
- https://www.linkedin.com/company/e-balance-project



E-Balance Bronsbergen

Invertors / Electronics

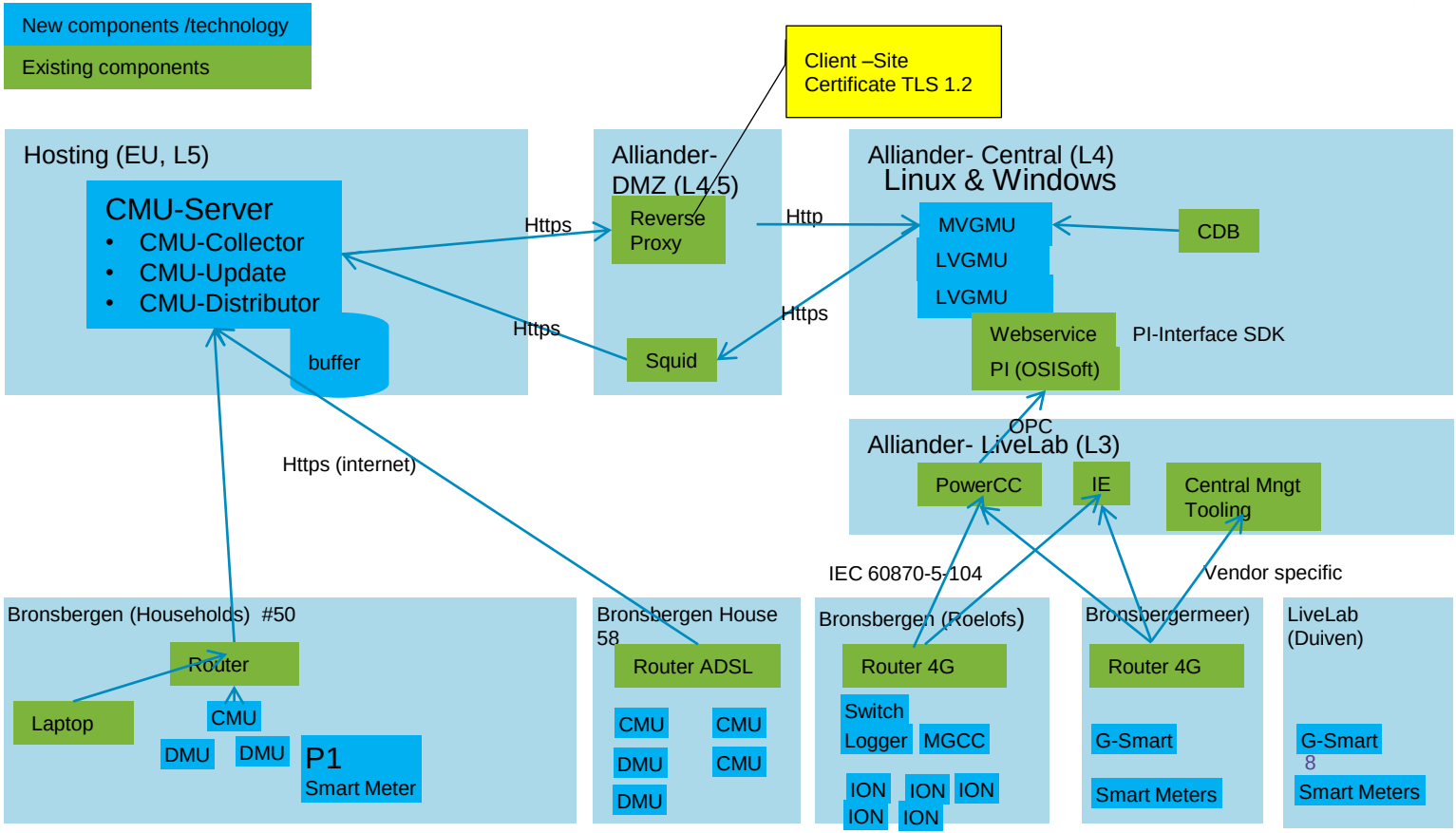
Solar Panels

Typical House

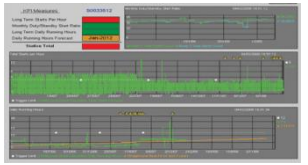
Batteries

ION meters

E-Balance architecture (simplified)



