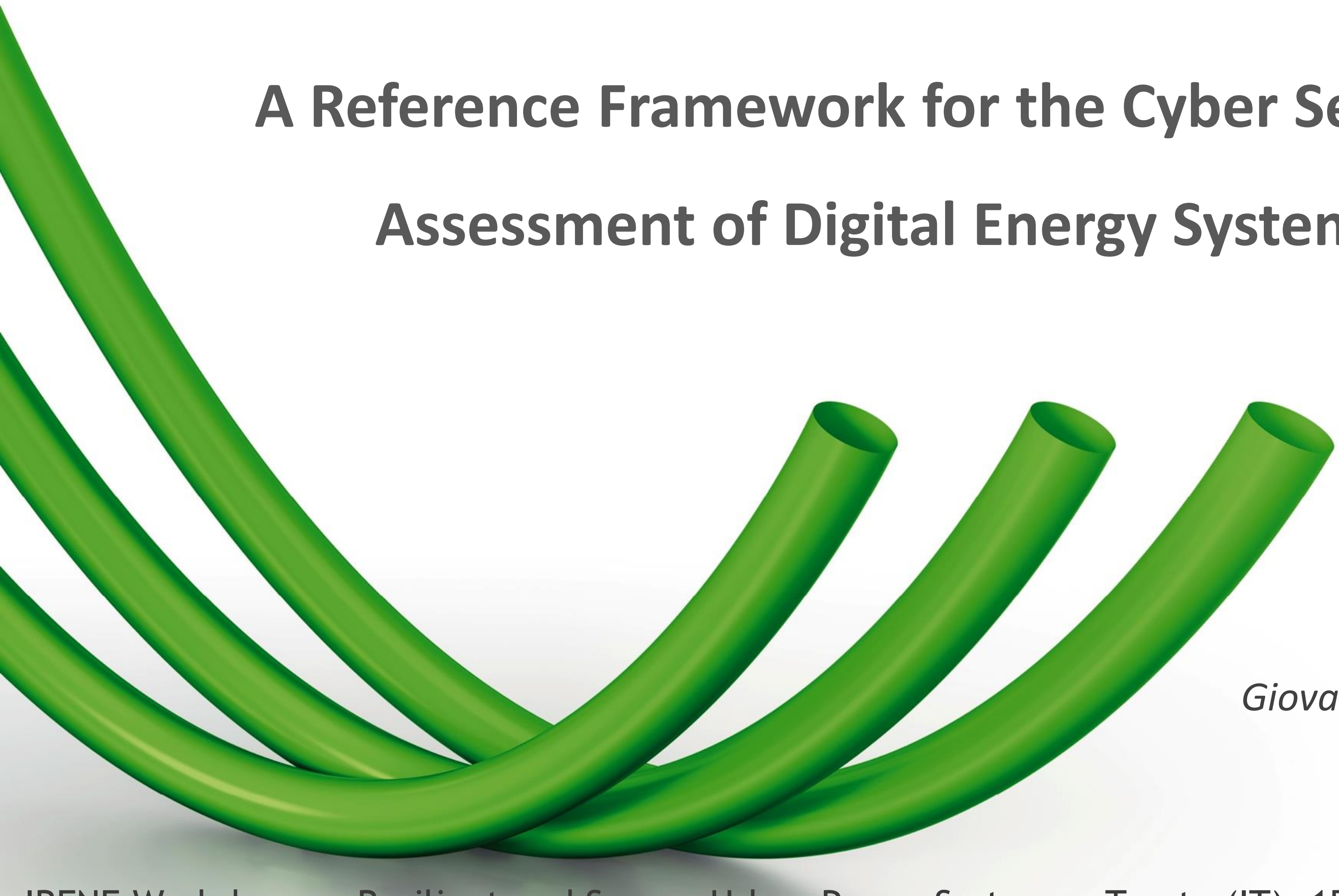
A Reference Framework for the Cyber Security Assessment of Digital Energy Systems



Giovanna Dondossola

IRENE Workshop on Resilient and Secure Urban Power Systems - Trento (IT), 15/09/2016

What RSE does

Applied research on the electro-energetic sector, experimental activities including **Cyber Security** experimental assessment

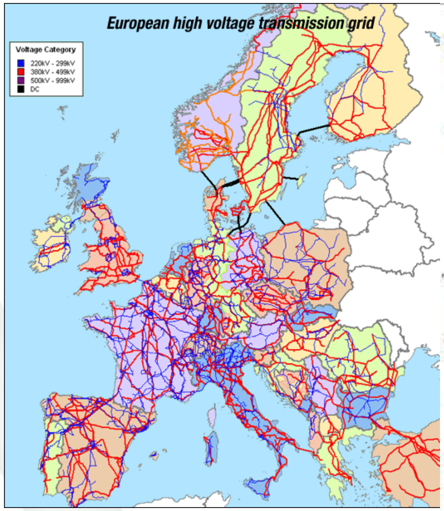
Agenda

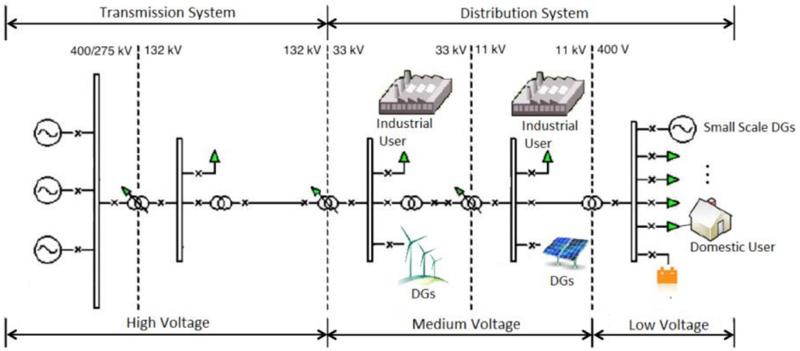
- Framework introduction
- Security design process
  - Methods
  - Tools
  - Standards

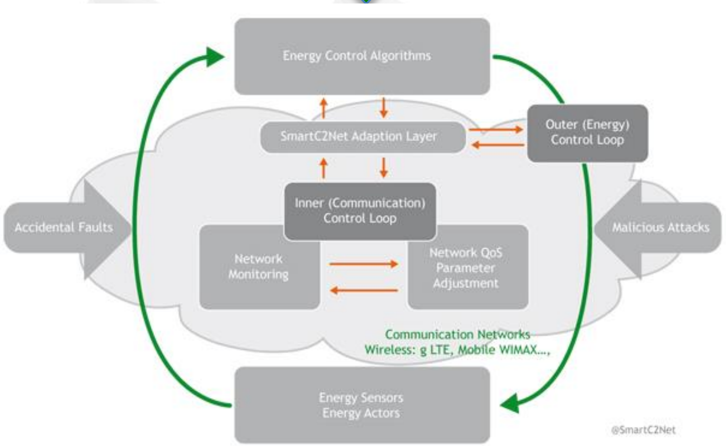
- Realistic scenarios
- QoS indicators

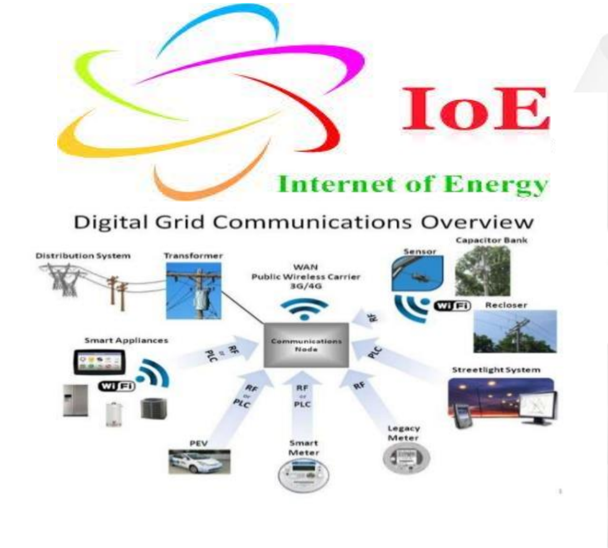
- Lab experiments

Energy Cyber Security – why

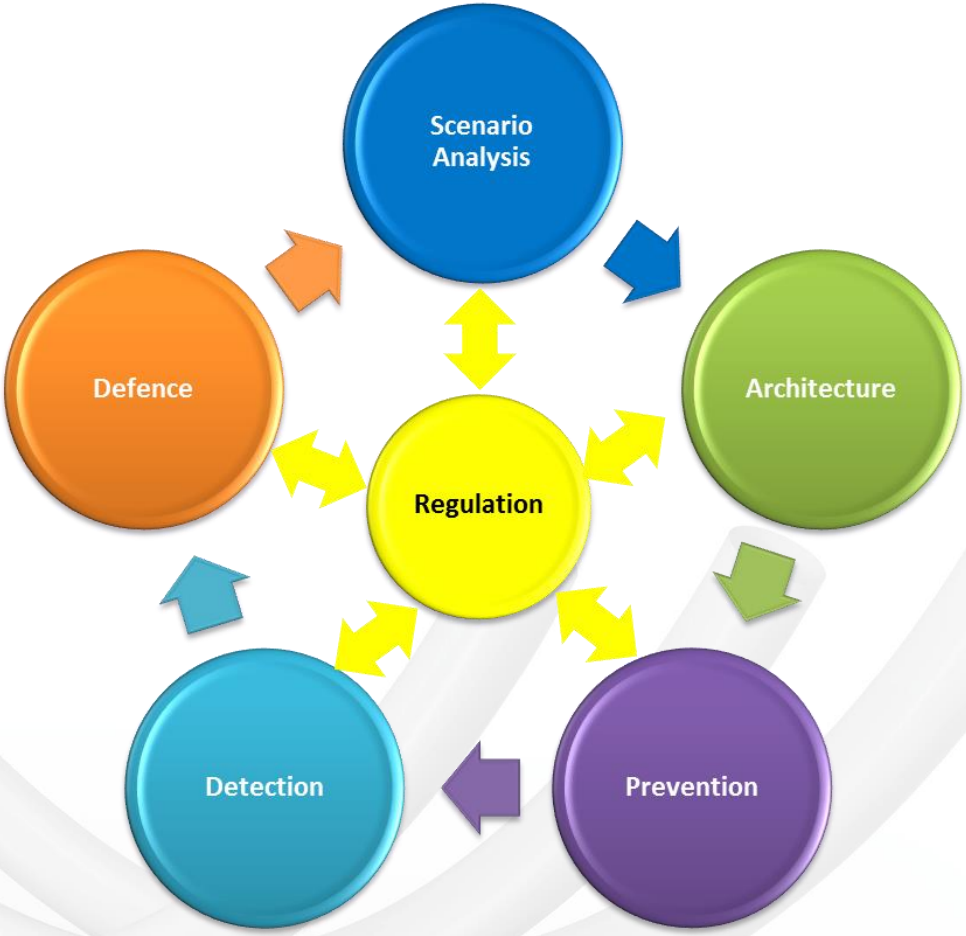




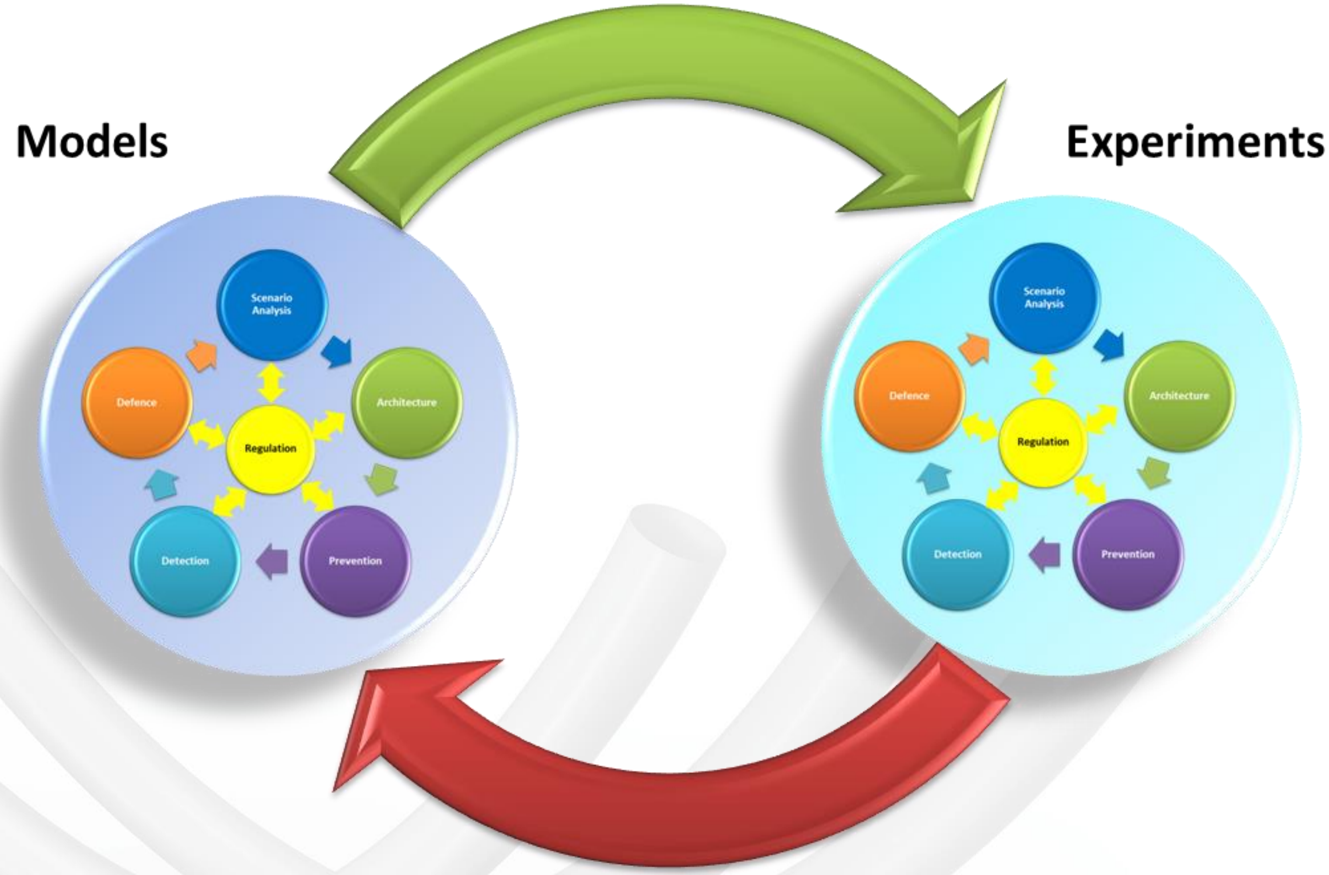

Energy Control Algorithms
SmartC2Net Adaption Layer
Outer (Energy) Control Loop
Inner (Communication) Control Loop
Accidental Faults
Malicious Attacks
Network Monitoring
Network QoS Parameter Adjustment
Communication Networks
Wireless: g LTE, Mobile WIMAX...,
Energy Sensors
Energy Actors
@SmartC2Net



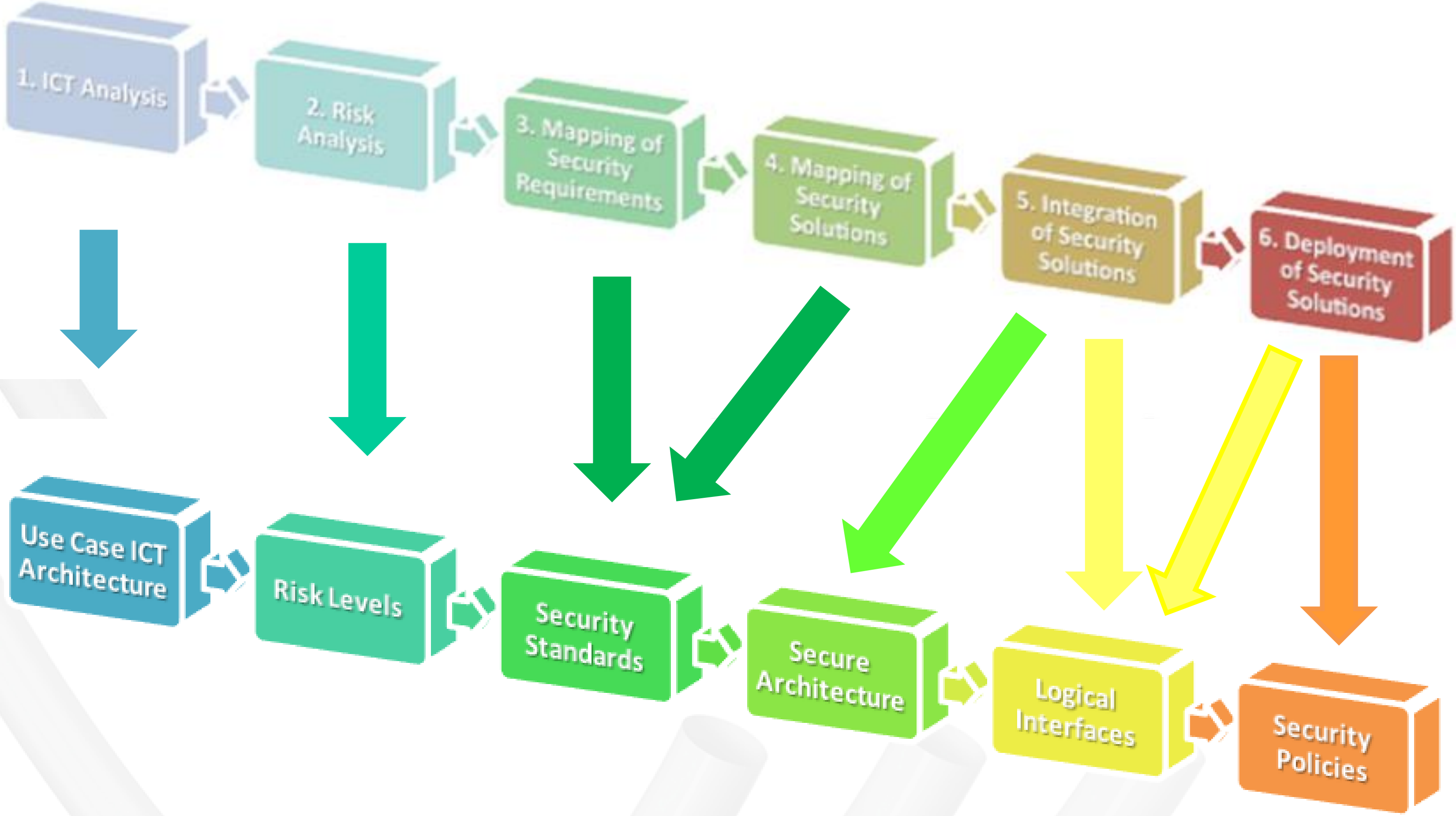
Cyber Security Framework



Cyber Security Framework (cont.)



Security Process


1. ICT Analysis
2. Risk Analysis
3. Mapping of Security Requirements
4. Mapping of Security Solutions
5. Integration of Security Solutions
6. Deployment of Security Solutions
Use Case ICT Architecture
Risk Levels
Security Standards
Secure Architecture
Logical Interfaces
Security Policies

Background knowledge

CEN/CENELEC/ETSI

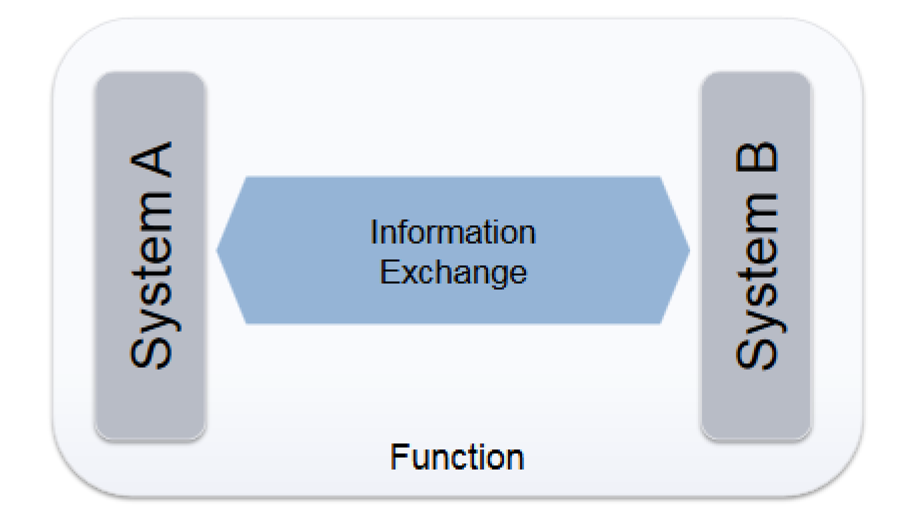
- Smart Grid Coordination Group
- European Mandate M/490 on Smart Grid Standardization

Methods

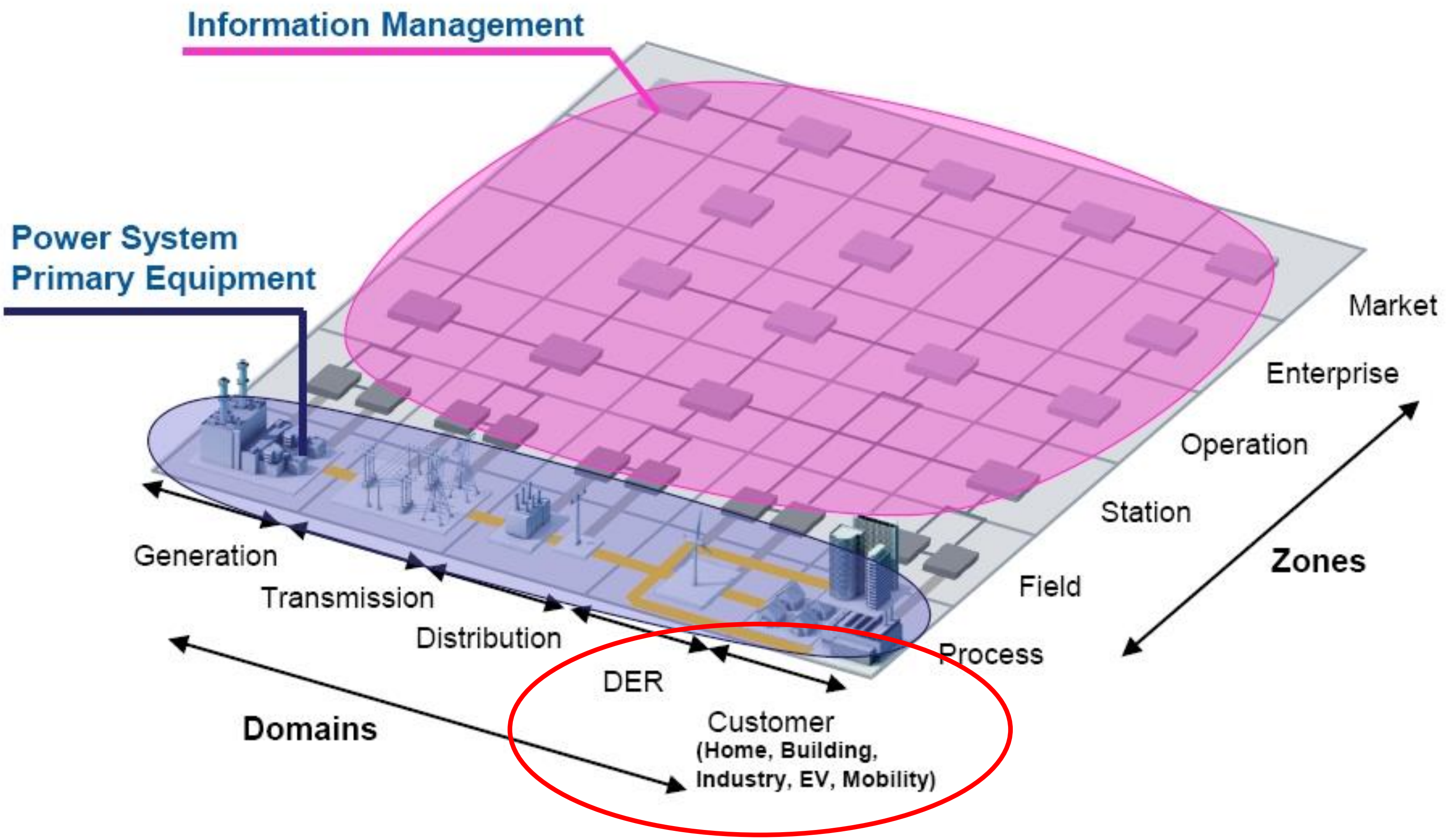
- Use Case Template
- SGAM Architecture and Toolbox
- Set of Standards
- Security Toolbox

Interoperability

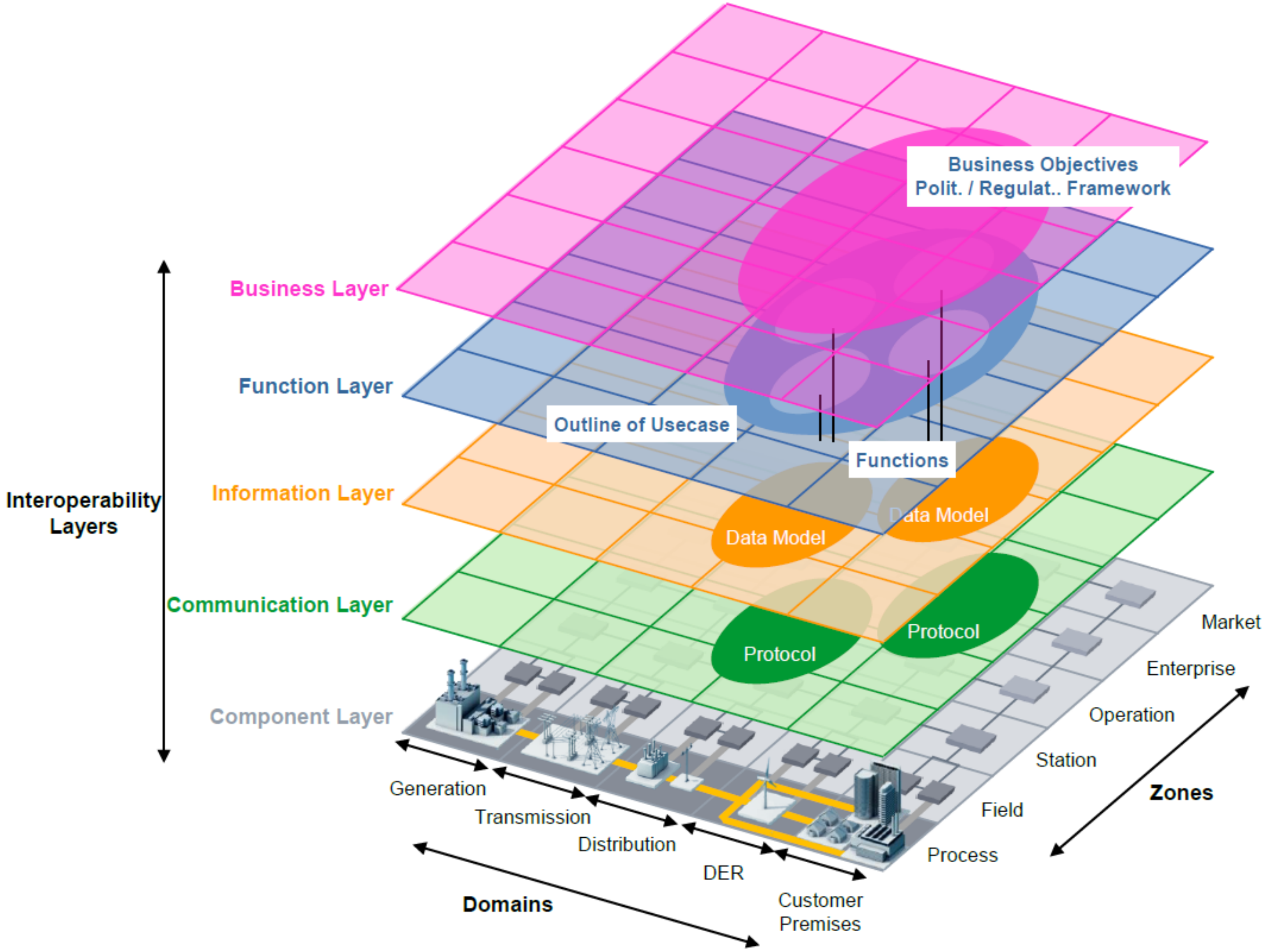
System capability of exchanging information with other systems and to use them



SGAM: the Smart Grid Plane
Power versus Information view

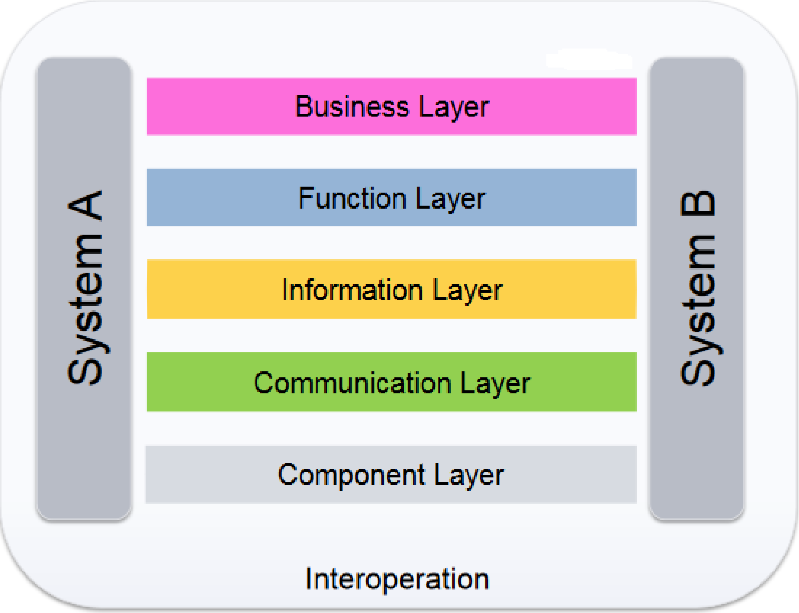


Smart Grid Architecture Model (SGAM)



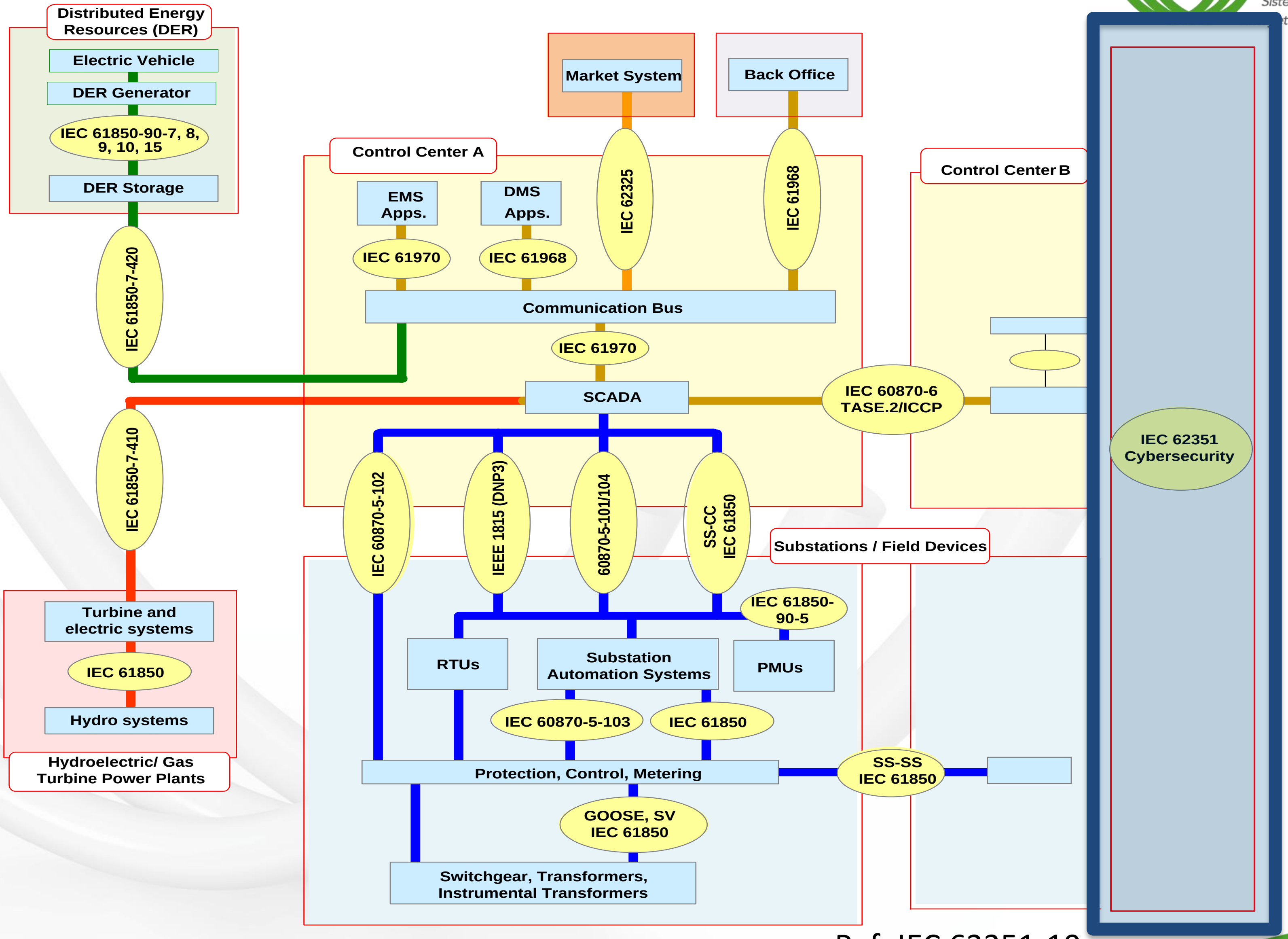
Ref: CEN – CENELEC - ETSI Smart Grid Coordination Group

Interoperability



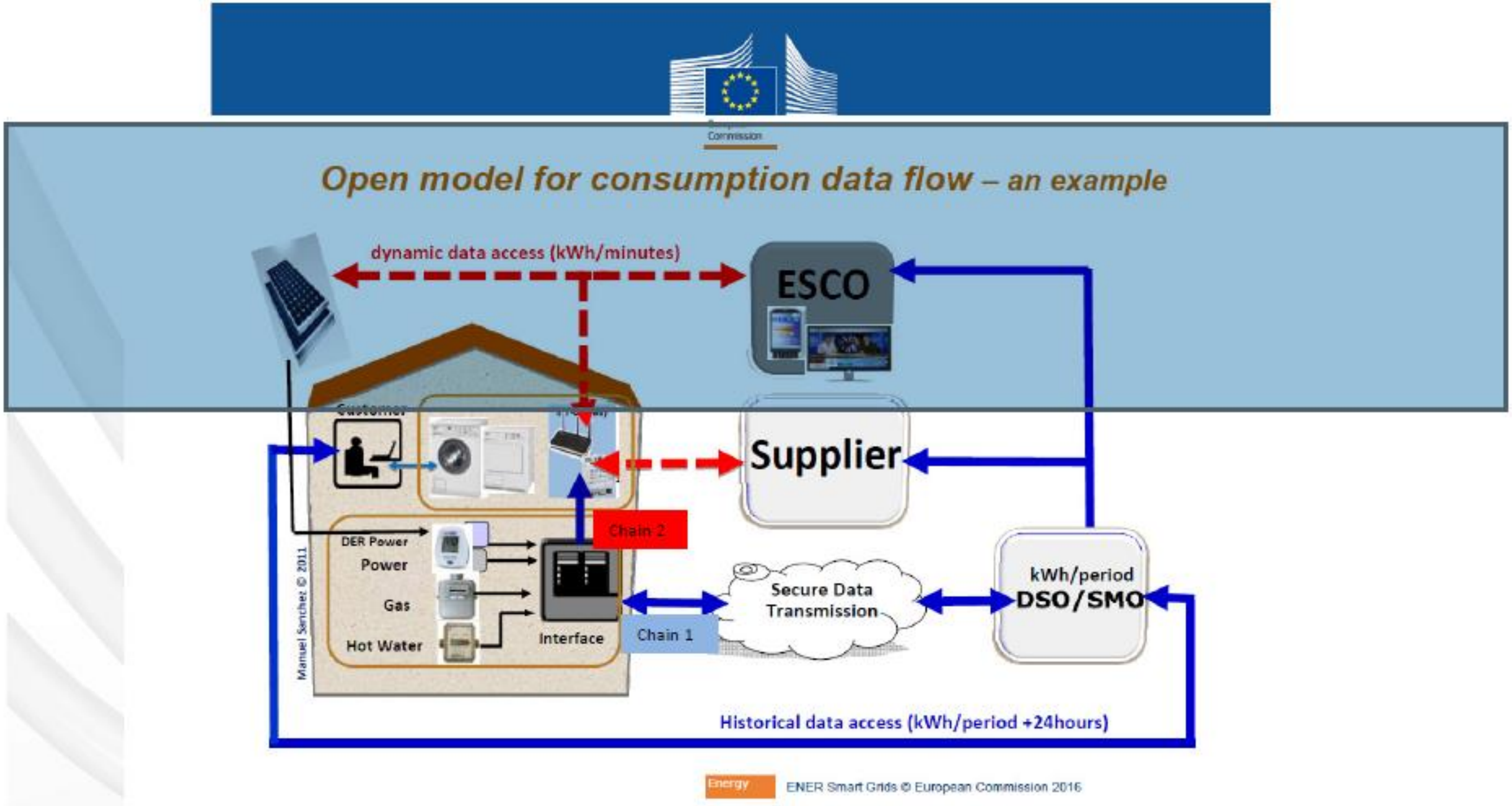
Need of data and protocol standards

Smart Grid Standards



Ref: IEC 62351-10

EU Smart Metering Model

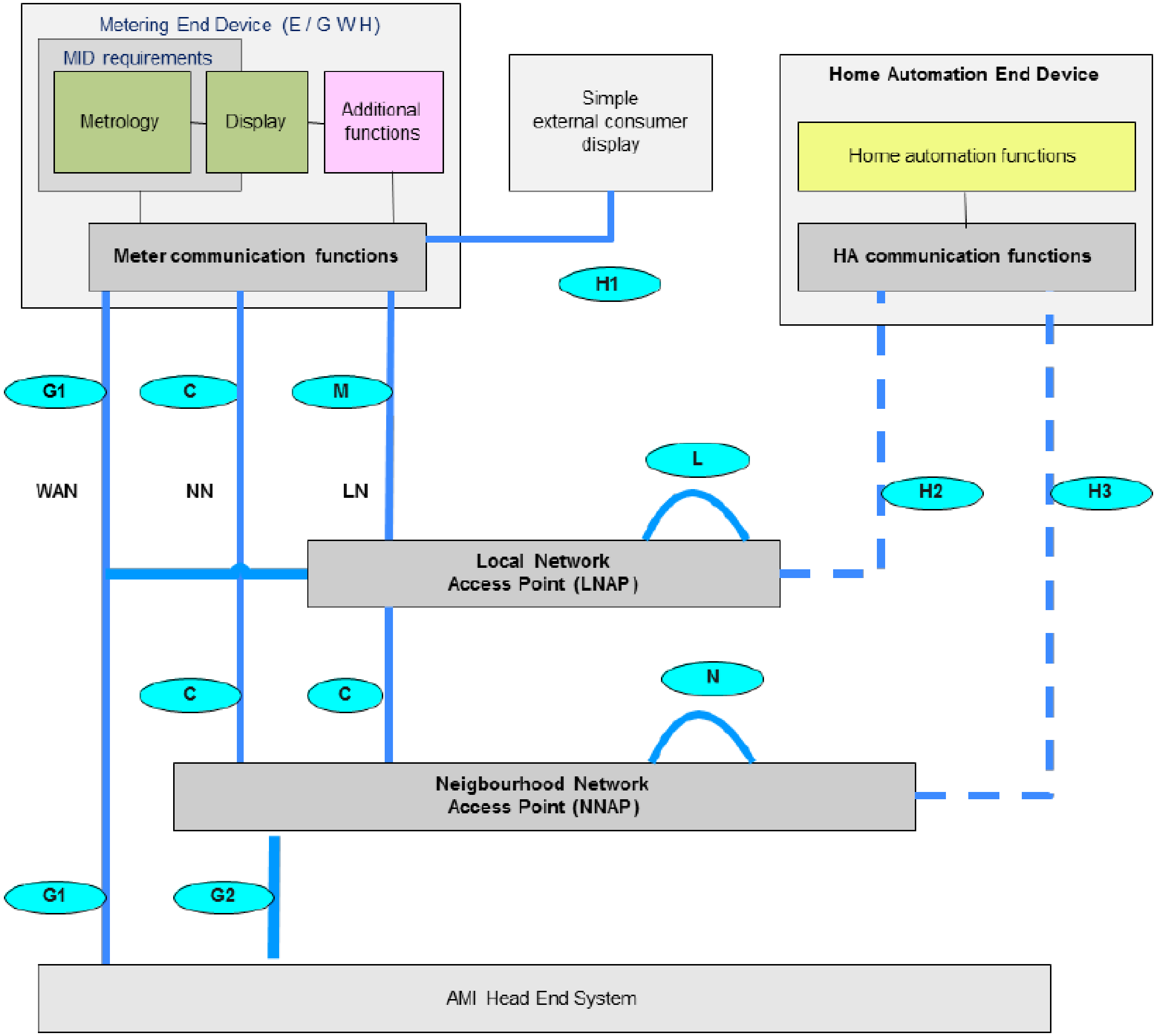


Open model for consumption data flow – an example

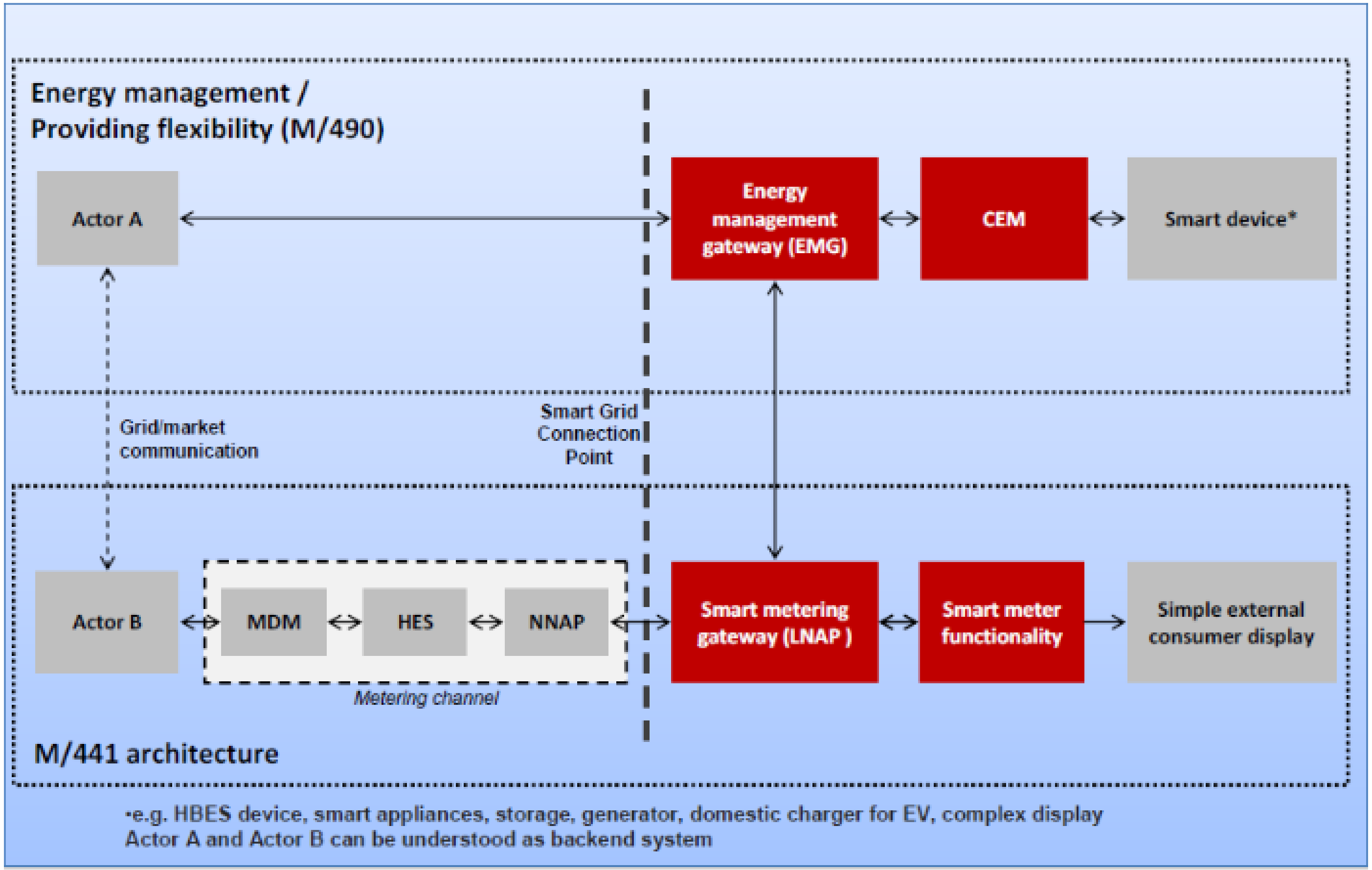
ENER Smart Grids © European Commission 2016