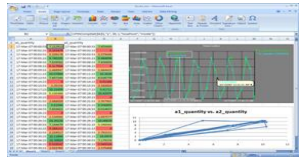
Simplified data chain LiveLab



Sensors → RTU → GPRS / CDMA Modem → Telecom provider → Firewall IT → Firewall IOT → Historical Database → Office users

Firewall IOT → Device Managers

Firewall IOT → DMS / SCADA

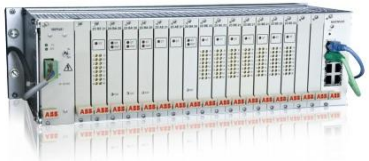


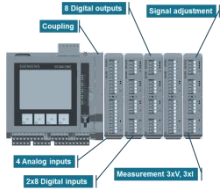
Communication standards LiveLab (only IP communication)

- IEC 61850 / IEC 60870-5-104 / Modbus/TCP (data)
- NTP, HTTP(s), SSH, SNMP, LDAP, Radius (IT Services)

Youtube

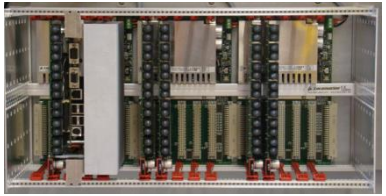
OT Devices in the field





Many vendors

- Some have IPsec (encryption)
- Some have IEC 61850-3 (hardware robustness)
- Some have SNMP
- Some have certificates



LiveLab in numbers

System	#
Wireless routers (GPRS)	74
Wireless routers (4G)	15
Wireless routers CDMA	8
RTU’s	150
Linux servers	4
Windows servers (OT)	12
Windows servers (IT)	20

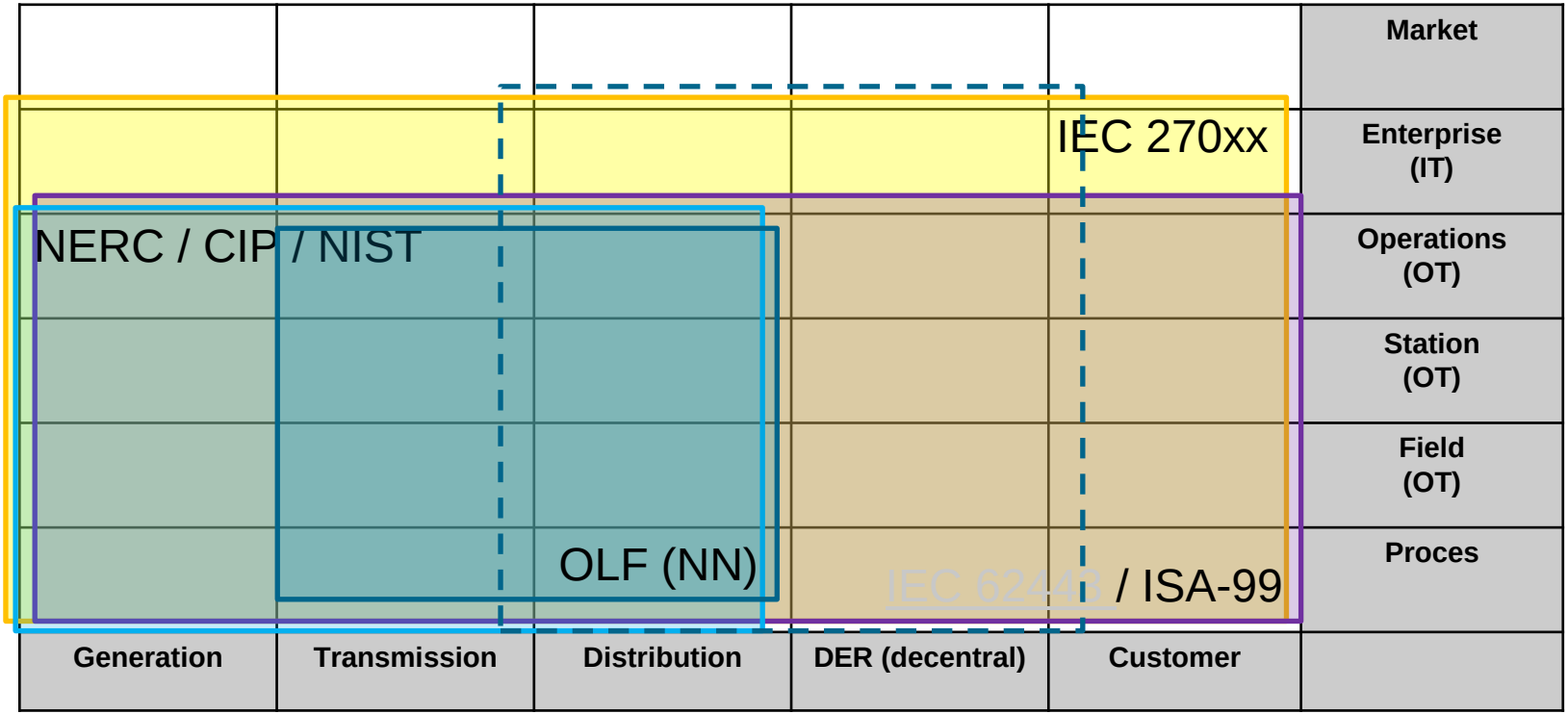
Cyber security risks to be mitigated

List of the highest cyber security risks (substation):

- Access to the central systems from a substations
- Access from one substation to another substation
- DoS attack from a substation
- Installing RAT (remote access tooling) on a substation to access the central systems
- Software changes on a substation that are not authorized