[1] Smart Metering, Standards & Interoperability - European Commission (EC)'s Directorate General for Energy - SGTF EG3 Workshop on Smart Home & Buildings, Brussels, 26 April 2016

Smart Metering Interfaces

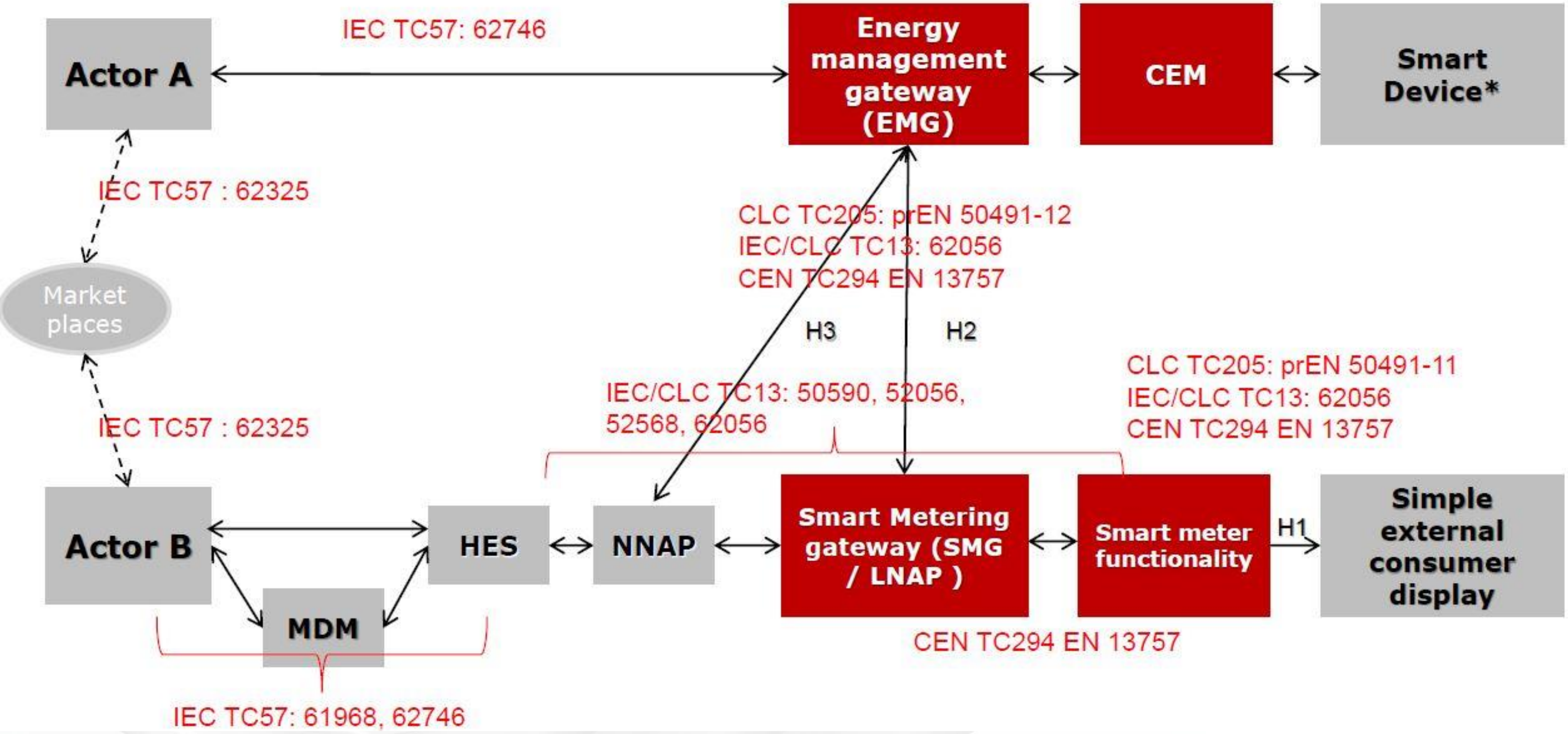

Metering End Device (E / G W H)
MID requirements
Metrology
Display
Additional functions
Meter communication functions
Simple external consumer display
H1
Home Automation End Device
Home automation functions
HA communication functions
G1
C
M
WAN
NN
LN
L
H2
H3
Local Network Access Point (LNAP)
C
C
N
Neigbourhood Network Access Point (NNAP)
G1
G2
AMI Head End System

SM communication architecture

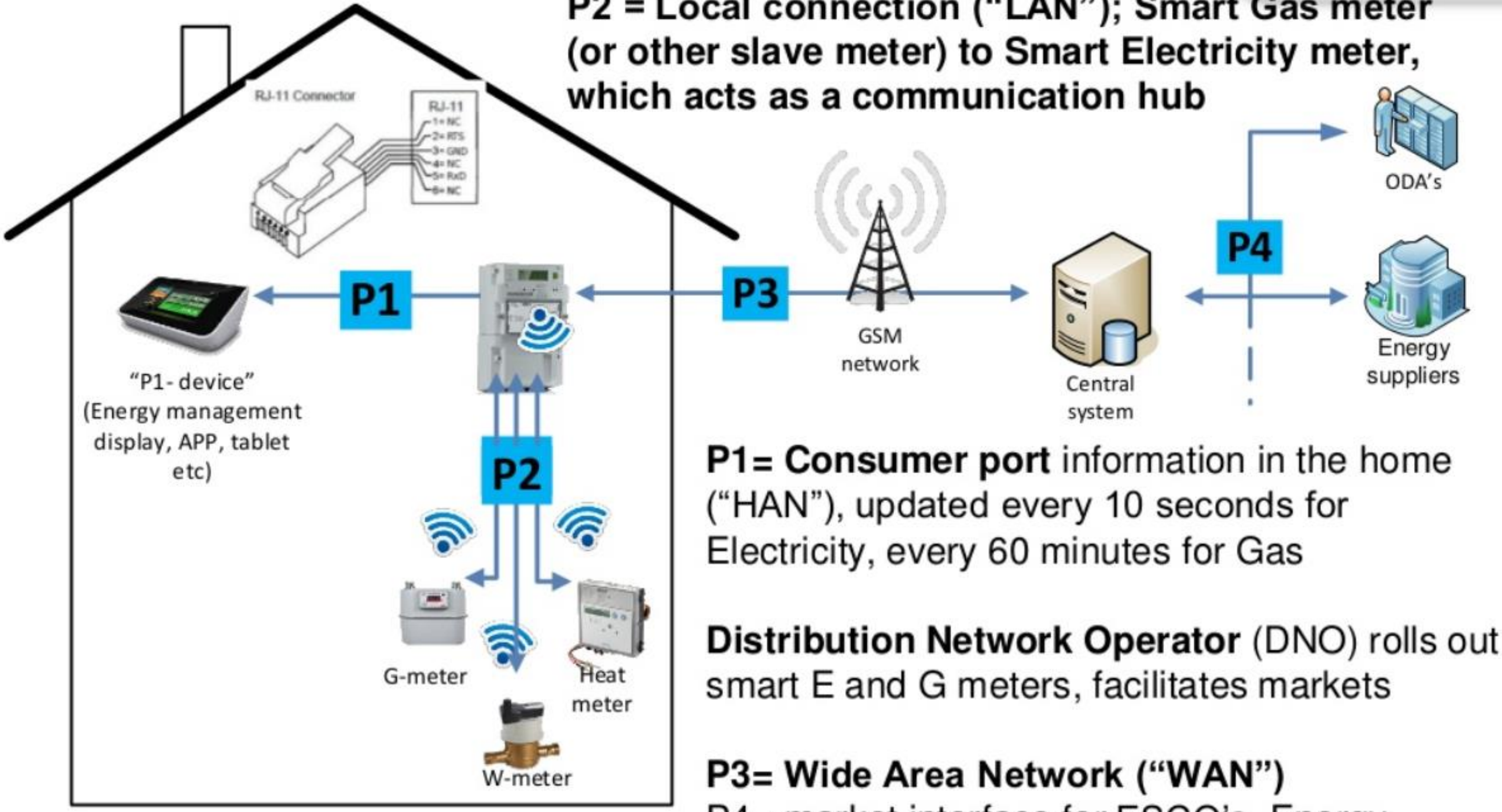

Energy management /
Providing flexibility (M/490)
Actor A
Energy management gateway (EMG)
CEM
Smart device*
Grid/market communication
Smart Grid Connection Point
Actor B
MDM
HES
NNAP
Metering channel
Smart metering gateway (LNAP)
Smart meter functionality
Simple external consumer display
M/441 architecture

•e.g. HBES device, smart appliances, storage, generator, domestic charger for EV, complex display
Actor A and Actor B can be understood as backend system

Standardization of the smart metering communications architecture (M/441 and M/490)



Smart Metering in the Netherlands



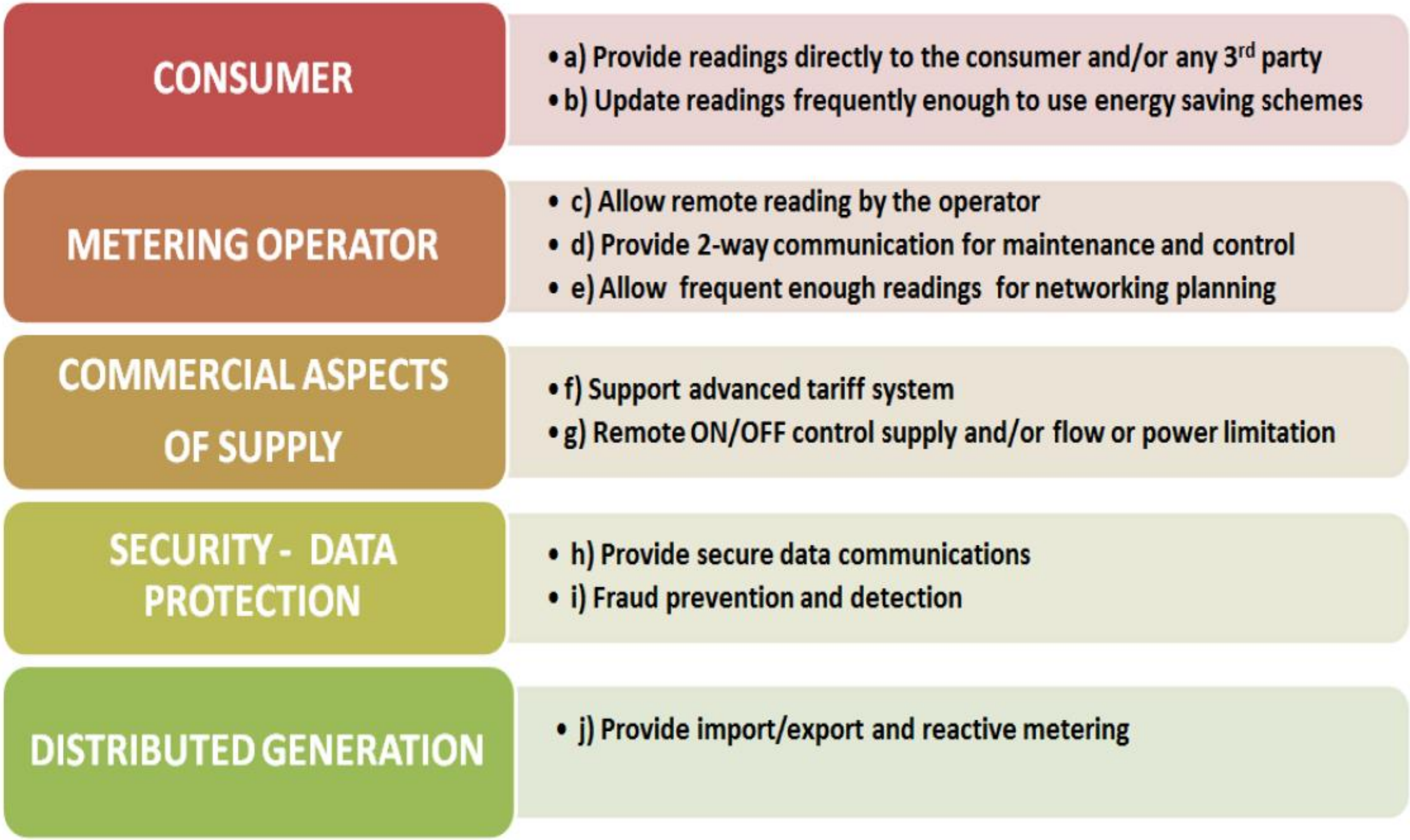
P2 = Local connection ("LAN"); Smart Gas meter (or other slave meter) to Smart Electricity meter, which acts as a communication hub

P1= Consumer port information in the home ("HAN"), updated every 10 seconds for Electricity, every 60 minutes for Gas

Distribution Network Operator (DNO) rolls out smart E and G meters, facilitates markets

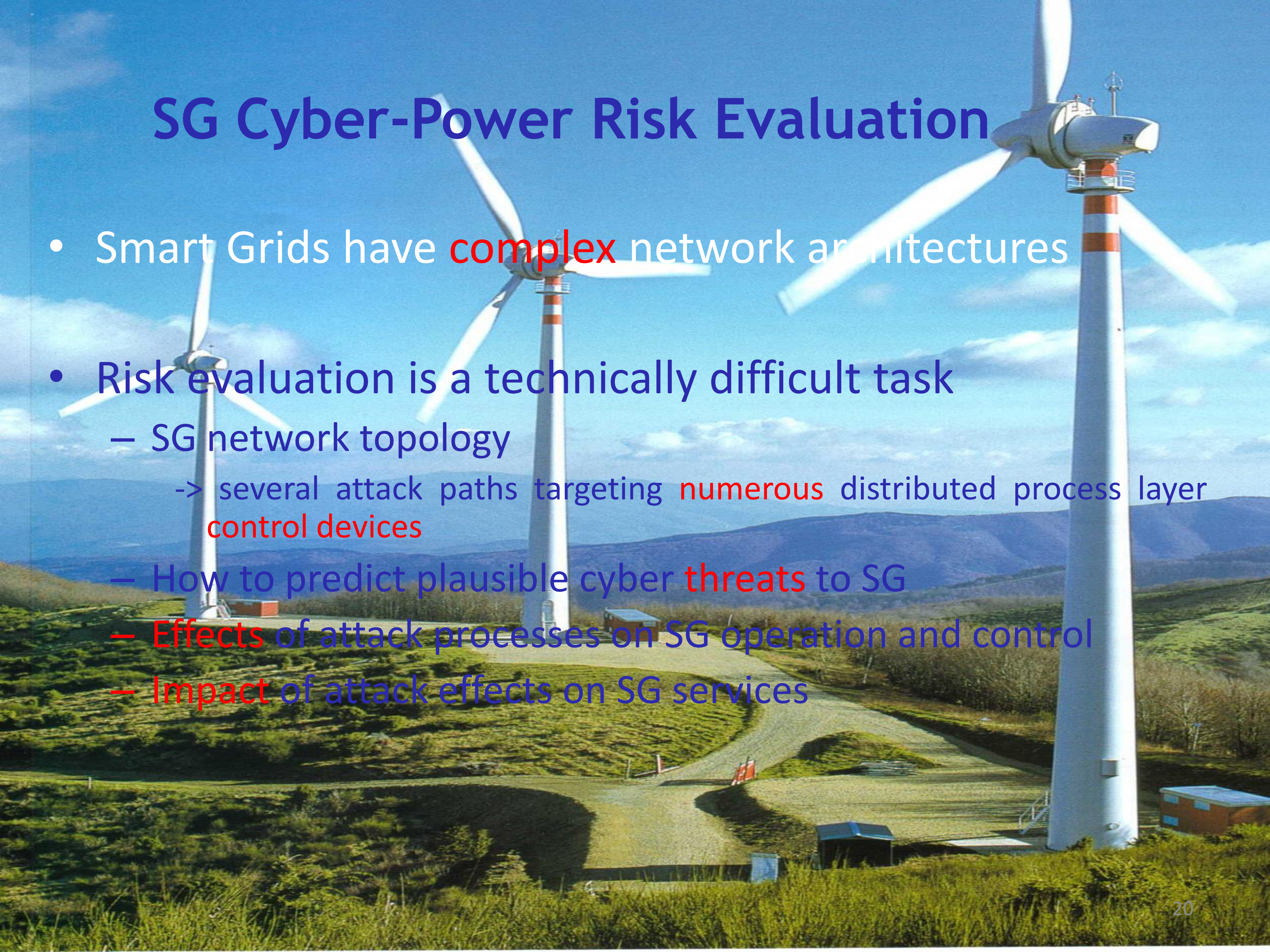
P3= Wide Area Network ("WAN")
P4= market interface for ESCO's, Energy Suppliers, aggregators; updated every 24 hours

EC 10 minimum (E)SM functionalities (2012/148/EU)



CONSUMER	• a) Provide readings directly to the consumer and/or any 3rd party • b) Update readings frequently enough to use energy saving schemes
METERING OPERATOR	• c) Allow remote reading by the operator • d) Provide 2-way communication for maintenance and control • e) Allow frequent enough readings for networking planning
COMMERCIAL ASPECTS OF SUPPLY	• f) Support advanced tariff system • g) Remote ON/OFF control supply and/or flow or power limitation
SECURITY - DATA PROTECTION	• h) Provide secure data communications • i) Fraud prevention and detection
DISTRIBUTED GENERATION	• j) Provide import/export and reactive metering

SG Cyber-Power Risk Evaluation



- Smart Grids have complex network architectures
- Risk evaluation is a technically difficult task
  - SG network topology

    -> several attack paths targeting numerous distributed process layer control devices
  - How to predict plausible cyber threats to SG
  - Effects of attack processes on SG operation and control
  - Impact of attack effects on SG services

Use Case details

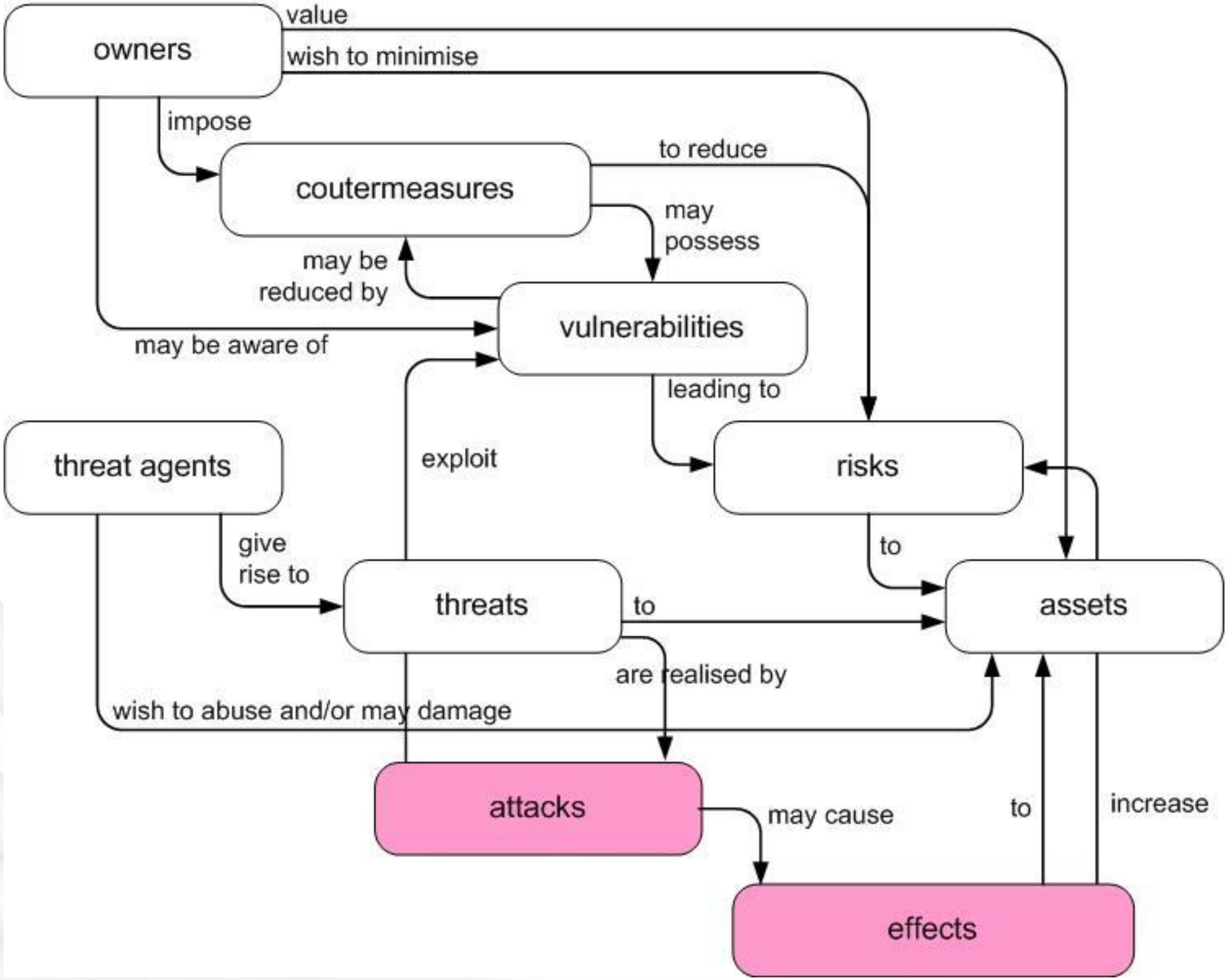
Parameter	Description
Geographical area	Geographical extension of the area covered by the grid service: multi-nation, nation, region, province, city
Population density	# of people in the area
Regulation	Applicable regulations
Grid size	Installed grid capacity
DER penetration	Total amount of Power from Renewable Energy Sources (RES)
DER size	Installed DER capacity
Grid topology	# HV/MV substations # MV loads # MV/LV substations # generators # storage devices # MV lines
Grid model parameters	Electrical parameters of grid components
DER model parameters	Electrical parameters of DER
Telecontrol Network Topology	# control centers # substation links per center # DER links per substation
Communication Network Topology	# gateways per network # communication (internal and external) interfaces per device
Data exchanges	Data models Communication protocol exchanges Communication interfaces Application message sequencing Data frequency Communication performance requirements Communication bandwidth requirements (traffic profile)