- Changes in Authorization / Authentication that are not authorized
- Switch off / on , reboot, modify of equipment on a substation without a recorded change or incident
- Installation of new equipment not managed by the change process
- Replacement of equipment by other equipment @ the same IP-address

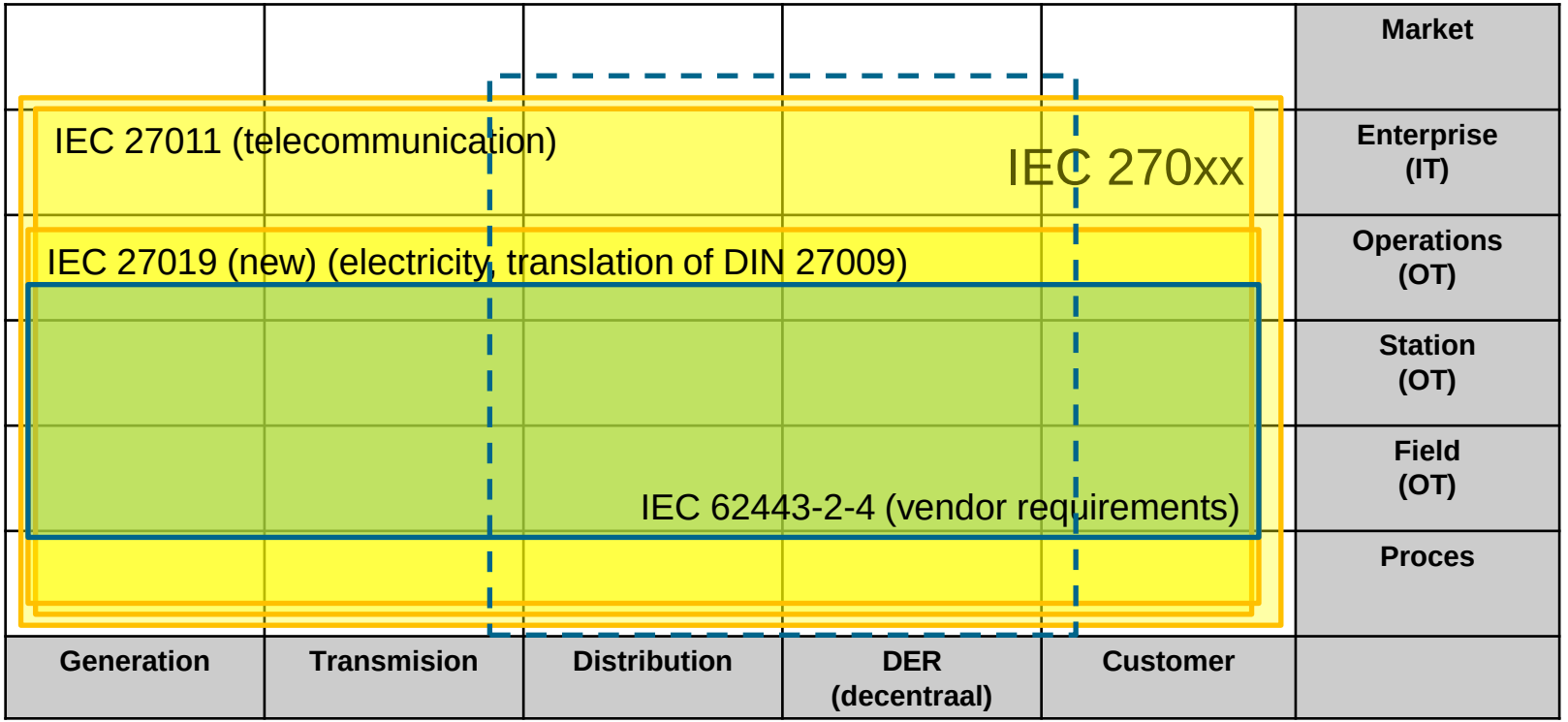
Security standards (Organization)