SG Cyber-Power Risk Evaluation

- Economically difficult to justify
  - High cost of security management

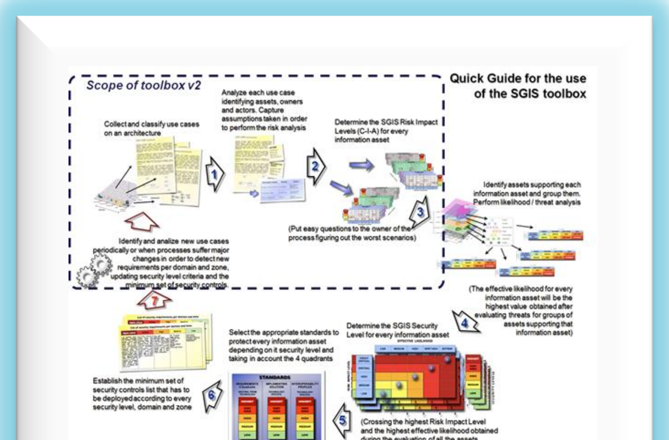
    min Risk -> >>>cost(Security)
  - Real benefits ?
- to control the value of risk to understand if we are spending enough for security

Cyber risk – conceptual model



SGIS Risk Analysis Process

Working Group SGIS (Smart Grid Information Security) of the CEN/CENELEC/ETSI Smart Grid Coordination Group



Scope of toolbox v2

Quick Guide for the use of the SGIS toolbox

Collect and classify use cases on an architecture

1 Analyze each use case identifying assets, owners and actors. Capture assumptions taken in order to perform the risk analysis

2 Determine the SGIS Risk Impact Levels (C-I-A) for every information asset

(Put easy questions to the owner of the process figuring out the worst scenarios)

3 Identify assets supporting each information asset and group them. Perform likelihood / threat analysis

(The effective likelihood for every information asset will be the highest value obtained after evaluating threats for groups of assets supporting that information asset)

4 Determine the SGIS Security Level for every information asset

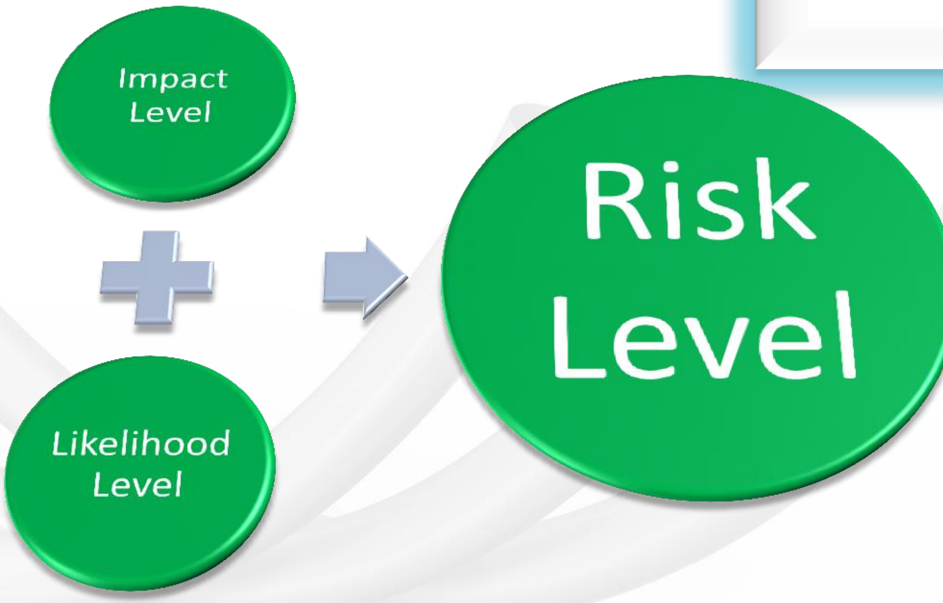
5 (Crossing the highest Risk Impact Level and the highest effective likelihood obtained during the evaluation of all the assets included in his map of dependencies)

Select the appropriate standards to protect every information asset depending on it security level and taking in account the 4 quadrants

6 Establish the minimum set of security controls list that has to be deployed according to every security level, domain and zone

7 Identify and analize new use cases periodically or when processes suffer major changes in order to detect new requirements per domain and zone, updating security level criteria and the minimum set of security controls

Source: CEN/CENELEC/ETSI 2012



Impact Level

Likelihood Level

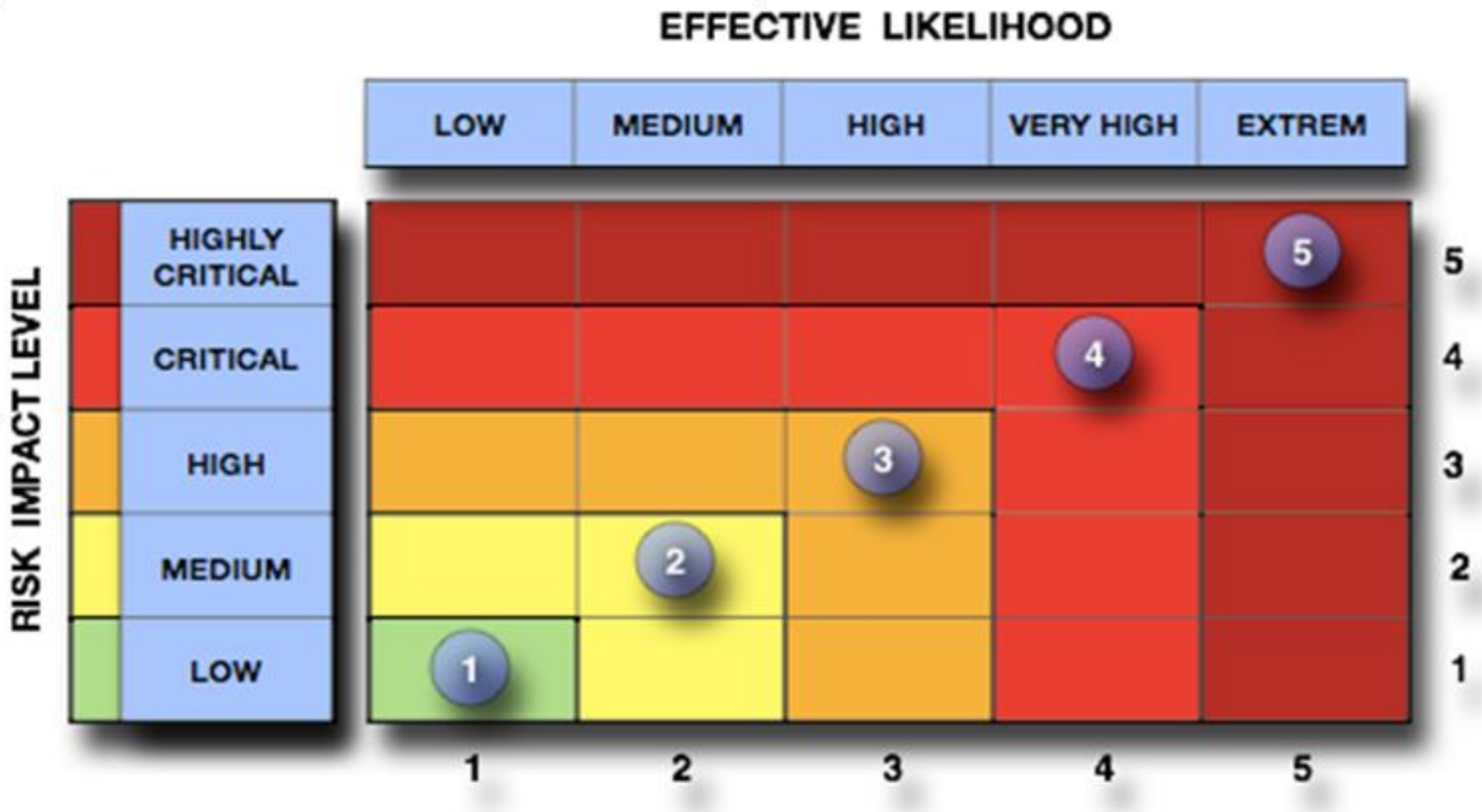
Risk Level

SGIS Risk Impact Levels

RISK IMPACT LEVELS	OPERATIONAL (availability)				LEGAL		HUMAN	REPUTATION	FINANCIAL
	Energy supply (Watt)	Energy flow (Watt/hour)	Population	Infrastructures	Data protection	other laws & regulations			
HIGHLY CRITICAL	regional grids from 10GW	from 10 GW/h	from 50% population in a country or from 25% in several countries	international critical infrastructures affected	not defined	company closure or collateral disruptions	direct and collateral deaths in several countries	permanent loss of trust affecting all corporation	Thirth party affected
CRITICAL	national grids from 1 GW to 10GW	from 1 GW/h to 10GW/h	from 25% to 50% population size affected	national critical infrastructures affected	not defined	temporary disruption of activities	direct and collateral deaths in a country	permanent loss of trust in a country	>=50% EBITDA
HIGH	city grids from 100MW to 1GW	from 100MW/h to 1GW/h	from 10% to 25% population size affected	essential infrastructures affected	unauthorized disclosure or modification of sensitive data	prison	direct deaths in a country	temporary loss of trust in a country	<50% EBITDA
MEDIUM	neighborhood grids from 10MW to 100MW	from 10MW/h to 100MW/h	from 2% to 10% population size affected	complimentary infrastructures affected	unauthorized disclosure or modification of personal data	fines	seriously injured or discapacity	temporary and local loss or trust	<33% EBITDA
LOW	home or building networks under 10 MW	under 10MW/h	under 2% population size affected in a country	no complimentary infrastructures	no personal nor sensitive data involved	warnings	minor accidents	short time & scope (warnings)	<1% EBITDA

MEASUREMENT CATEGORIES

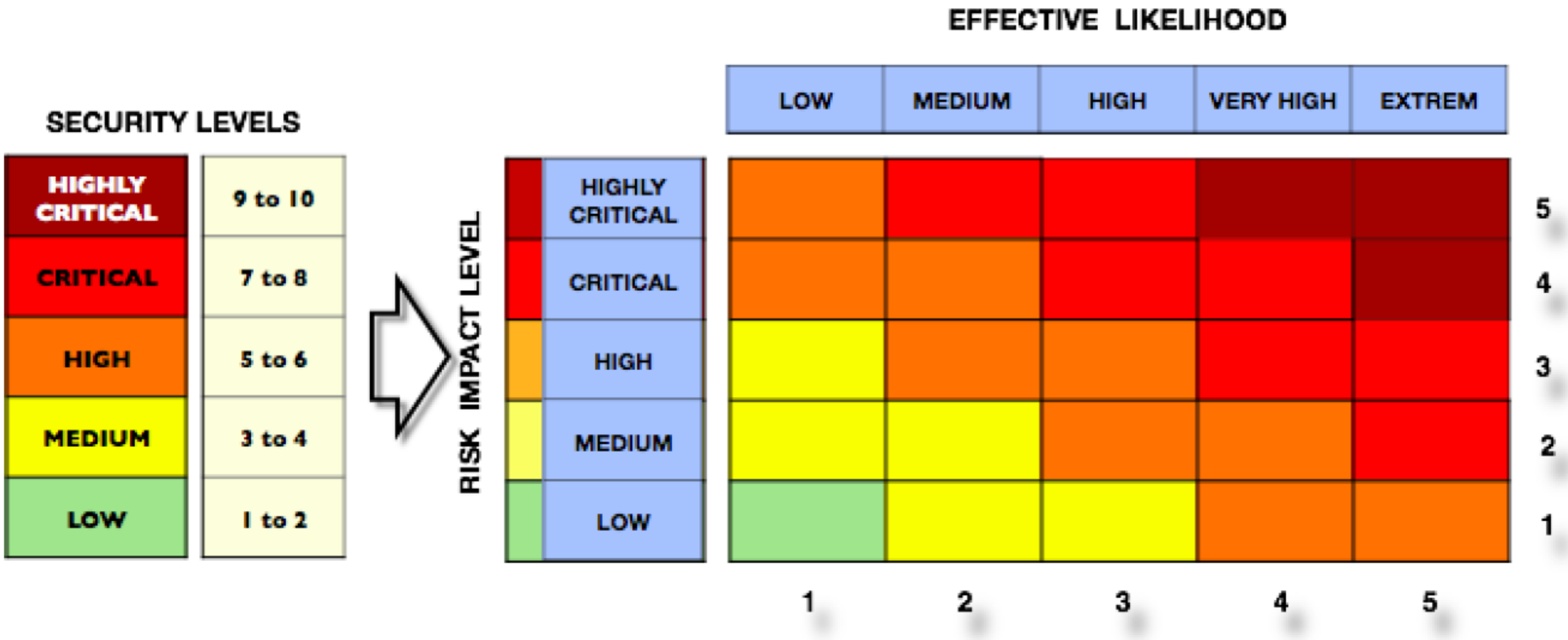
SGIS Security Levels v1



EFFECTIVE LIKELIHOOD

RISK IMPACT LEVEL		LOW	MEDIUM	HIGH	VERY HIGH	EXTREM	
HIGHLY CRITICAL						5	5
CRITICAL					4		4
HIGH				3			3
MEDIUM			2				2
LOW		1					1
		1	2	3	4	5	

SGIS Security Levels v2



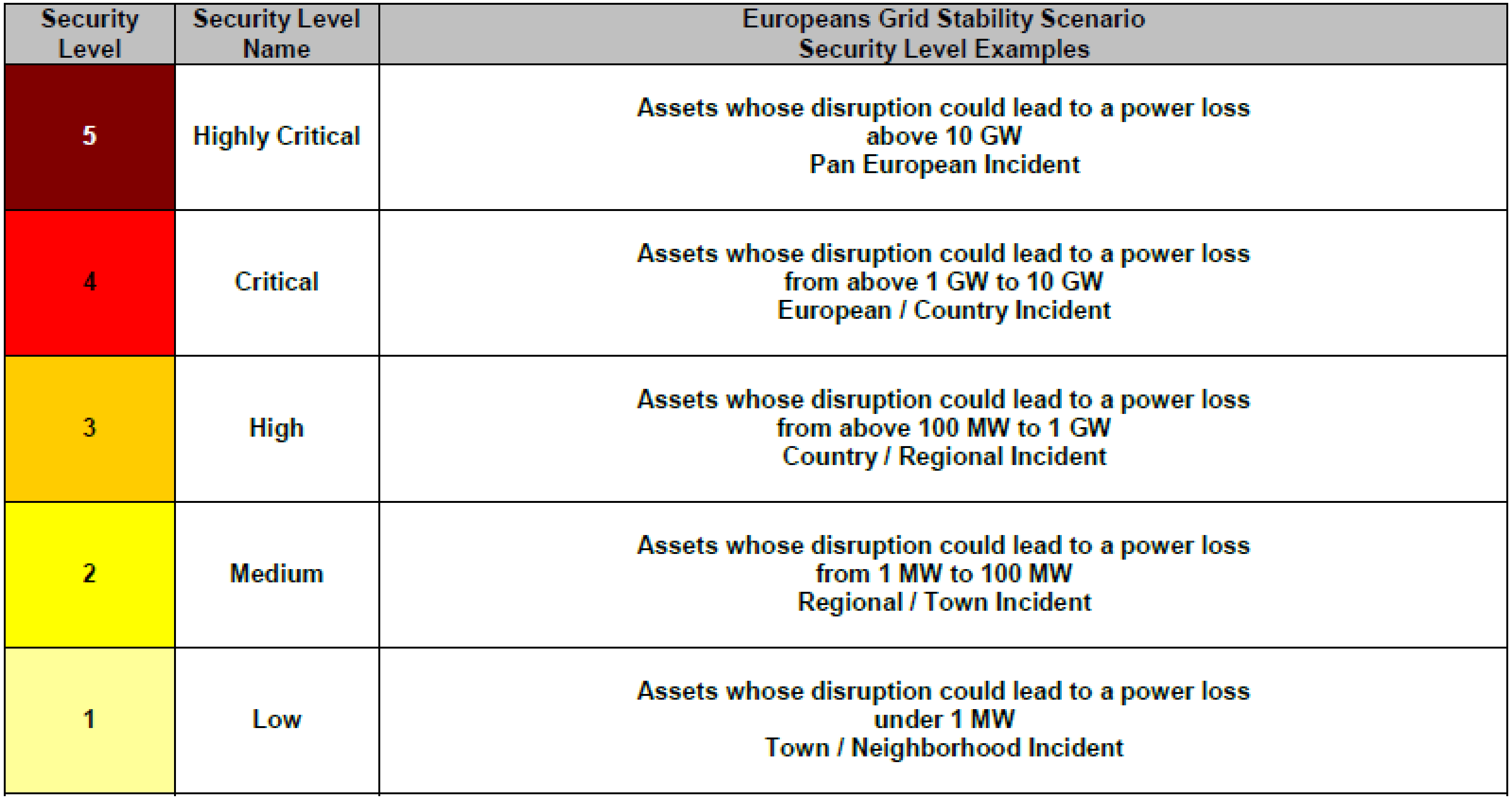
SECURITY LEVELS

HIGHLY CRITICAL	9 to 10
CRITICAL	7 to 8
HIGH	5 to 6
MEDIUM	3 to 4
LOW	1 to 2

EFFECTIVE LIKELIHOOD

RISK IMPACT LEVEL	LOW	MEDIUM	HIGH	VERY HIGH	EXTREM	
HIGHLY CRITICAL	🟧	🟥	🟥	🟫	🟫	5
CRITICAL	🟧	🟧	🟥	🟥	🟫	4
HIGH	🟨	🟧	🟧	🟥	🟥	3
MEDIUM	🟨	🟨	🟧	🟧	🟥	2
LOW	🟩	🟨	🟨	🟧	🟧	1
	1	2	3	4	5	

SGIS Security Levels



Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Cyber risk assessment

$$R_{Cyber-Power} = \sum_{j} P^{j} * (\gamma^{j} \mid P_{S})$$

- j is an attack process i.e. a logical sequence of attack steps deploying specific techniques
- P^{j} is the success probability of the attack process j
- $\gamma^{j} \mid P_{S}$ is the impact of the attack process j conditioned by the probability P_S that the Power System is in the state S

Cyber risk assessment (cont.)

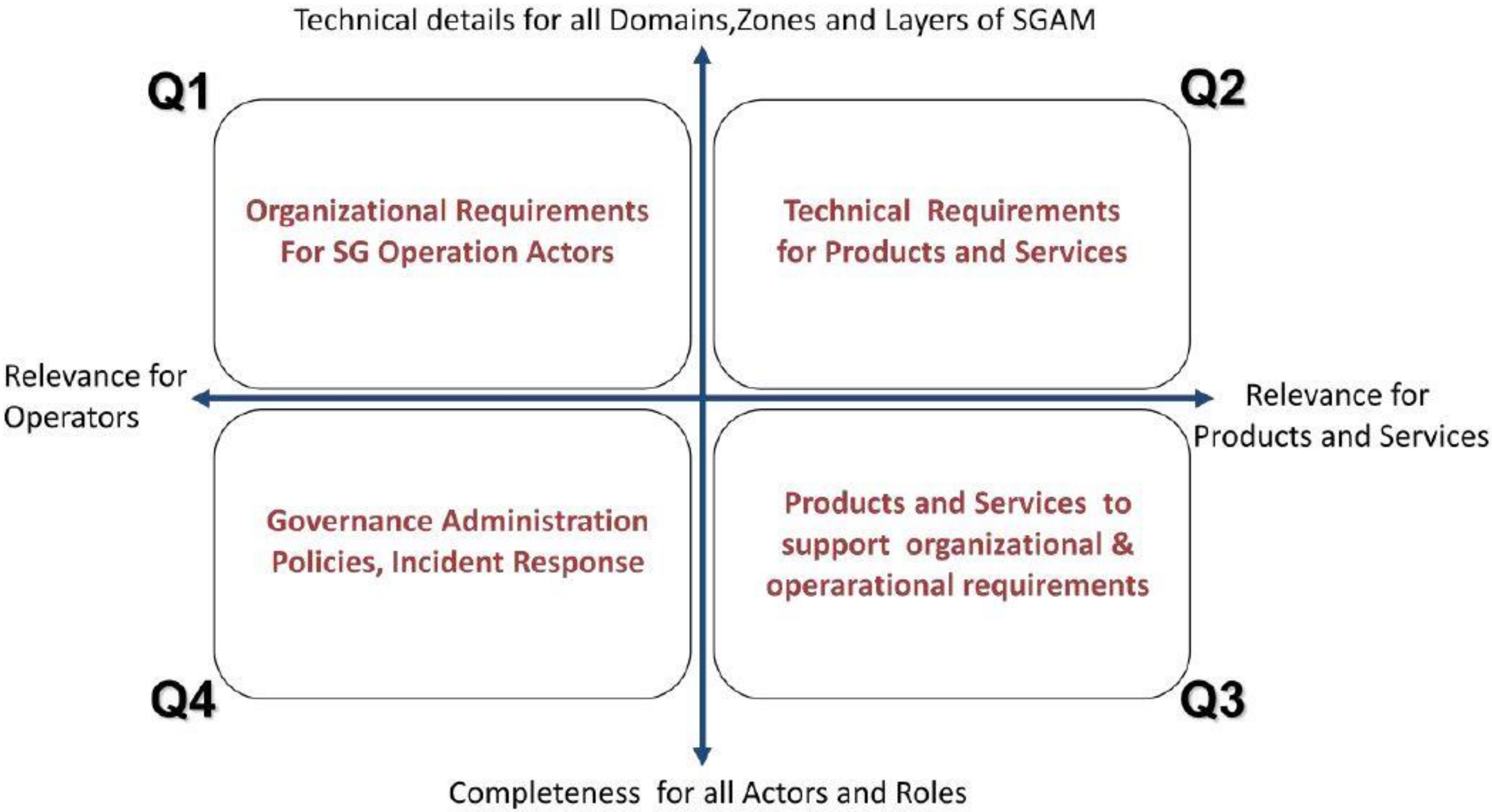
$$P^j = (\pi_K^{j,1} \mid \pi_V^{j,1} * \pi_T^{j,1}) \mid \ldots \mid \pi_K^{j,n-1}(\mid \pi_V^{j,n-1} * \pi_T^{j,n-1}) \mid (\pi_K^{j,n} \mid \pi_V^{j,n} * \pi_T^{j,n})$$

- n is the number of attack steps of the attack process j

- $\pi_{V/T/K}^{j,i}$ are the probabilities of, respectively, the existence of the vulnerability V, the occurrence of the threat T and the successfulness of the attack K referred to the step i of the attack process j

- $\pi_K^{j,i} \mid \pi_V^{j,i} * \pi_T^{j,i}$ is the probability of the step *i*-attack *j* successfulness conditioned by the probabilities of a vulnerability existence V and a threat occurrence T, assumed to be statistically independent events

Security standard areas



Technical details for all Domains,Zones and Layers of SGAM

Q1

Organizational Requirements For SG Operation Actors

Q2

Technical Requirements for Products and Services

Relevance for Operators

Relevance for Products and Services

Governance Administration Policies, Incident Response

Products and Services to support organizational & operarational requirements

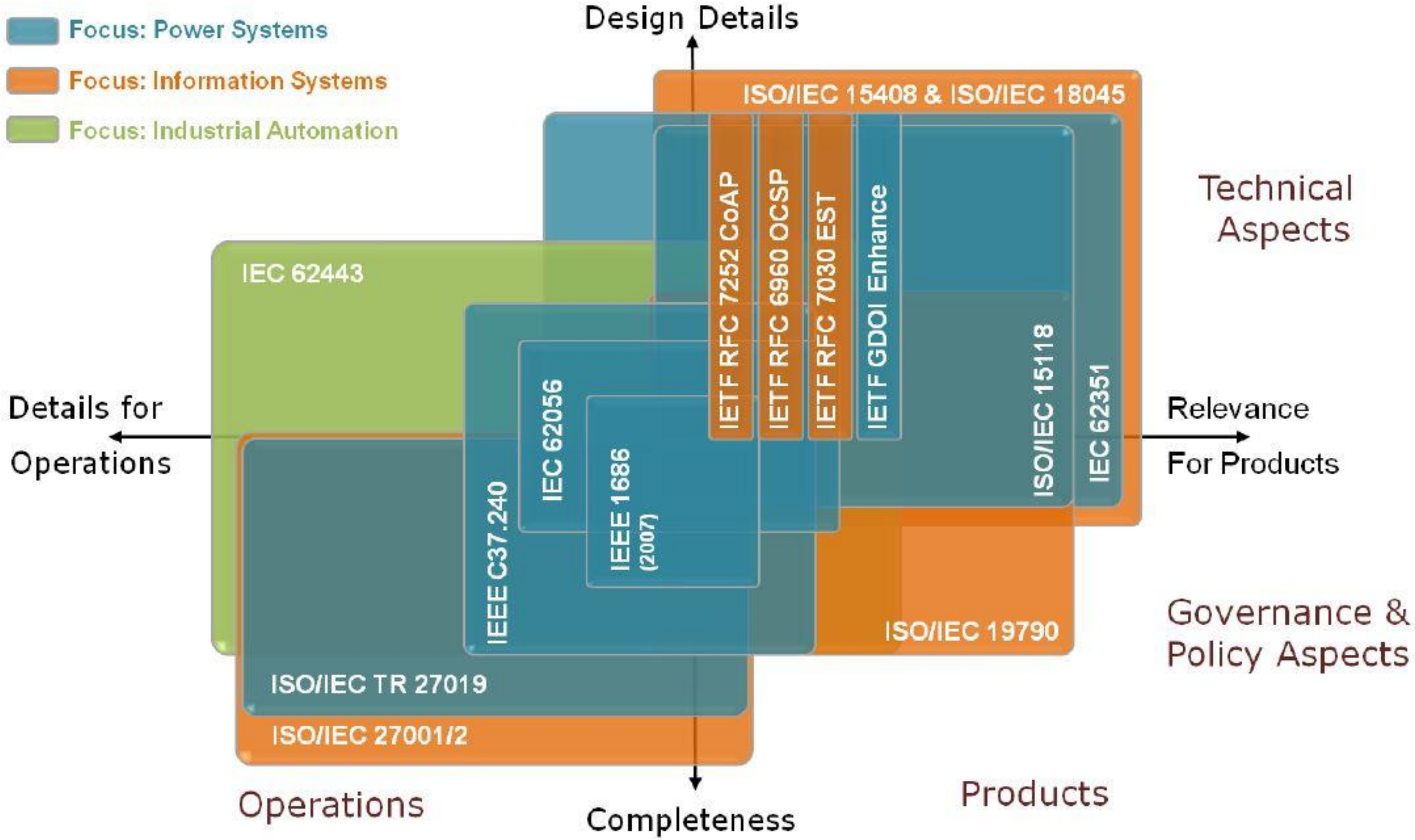
Q4

Q3

Completeness for all Actors and Roles

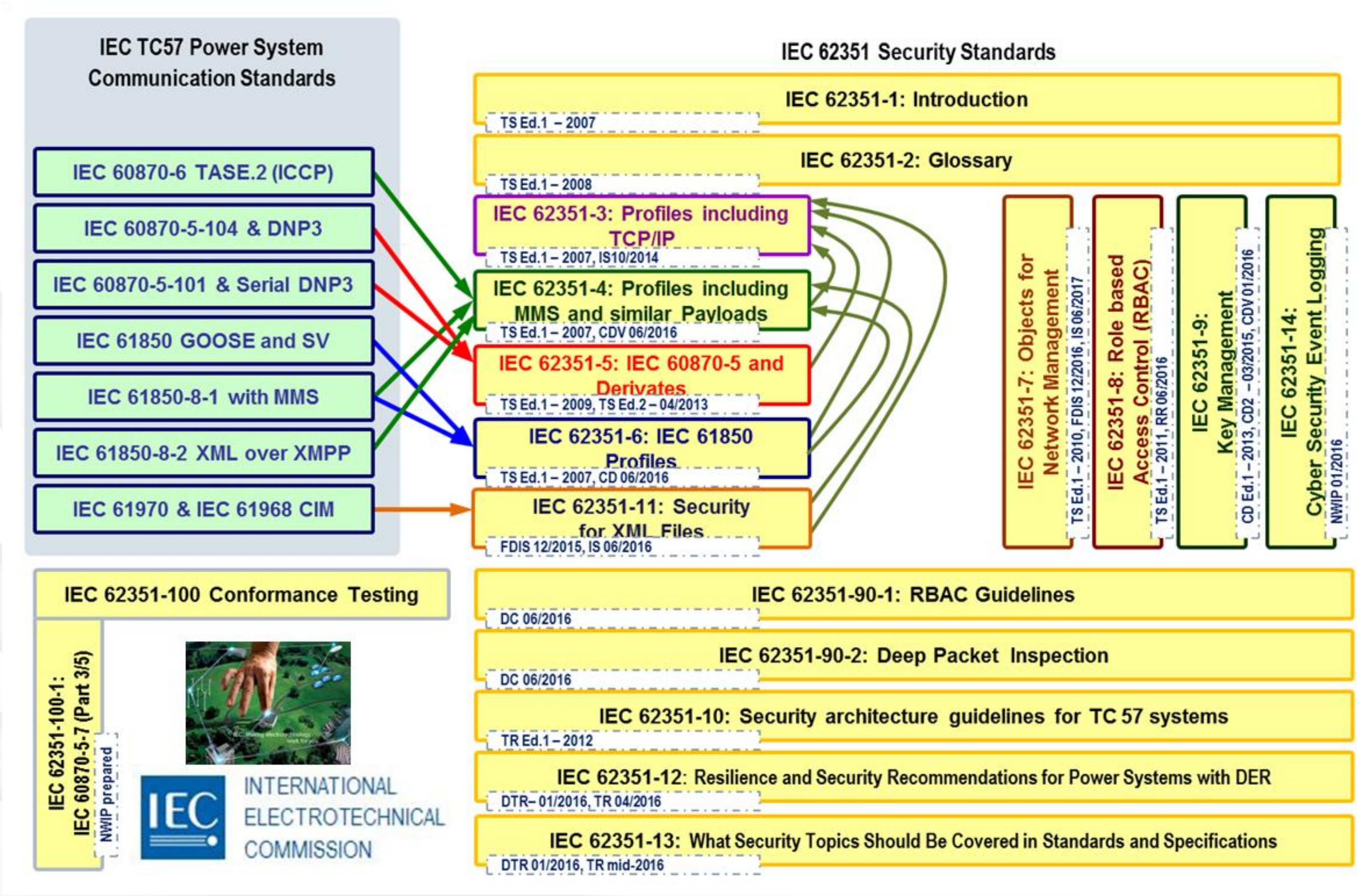
Source: CEN/CENELEC/ETSI SGIS Report 2014

Security standards coverage



Source: CEN/CENELEC/ETSI SEG-CG/CSP Report 2016

IEC 62351



IEC TC57 Power System Communication Standards

- IEC 60870-6 TASE.2 (ICCP)
- IEC 60870-5-104 & DNP3
- IEC 60870-5-101 & Serial DNP3
- IEC 61850 GOOSE and SV
- IEC 61850-8-1 with MMS
- IEC 61850-8-2 XML over XMPP
- IEC 61970 & IEC 61968 CIM

IEC 62351 Security Standards

- IEC 62351-1: Introduction — TS Ed.1 – 2007
- IEC 62351-2: Glossary — TS Ed.1 – 2008
- IEC 62351-3: Profiles including TCP/IP — TS Ed.1 – 2007, IS10/2014
- IEC 62351-4: Profiles including MMS and similar Payloads — TS Ed.1 – 2007, CDV 06/2016
- IEC 62351-5: IEC 60870-5 and Derivates — TS Ed.1 – 2009, TS Ed.2 – 04/2013
- IEC 62351-6: IEC 61850 Profiles — TS Ed.1 – 2007, CD 06/2016
- IEC 62351-11: Security for XML Files — FDIS 12/2015, IS 06/2016
- IEC 62351-7: Objects for Network Management — TS Ed.1 – 2010, FDIS 12/2016, IS 06/2017
- IEC 62351-8: Role based Access Control (RBAC) — TS Ed.1 – 2011, RR 06/2016
- IEC 62351-9: Key Management — CD Ed.1 – 2013, CD2 – 03/2015, CDV 01/2016
- IEC 62351-14: Cyber Security Event Logging — NWIP 01/2016
- IEC 62351-90-1: RBAC Guidelines — DC 06/2016
- IEC 62351-90-2: Deep Packet Inspection — DC 06/2016
- IEC 62351-10: Security architecture guidelines for TC 57 systems — TR Ed.1 – 2012
- IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER — DTR – 01/2016, TR 04/2016
- IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications — DTR 01/2016, TR mid-2016

IEC 62351-100 Conformance Testing

IEC 62351-100-1: IEC 60870-5-7 (Part 3/5) — NWIP prepared

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

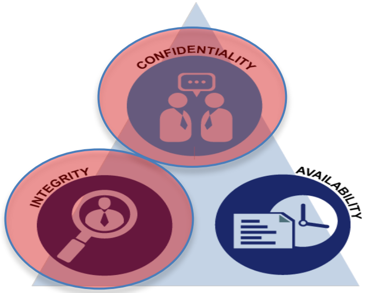
Source: IEC TC57 WG15

Preventive measures
IEC 62351 Part 3
Communication network and system security – Profile including TCP/IP

IEC 62351 Part 3 (IS 2014) specifies how to provide security for TCP/IP-based SCADA and telecontrol protocols

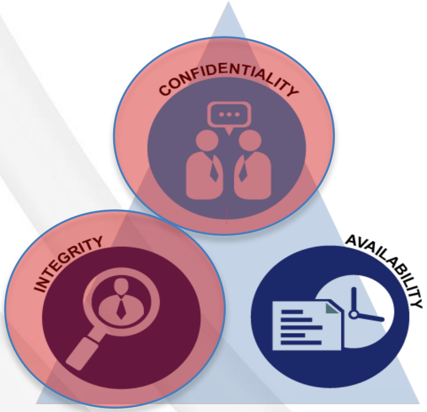
Constraints on Transport Layer Security (TLS) for end-to-end security

- Counters unauthorised access or modification or theft of information
- TLS profile
- Peer authentication through bi-directional PKI certificate exchange and validation is mandatory
- Public key exchange, packet encryption
- Session renegotiation, Session resumption
- Certificate validation protocol
- For key management refers to IEC 62351-9



Defensive measures

Residual risks from threats uncovered by the end-to-end security measures require the implementation of a monitoring framework



Residual risks

Need monitoring

Defensive measures

IEC 62351 Part 7: Network and System Management (NSM) data object models

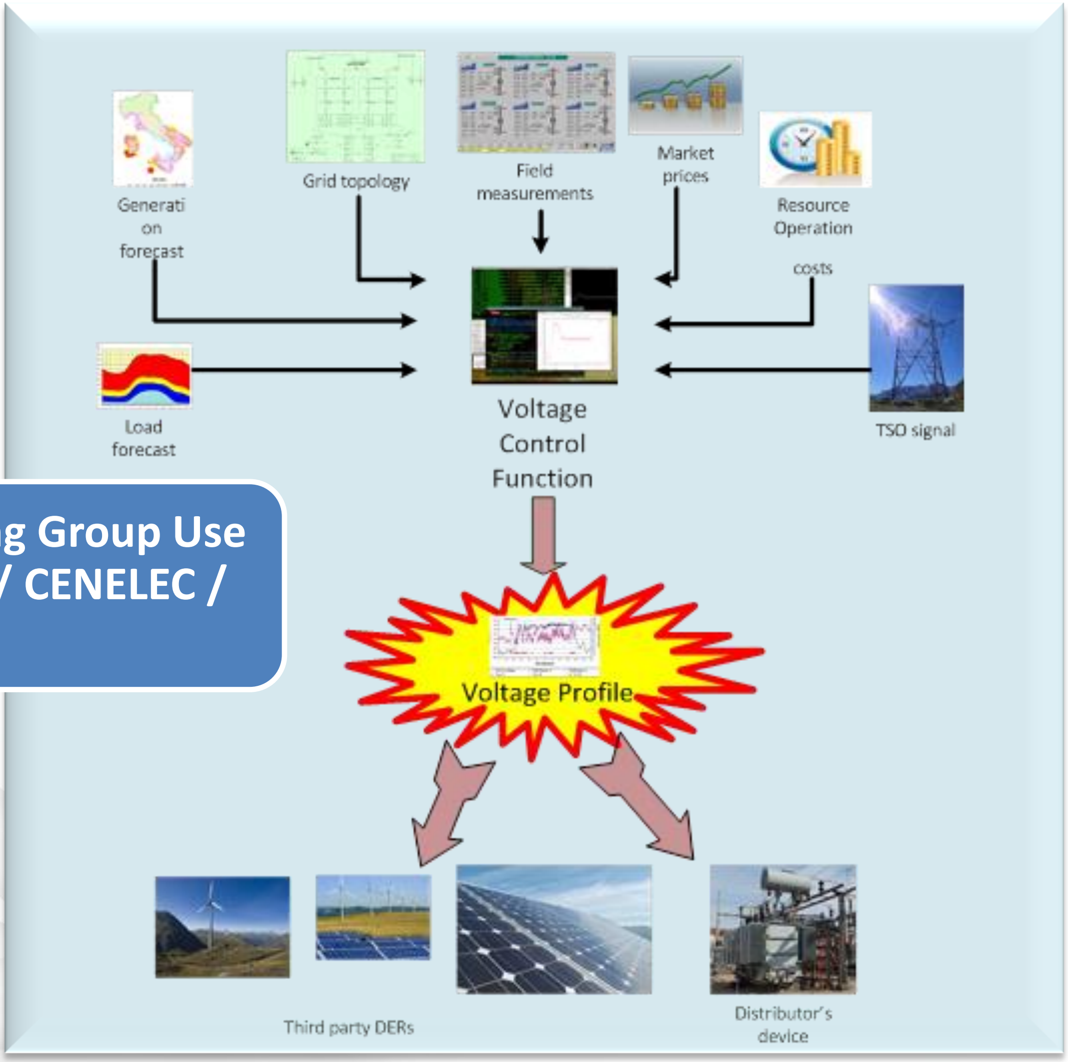
IEC 62351 Part 7 (IS within 2016) specifies data object models to monitor the health and the condition of the components of the power systems

Monitoring for security purposes, enabling anomaly detection and recovery functions

Monitoring network and IED devices and correlation of information from

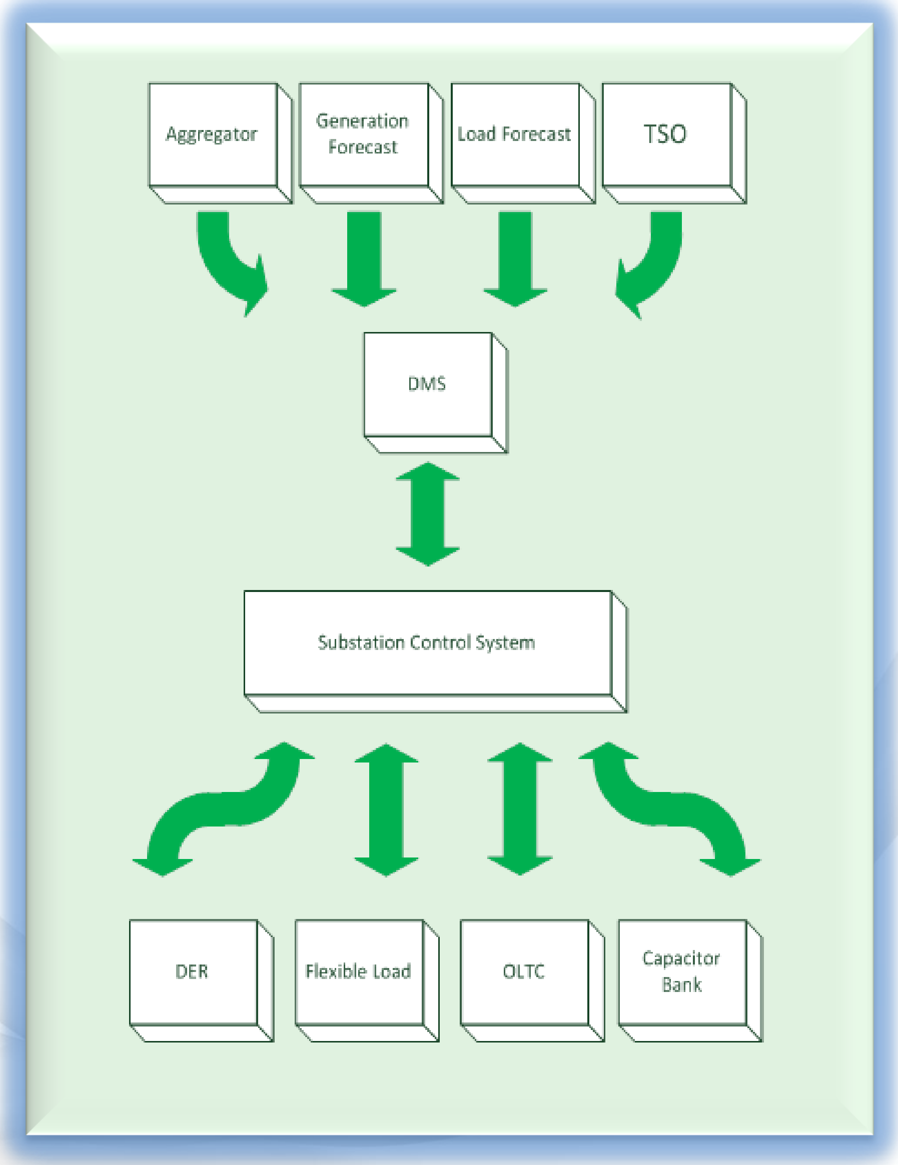
- IEC 62351-7 data objects, specific to power system operation
- IETF data objects