Most of standards are not suitable for the new role of Alliander, most standards do not cover the whole arena.



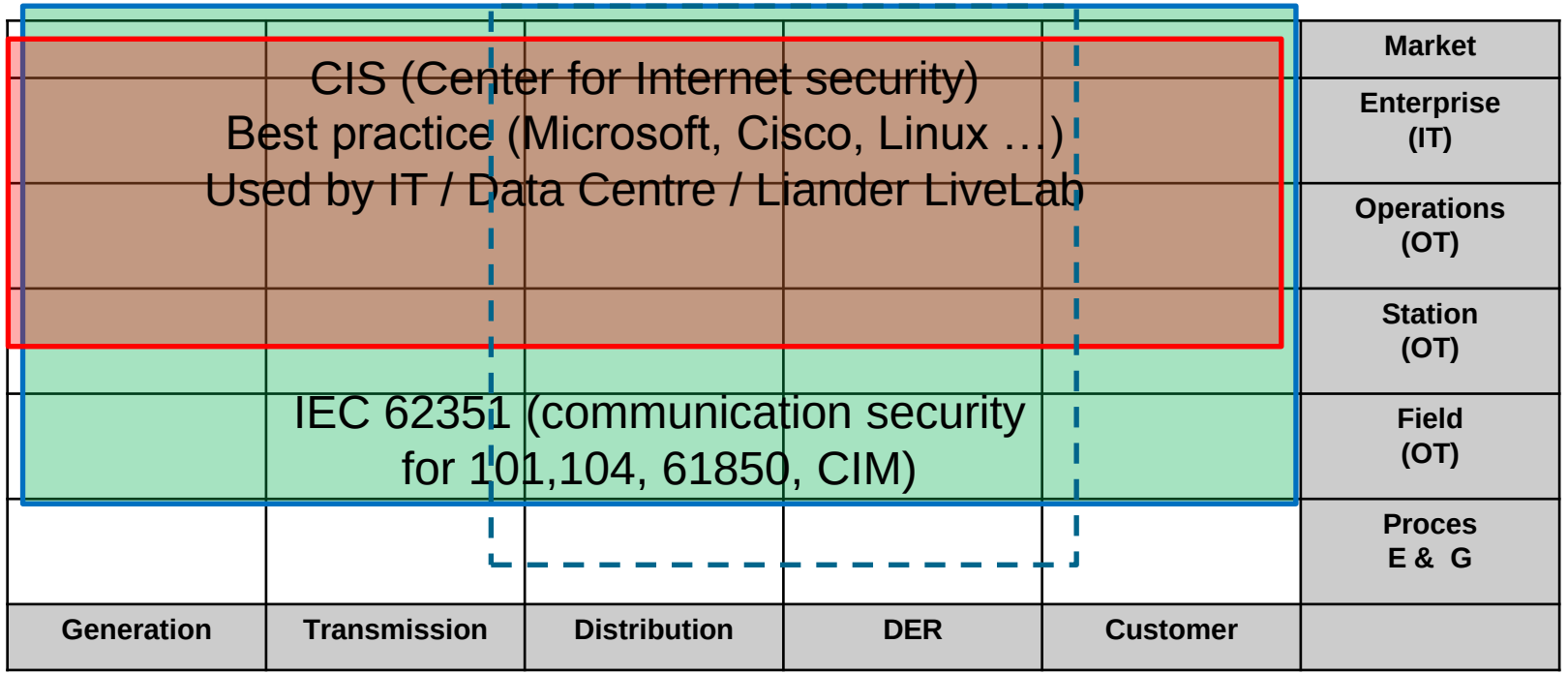
Organizational security

preferred standards: IEC 27002, 27011,27019, 62443-2-4



Technical implementation of security

(patches, passwords, anti-virus, hardening, access, encryption …)



Defence in Depth

Defence in depth is only possible when IT and OT work closely together

LL = LiveLab/OT , SP = Service Provider (external)

	RTU	Modem	Wireless transmission	Firewalls	Netwerk equipment	Servers	Workplaces & mobile devices
Hardware robustness	LL	LL	SP	IT	IT	IT	IT
Hardening of systems /malware	LL	LL	SP	IT	IT	LL/IT	IT
Patch Management	LL	LL	SP	IT	IT	LL/IT	IT
Anti Virus management	LL		SP			IT	IT
Monitoring of systems / logging	LL/IT	LL/IT	SP	IT	IT	IT/LL	IT
Backup and restore	LL	LL	SP	IT	IT	IT	IT
Network segments with limited interaction		LL/IT	SP	IT/LL	IT/LL	IT	
Controlled remote access / user management	LL	LL	SP	IT/LL	IT/LL	LL/IT	LL/IT
Time management	LL	LL	SP	IT	IT	IT	IT
Encryption / certificates	LL/IT	LL/IT	SP	IT	IT	IT/LL	IT
File transfer Internet <-> IT <-> OT				IT/LL		IT/LL	IT

Guidelines / standards for OT

Defence	Standard
Hardware robustness	IEC 61850-3
Hardening of systems	IEC 62443-2-4 / CIS / IEC 27019 / Wurldtech
Patch management	IEC 62443-2-4 / CIS / IEC 27019
Anti Virus management	IEC 62443-2-4 / CIS / IEC 27019
Monitoring of systems	SNMP / ICMP / IEC 27019 / syslog, application log (not standarized)
Backup and restore	IEC 62443-2-4 / CIS / IEC 27019
Network segments with limited interaction	IEC 62351 -10 / IEC 27019
Controlled remote access / user management	IEC 62351 -10 / Windows A/D / Citrix / LDAP / RADIUS / IEC 27019 / SSH
Time management	NTP / PTP / GPS
Encryption / certificates	IEC 62351 / IPsec
File transfer Internet <-> IT <-> OT	IEC 62351 -10

File transfer Internet <-> IT <-> OT

The biggest risk in the OT environment is the USB stick & Internet file downloading:

- https://en.wikipedia.org/wiki/Stuxnet

The solution is to make a File Transfer system between IT and OT

No vendor is allowed to place files on a system directly

Close cooperation with the IT department is required

IT systems protection (data center)

Added value of IT for cyber security

- All the servers are installed in well protected data centers (logical en physical)

Current situation @ Livelab

- All the servers are fully managed (monitoring, backup, patch management….)

Lessons learned

- Special treatment is needed for these servers.
- The security knowledge of vendors of systems is less then the IT department (specialism of IT).
- Close cooperation with vendors is required to implement security.
- Security of 3rd party software (used in SCADA systems)

Lessons learned

- Close cooperation with the IT department is required. (@Alliander OT LiveLab and IT are now part of the same IT organization.
- Just do it (Patch Management, Anti Virus Management, Monitoring, ID Management and others are required, so why wait).
- Vendors are also interested in what we are doing and want to cooperate (Siemens, Remsdaq, WAGO, Bachmann, Phoenix, PowerSense …..).
- Active support from employees and staff is needed.
- We have not seen a failure of systems by implementing security.
- It is not just another IT department (focus on Business).

Expert knowledge and innovation for a digital grid