Voltage Control Use Case

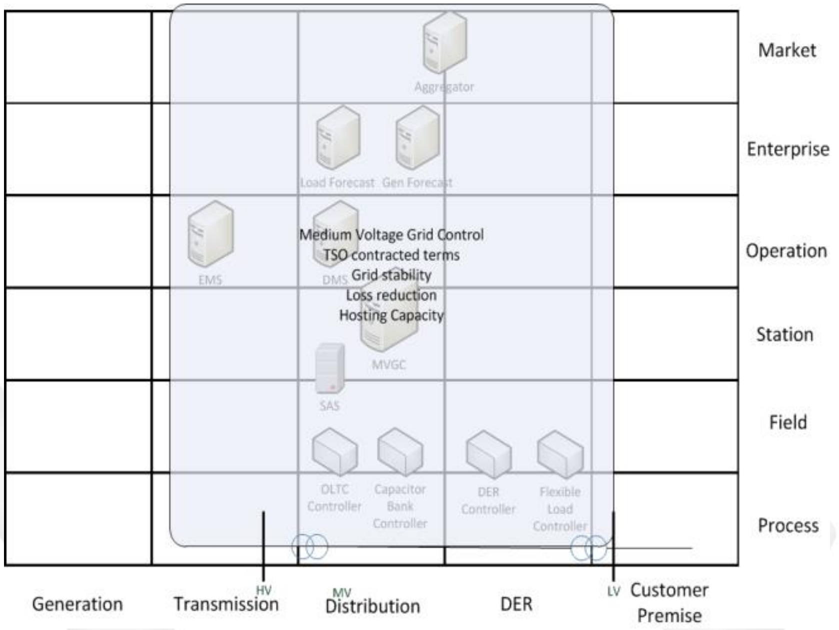


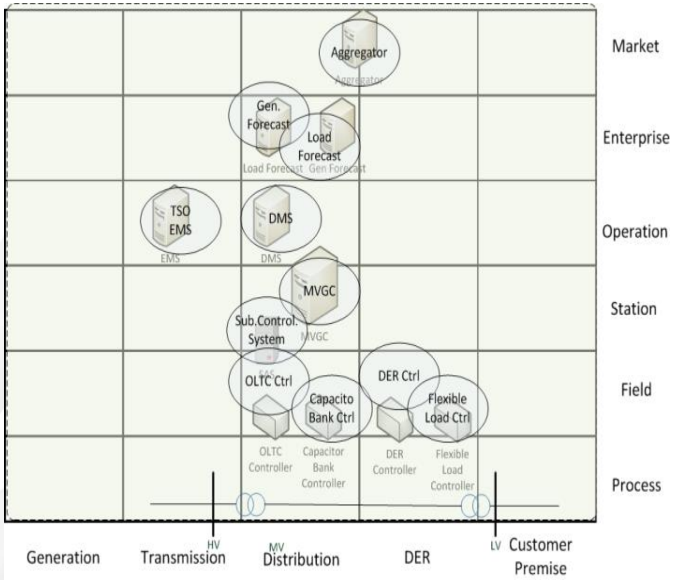
Based on SGSP Working Group Use Case WGSP-0200 CEN / CENELEC / ETSI

VC - Actors and Interactions

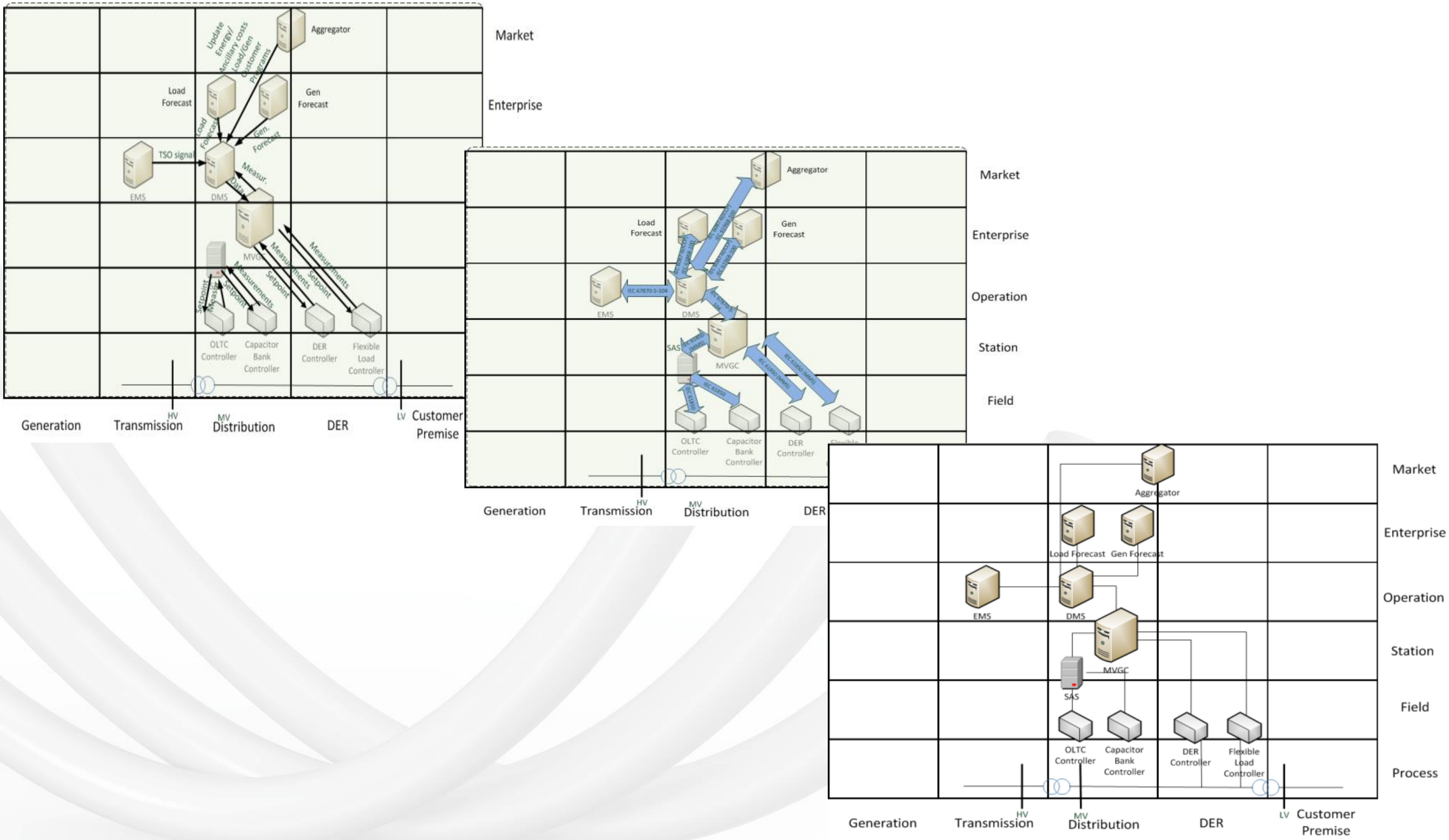


VC - SGAM mapping

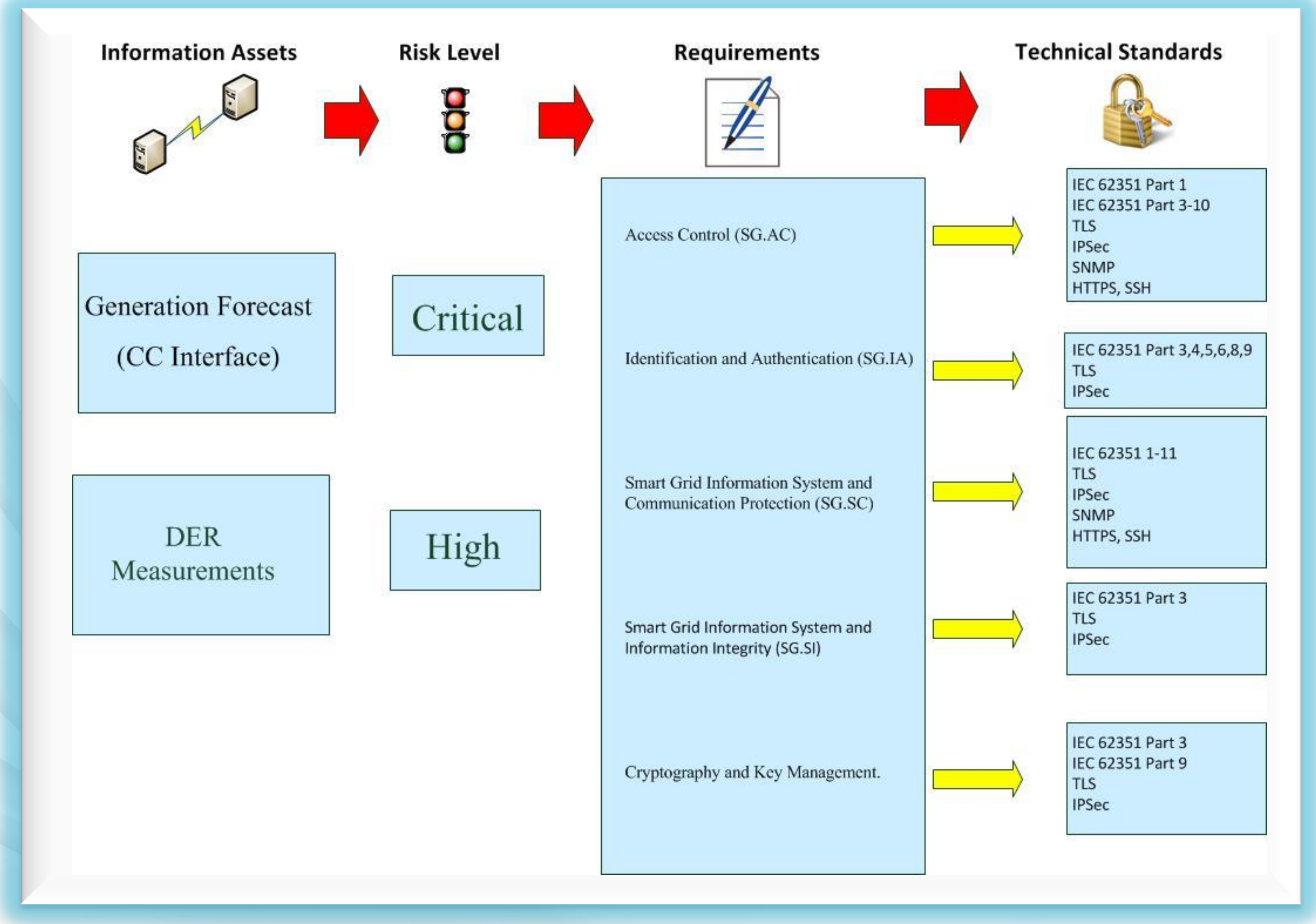




VC – SGAM mapping (cont.)



VC - Security Analysis



Information Assets

Risk Level

Requirements

Technical Standards

Generation Forecast (CC Interface)

Critical

DER Measurements

High

Access Control (SG.AC)

Identification and Authentication (SG.IA)

Smart Grid Information System and Communication Protection (SG.SC)

Smart Grid Information System and Information Integrity (SG.SI)

Cryptography and Key Management.

IEC 62351 Part 1
IEC 62351 Part 3-10
TLS
IPSec
SNMP
HTTPS, SSH

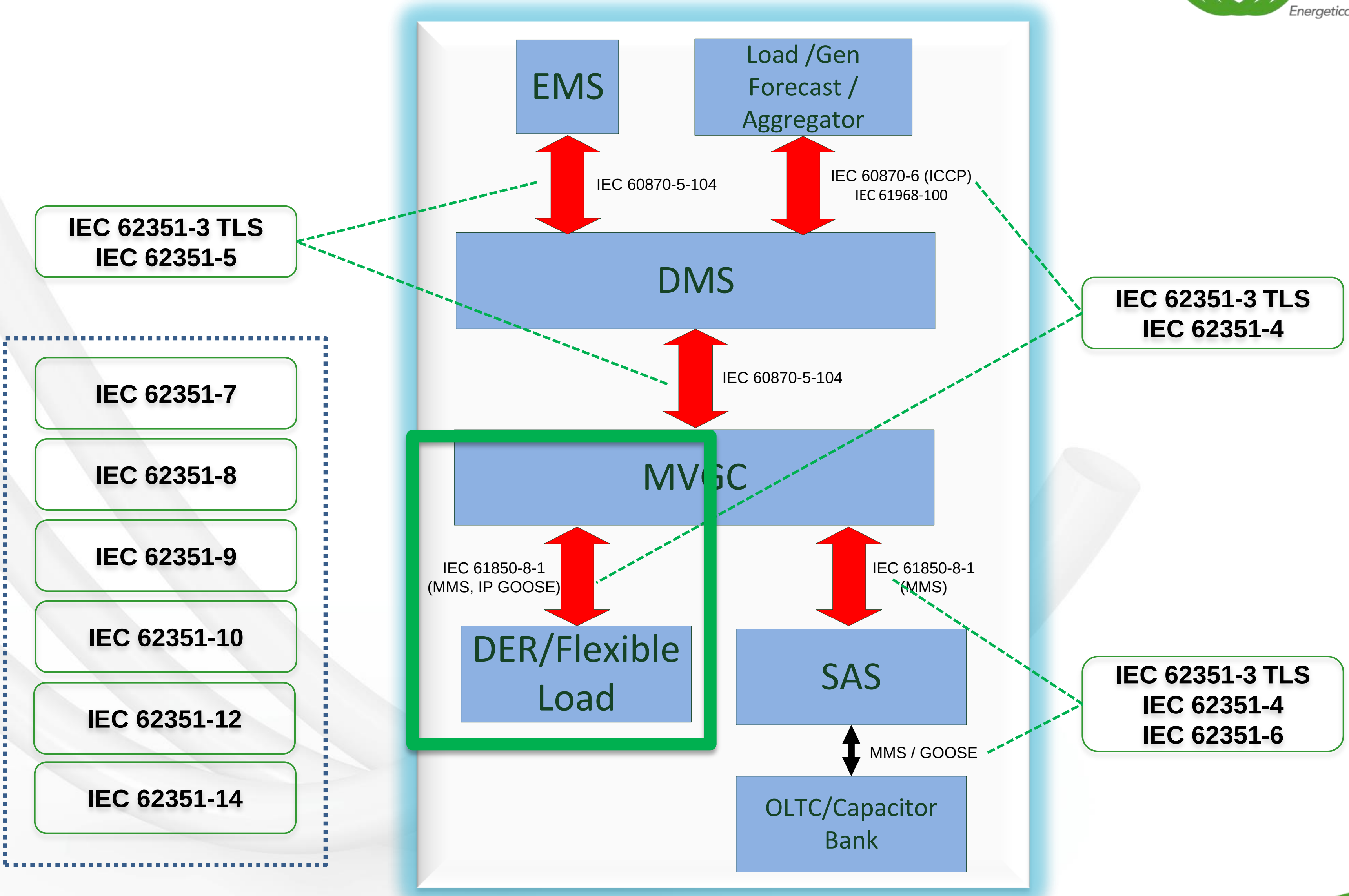
IEC 62351 Part 3,4,5,6,8,9
TLS
IPSec

IEC 62351 1-11
TLS
IPSec
SNMP
HTTPS, SSH

IEC 62351 Part 3
TLS
IPSec

IEC 62351 Part 3
IEC 62351 Part 9
TLS
IPSec

IEC 62351 in Voltage Control



EMS

Load /Gen Forecast / Aggregator

IEC 60870-5-104

IEC 60870-6 (ICCP)
IEC 61968-100

DMS

IEC 60870-5-104

MVGC

IEC 61850-8-1
(MMS, IP GOOSE)

IEC 61850-8-1
(MMS)

DER/Flexible Load

SAS

MMS / GOOSE

OLTC/Capacitor Bank

IEC 62351-3 TLS
IEC 62351-5

IEC 62351-3 TLS
IEC 62351-4

IEC 62351-3 TLS
IEC 62351-4
IEC 62351-6

IEC 62351-7

IEC 62351-8

IEC 62351-9

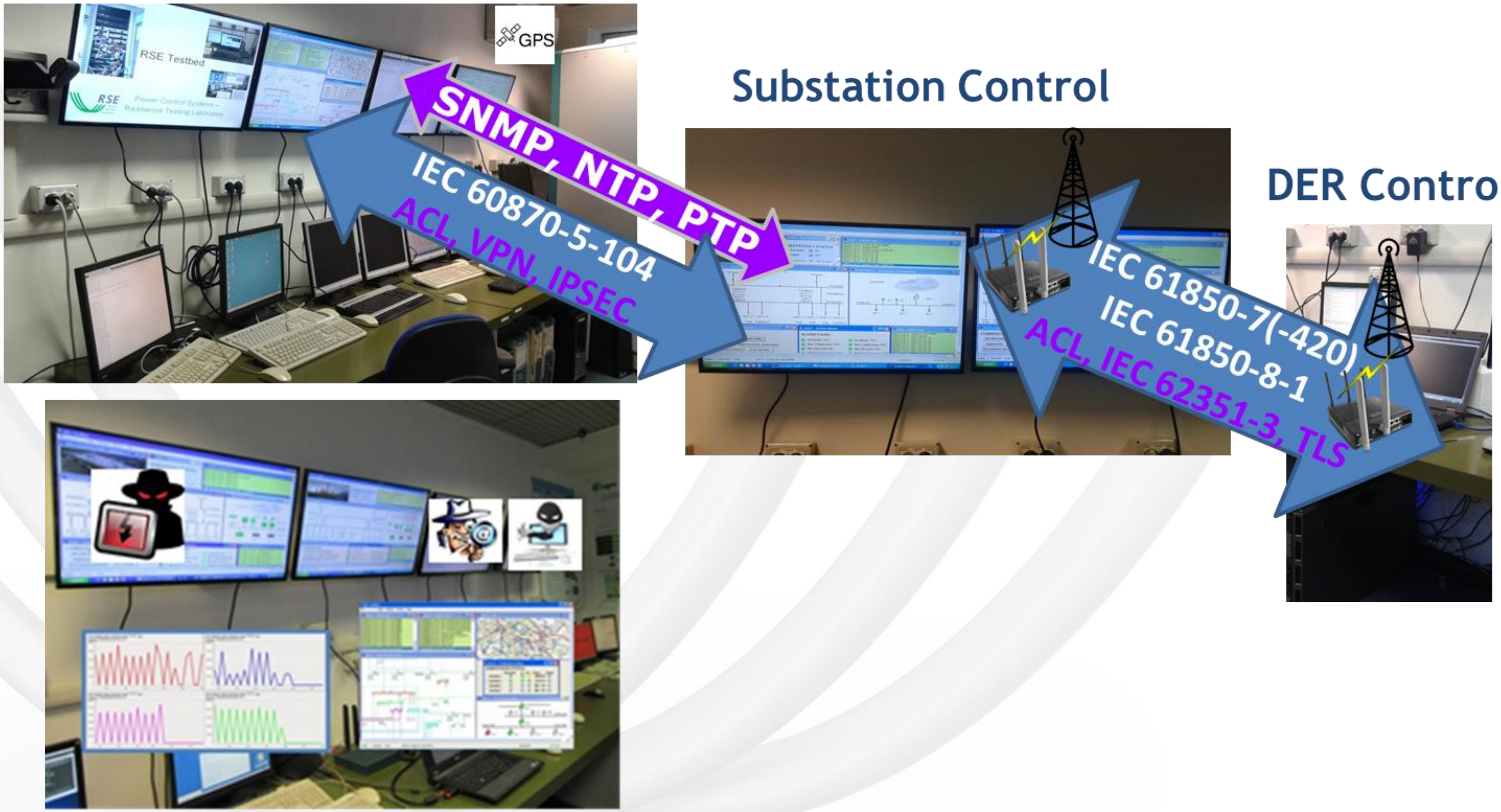
IEC 62351-10

IEC 62351-12

IEC 62351-14

RSE PCS-ResTest Lab

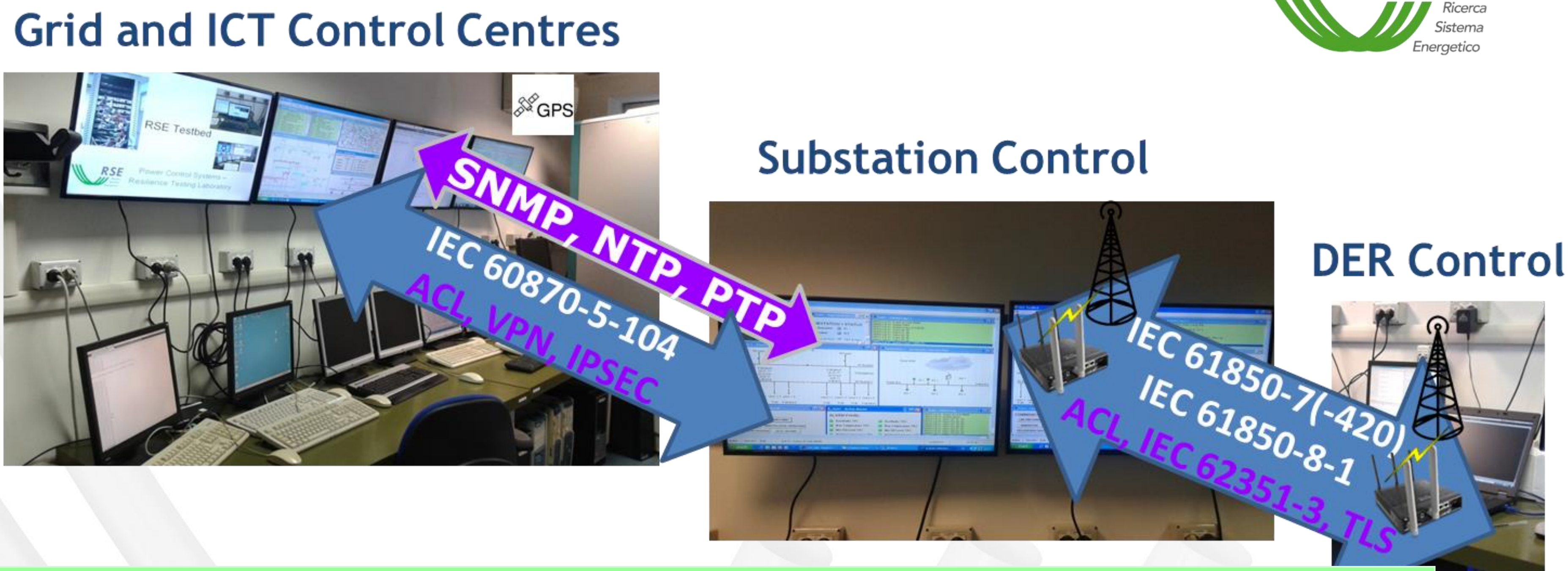
Grid and ICT Control Centres



Substation Control

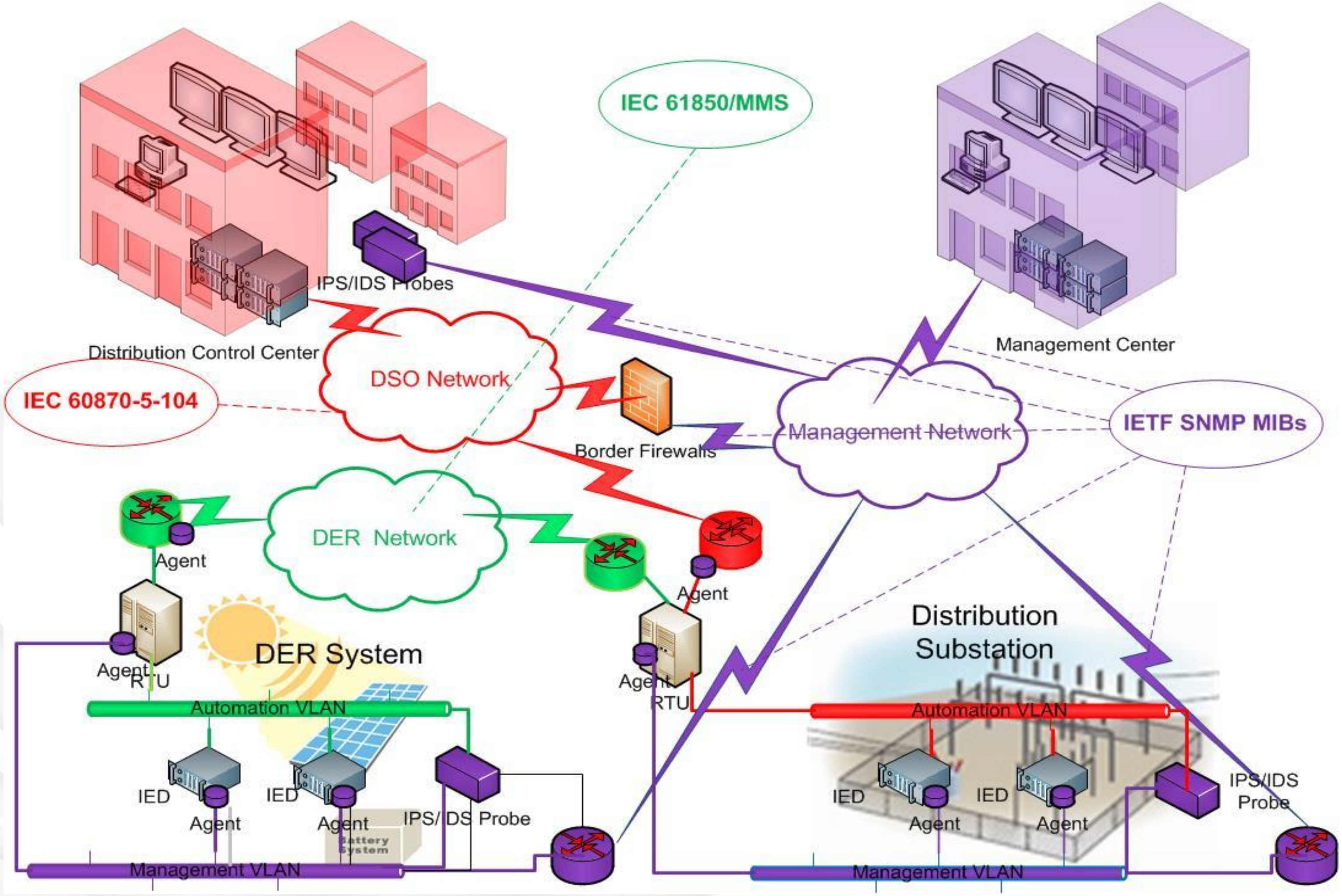
DER Control

PCS-ResTest lab

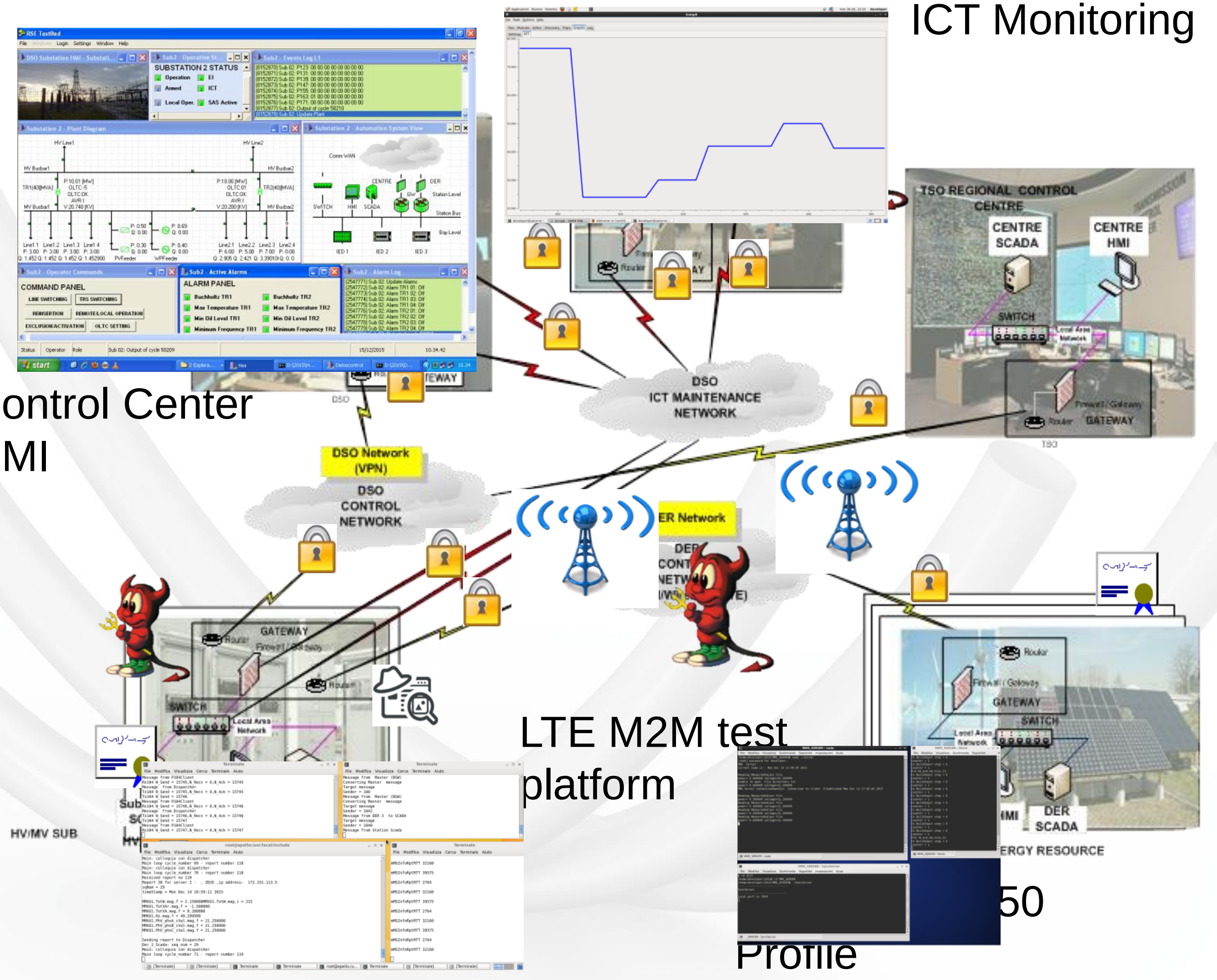


- Control applications →
  - DSO: Operation, Automation, Voltage Control (DER)
  - TSO/DSO: Load Shedding, Voltage Regulation
- Standard communications → data models, exchange protocols
- Standard security → confidentiality, integrity, availability, not repudiation
  - **preventive** → authentication and cyber channels
  - **defensive** → monitoring, detection, diagnosis, recovery
- Power contingencies / ICT anomalies (accidental, intentional)
  - **Attacks** → simple (UDP flooding), medium (reset), complex (malware)

Areas and Networks



Technologies and Tools



ICT Monitoring

Control Center HMI

LTE M2M test platform

50

Profile

- Communication modules
- Monitoring
- End to end Security
- Point to point Security
- 4G/3G/2G M2M
- Attack tools
- Visualisers
- QoS Analyser
- ICT network simulators

QoS Test Cases

Security Tests

Analysis of security overhead on communication performance

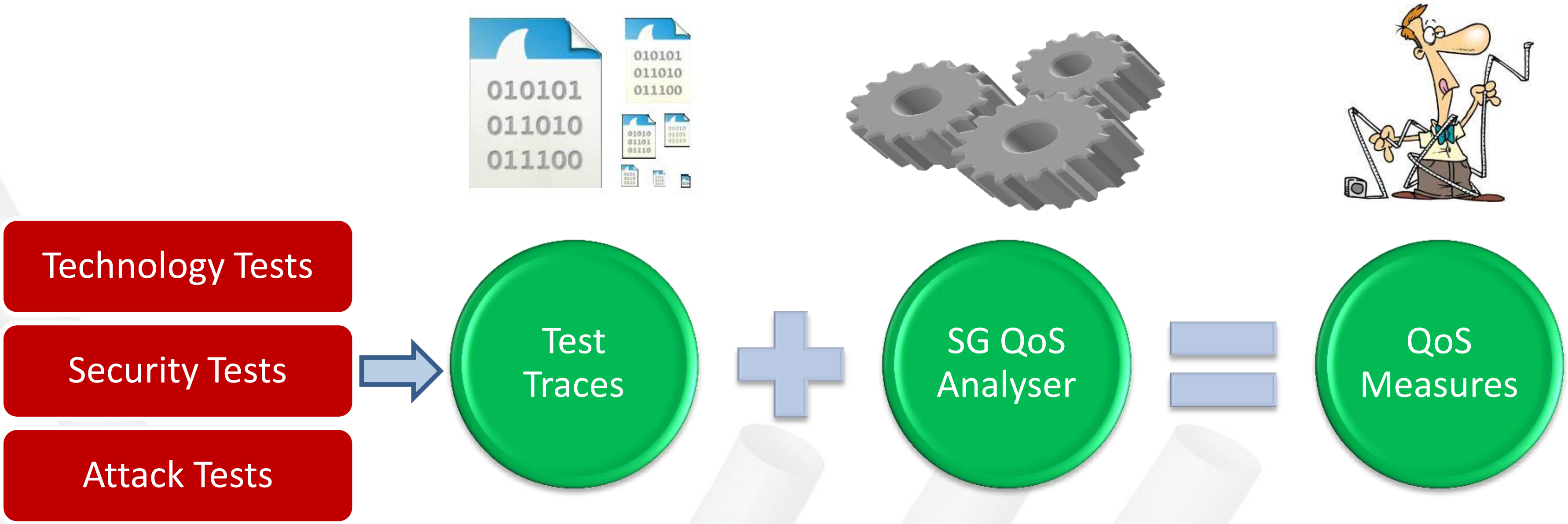
Technology Tests

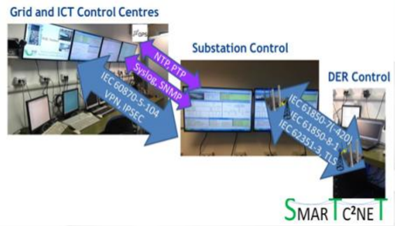
Analysis of communication performances with different communication technologies

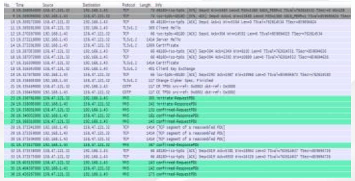
Attack Tests

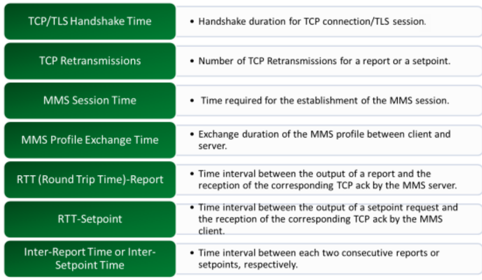
Analysis of attack effects on communication performances

QoS Measurements



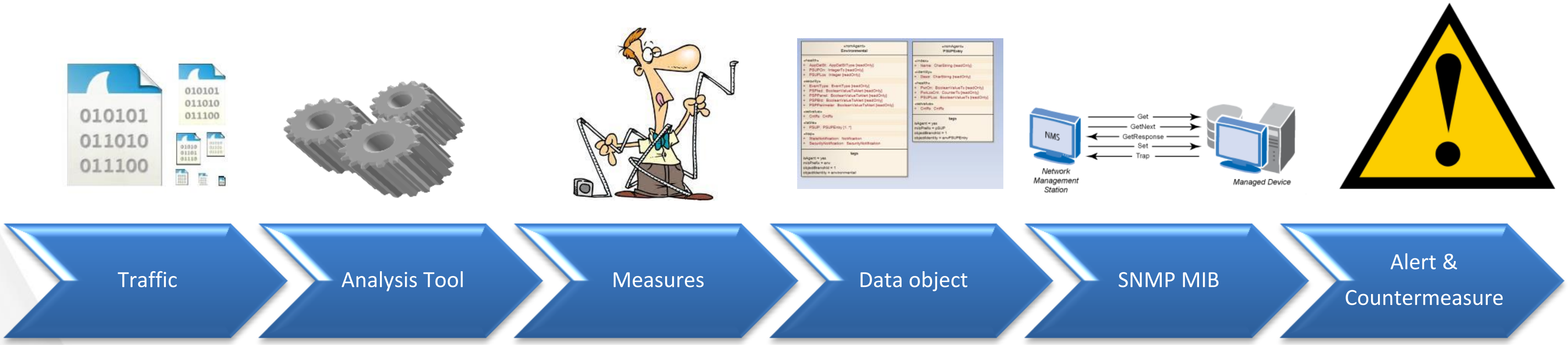






TCP/TLS Handshake Time	• Handshake duration for TCP connection/TLS session.
TCP Retransmissions	• Number of TCP Retransmissions for a report or a setpoint.
MMS Session Time	• Time required for the establishment of the MMS session.
MMS Profile Exchange Time	• Exchange duration of the MMS profile between client and server.
RTT (Round Trip Time)-Report	• Time interval between the output of a report and the reception of the corresponding TCP ack by the MMS server.
RTT-Setpoint	• Time interval between the output of a setpoint request and the reception of the corresponding TCP ack by the MMS client.
Inter-Report Time or Inter-Setpoint Time	• Time interval between each two consecutive reports or setpoints, respectively.

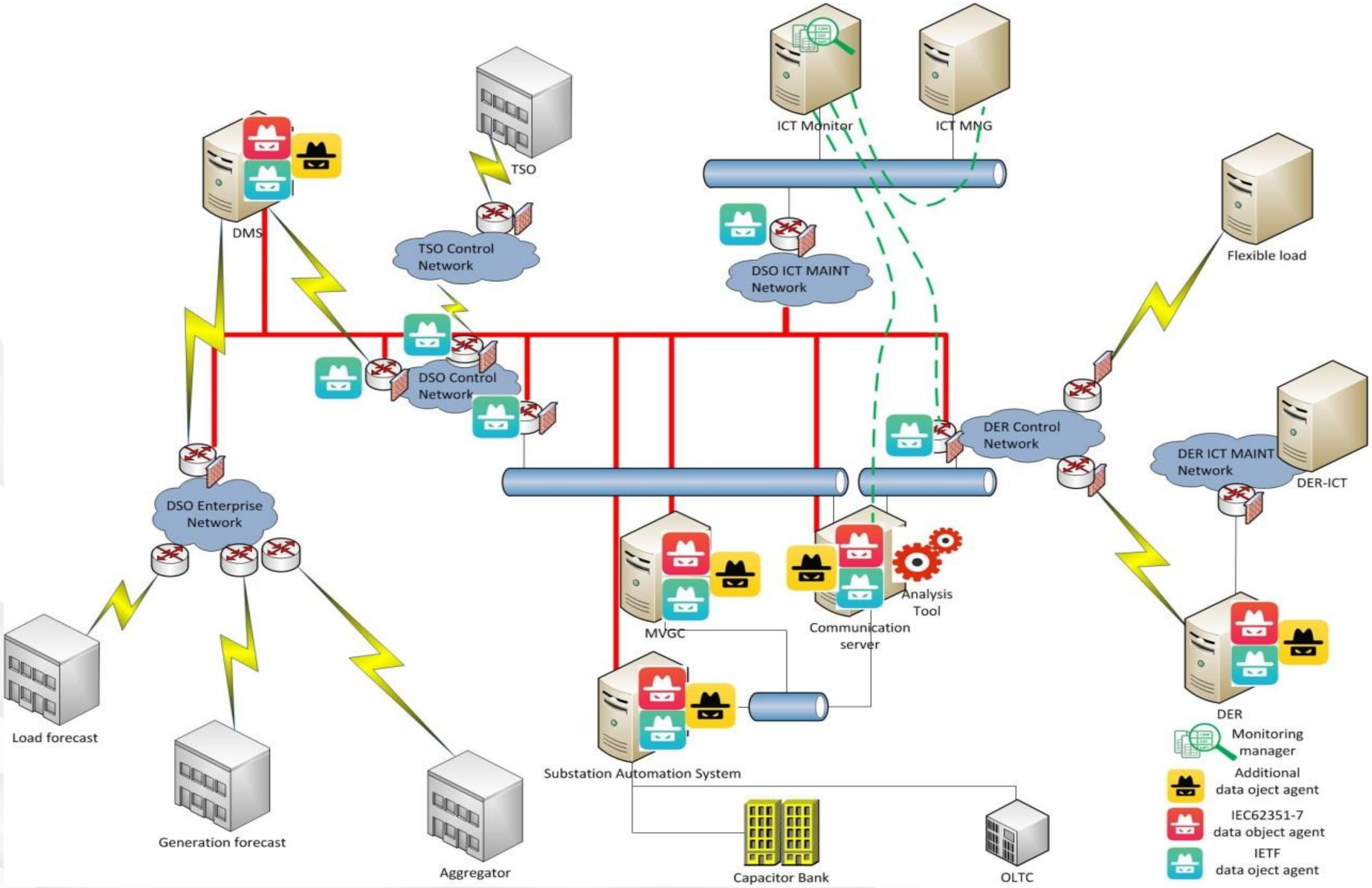
Monitoring Framework



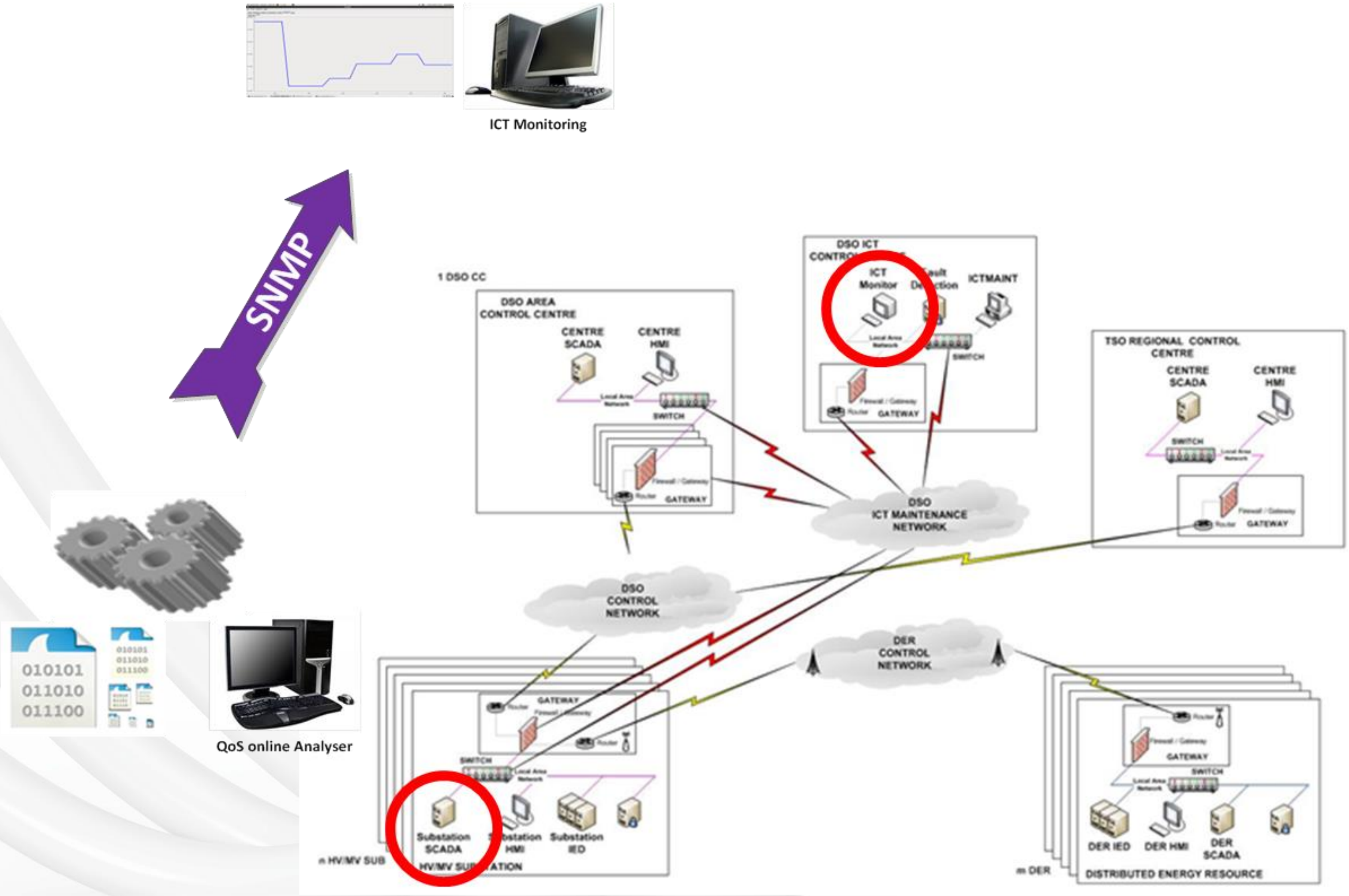
Traffic → Analysis Tool → Measures → Data object → SNMP MIB → Alert & Countermeasure

- **Analysis Tool** parses online network **Traces** and calculates the QoS **Measures** of monitored **Objects**
- **SNMP Agents** provide values of monitored **Objects** to **SNMP Managers**, i.e. ICT Monitoring and Fault Management, that signal **Alerts**
- Monitored **Objects** from VCTest Bed as part of the international standard IEC 62351-7

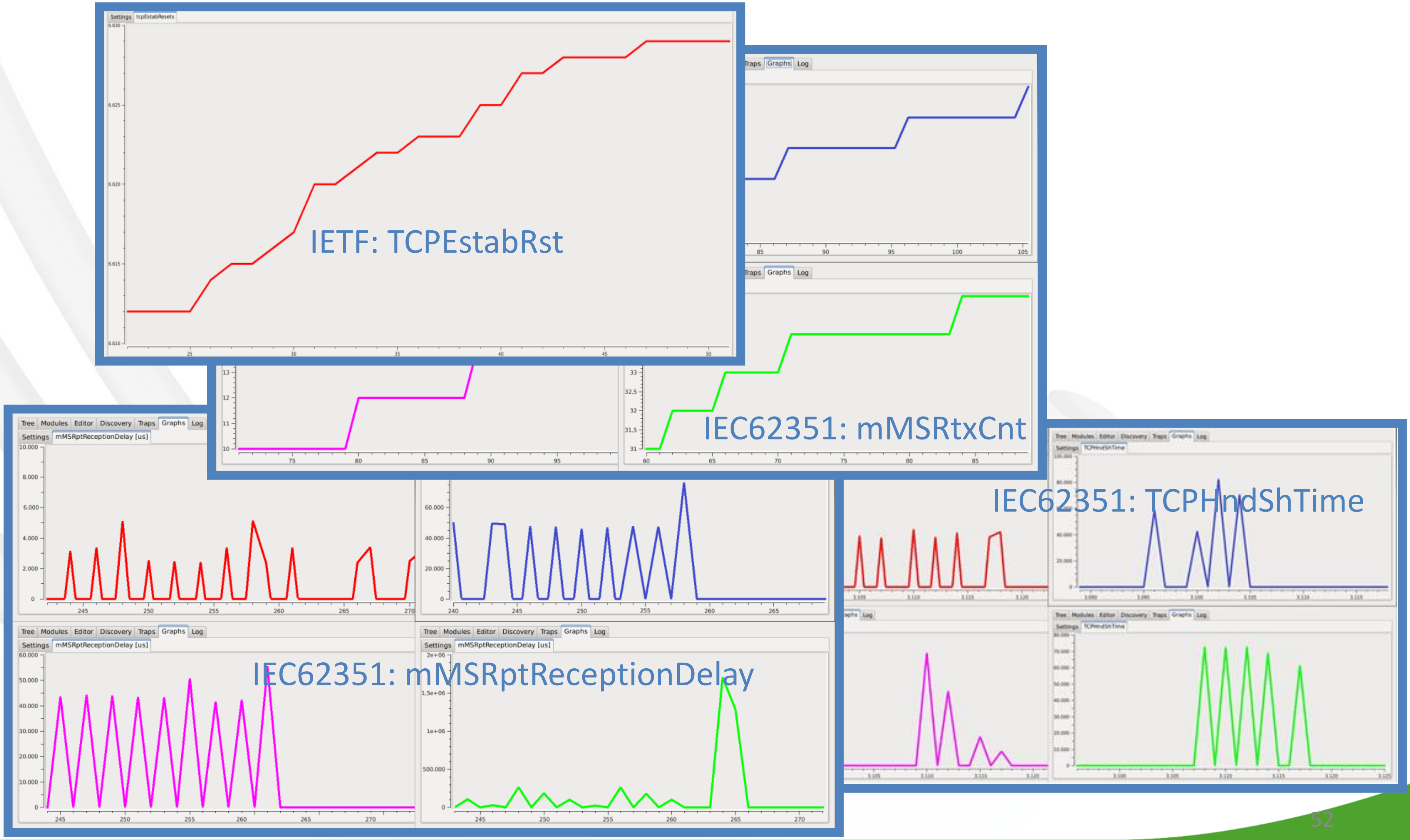
Monitoring Architecture



Monitoring Architecture (cont.)



Monitoring object visualization - communication under attack

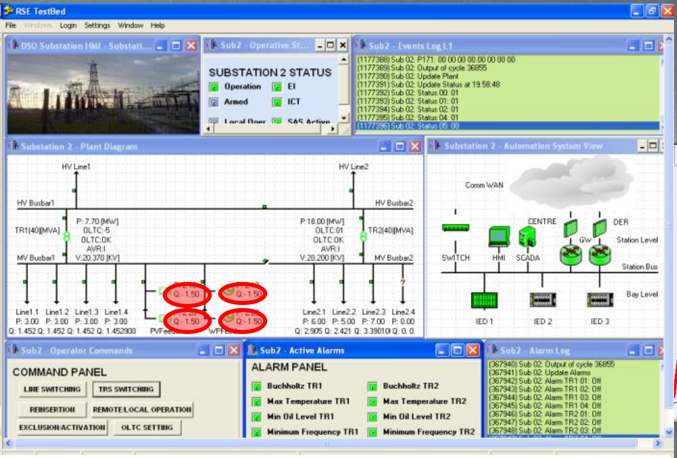

IETF: TCPEstabRst

IEC62351: mMSRtxCnt

IEC62351: TCPHndShTime

IEC62351: mMSRptReceptionDelay

PCS – ResTest Lab



SUBSTATION 2 STATUS

- ☑ Operation ☑ EI
- □ Armed ☑ ICT
- □ Local Oper ☑ SAS Active

```
(1177388) Sub 02: P171: 00 00 00 00 00 00 00 00
(1177389) Sub 02: Output of cycle 36855
(1177390) Sub 02: Update Plant
(1177391) Sub 02: Update Status at 19.58.48
(1177392) Sub 02: Status 00: 01
(1177393) Sub 02: Status 01: 01
(1177394) Sub 02: Status 02: 01
(1177395) Sub 02: Status 04: 01
(1177396) Sub 02: Status 05: 00
```

P: 7.70 [MW]
OLTC:-5
OLTC:OK
AVR:I
V:20.370 [KV]

P:18.00 [MW]
OLTC:01
OLTC:OK
AVR:I
V:20.200 [KV]

Line1.1	Line1.2	Line1.3	Line1.4
P: 3.00	P: 3.00	P: 3.00	P: 3.00
Q: 1.452	Q: 1.452	Q: 1.452	Q: 1.452900

Q:-1.50 Q:-1.50 Q:-1.50 Q:-1.50

Line2.1	Line2.2	Line2.3	Line2.4
P: 6.00	P: 5.00	P: 7.00	P: 0.00
Q: 2.905	Q: 2.421	Q: 3.39010	Q: 0.0

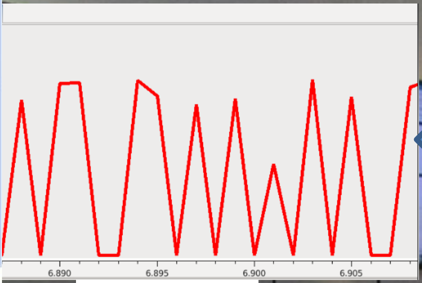
COMMAND PANEL

ALARM PANEL

- ☑ Buchholtz TR1 ☑ Buchholtz TR2
- ☑ Max Temperature TR1 ☑ Max Temperature TR2
- ☑ Min Oil Level TR1 ☑ Min Oil Level TR2
- ☑ Minimum Frequency TR1 ☑ Minimum Frequency TR2

```
(367940) Sub 02: Output of cycle 36855
(367941) Sub 02: Update Alarms
(367942) Sub 02: Alarm TR1 01: Off
(367943) Sub 02: Alarm TR1 02: Off
(367944) Sub 02: Alarm TR1 03: Off
(367945) Sub 02: Alarm TR1 04: Off
(367946) Sub 02: Alarm TR2 01: Off
(367947) Sub 02: Alarm TR2 02: Off
(367948) Sub 02: Alarm TR2 03: Off
```

SETPOINT (Q) 4 DER

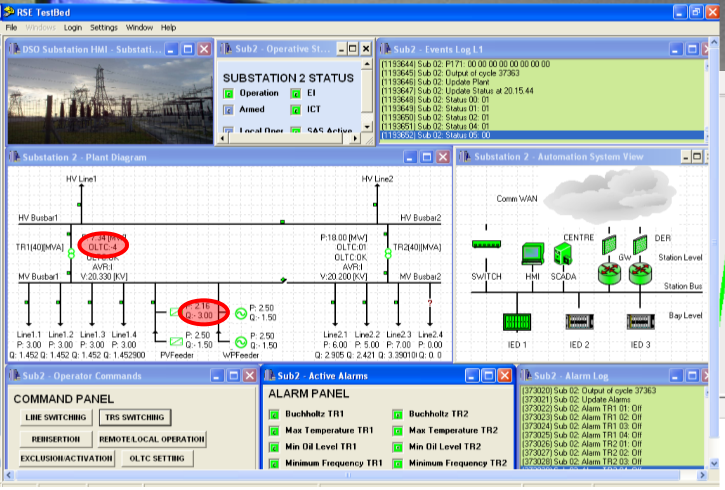


Report Delay

QoS

SCENARIO 1:
VERY HIGH GENERATION
NORMAL COMMUNICATIONS

PCS – ResTest Lab



SUBSTATION 2 STATUS

☑ Operation	☑ EI
☐ Armed	☑ ICT
☐ Local Oper	☑ SAS Active

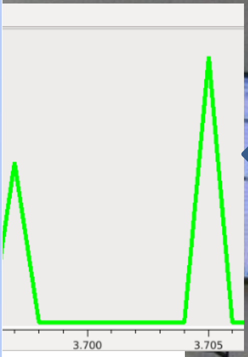
```
(1193644) Sub 02: P171: 00 00 00 00 00 00 00 00
(1193645) Sub 02: Output of cycle 37363
(1193646) Sub 02: Update Plant
(1193647) Sub 02: Update Status at 20.15.44
(1193648) Sub 02: Status 00: 01
(1193649) Sub 02: Status 01: 01
(1193650) Sub 02: Status 02: 01
(1193651) Sub 02: Status 04: 01
(1193652) Sub 02: Status 05: 00
```

COMMAND PANEL

ALARM PANEL

☑ Buchholtz TR1	☑ Buchholtz TR2
☑ Max Temperature TR1	☑ Max Temperature TR2
☑ Min Oil Level TR1	☑ Min Oil Level TR2
☑ Minimum Frequency TR1	☑ Minimum Frequency TR2

```
(373020) Sub 02: Output of cycle 37363
(373021) Sub 02: Update Alarms
(373022) Sub 02: Alarm TR1 01: Off
(373023) Sub 02: Alarm TR1 02: Off
(373024) Sub 02: Alarm TR1 03: Off
(373025) Sub 02: Alarm TR1 04: Off
(373026) Sub 02: Alarm TR2 01: Off
(373027) Sub 02: Alarm TR2 02: Off
(373028) Sub 02: Alarm TR2 03: Off
```



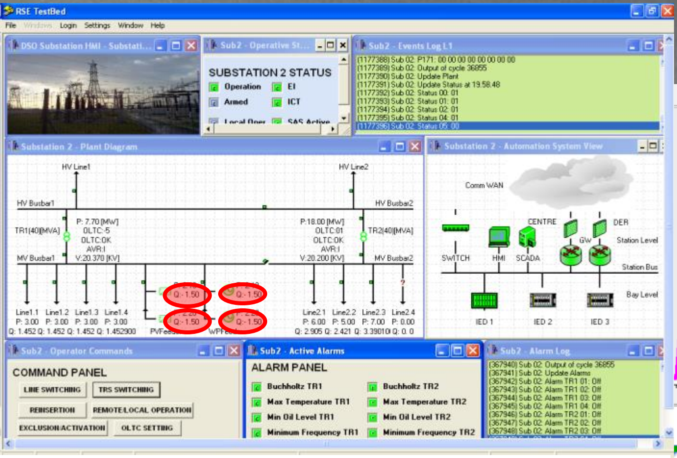
QoS

Report Delay

SETPOINT (Q) 1 DER
SETPOINT OLTC

SCENARIO 2:
VERY HIGH GENERATION
COMMUNICATIONS UNDER ATTACK

PCS – ResTest Lab



SUBSTATION 2 STATUS

- ☑ Operation
- ☑ EI
- □ Armed
- ☑ ICT
- □ Local Oper
- ☑ SAS Active

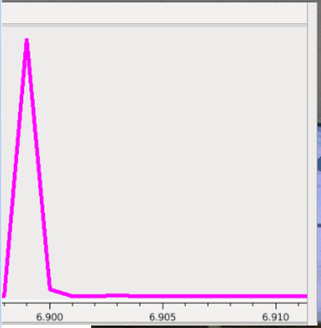
```
(1177388) Sub 02: P171: 00 00 00 00 00 00 00 00
(1177389) Sub 02: Output of cycle 36855
(1177390) Sub 02: Update Plant
(1177391) Sub 02: Update Status at 19.58.48
(1177392) Sub 02: Status 00: 01
(1177393) Sub 02: Status 01: 01
(1177394) Sub 02: Status 02: 01
(1177395) Sub 02: Status 04: 01
(1177396) Sub 02: Status 05: 00
```

COMMAND PANEL

ALARM PANEL

- ☑ Buchholtz TR1
- ☑ Buchholtz TR2
- ☑ Max Temperature TR1
- ☑ Max Temperature TR2
- ☑ Min Oil Level TR1
- ☑ Min Oil Level TR2
- ☑ Minimum Frequency TR1
- ☑ Minimum Frequency TR2

```
(367940) Sub 02: Output of cycle 36855
(367941) Sub 02: Update Alarms
(367942) Sub 02: Alarm TR1 01: Off
(367943) Sub 02: Alarm TR1 02: Off
(367944) Sub 02: Alarm TR1 03: Off
(367945) Sub 02: Alarm TR1 04: Off
(367946) Sub 02: Alarm TR2 01: Off
(367947) Sub 02: Alarm TR2 02: Off
(367948) Sub 02: Alarm TR2 03: Off
```



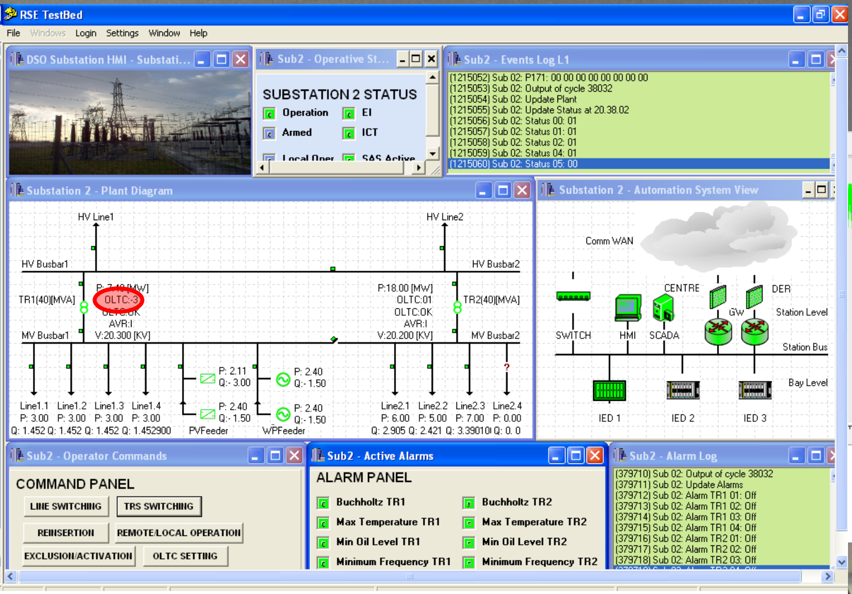
pS

SETPOINT (Q) 4 DER

Report Delay

SCENARIO 3:
VERY HIGH GENERATION
COMMUNICATIONS UNDER ATTACK
AUTOMATIC RECOVERY

PCS – ResTest Lab



SUBSTATION 2 STATUS

- ☑ Operation ☑ EI
- ☐ Armed ☑ ICT
- ☐ Local Oper ☑ SAS Active

```
(1215052) Sub 02: P171: 00 00 00 00 00 00 00 00
(1215053) Sub 02: Output of cycle 38032
(1215054) Sub 02: Update Plant
(1215055) Sub 02: Update Status at 20.38.02
(1215056) Sub 02: Status 00: 01
(1215057) Sub 02: Status 01: 01
(1215058) Sub 02: Status 02: 01
(1215059) Sub 02: Status 04: 01
(1215060) Sub 02: Status 05: 00
```

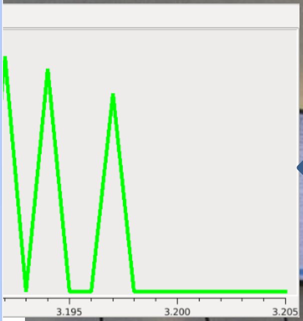
COMMAND PANEL

LINE SWITCHING | TRS SWITCHING | REINSERTION | REMOTE/LOCAL OPERATION | EXCLUSION/ACTIVATION | OLTC SETTING

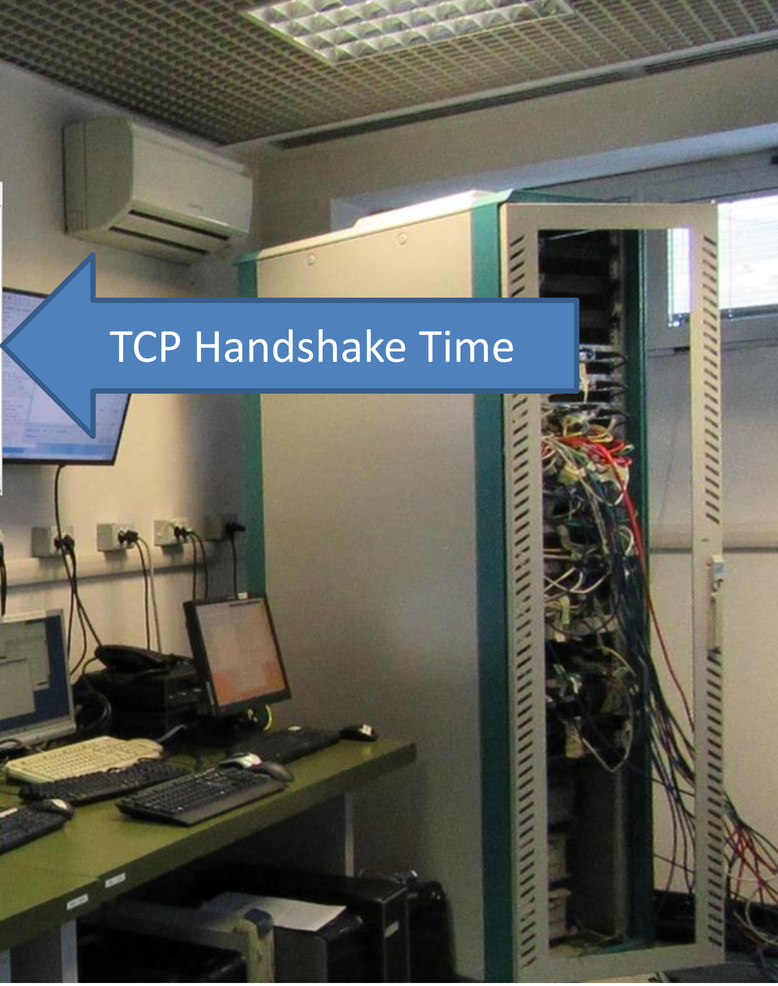
ALARM PANEL

- ☑ Buchholtz TR1 ☑ Buchholtz TR2
- ☑ Max Temperature TR1 ☑ Max Temperature TR2
- ☑ Min Oil Level TR1 ☑ Min Oil Level TR2
- ☑ Minimum Frequency TR1 ☑ Minimum Frequency TR2

```
(379710) Sub 02: Output of cycle 38032
(379711) Sub 02: Update Alarms
(379712) Sub 02: Alarm TR1 01: Off
(379713) Sub 02: Alarm TR1 02: Off
(379714) Sub 02: Alarm TR1 03: Off
(379715) Sub 02: Alarm TR1 04: Off
(379716) Sub 02: Alarm TR2 01: Off
(379717) Sub 02: Alarm TR2 02: Off
(379718) Sub 02: Alarm TR2 03: Off
```



TCP Handshake Time



SETPOINT OLTC

SCENARIO 4:
VERY HIGH GENERATION COMMUNICATIONS UNDER ATTACK ADAPTIVE CONTROL

Key messages

- Cyber security in Digital Energy is a priority
- Security standards have reached a good level of maturity
- Risk assessment is the most challenging phase of the security process
- Assessment of realistic energy control scenarios is an essential exercise
- Detect, respond and recover functions are needed for the situational awareness and the management of residual risks
- Cyber security in energy sector regulations is in progress

Thank you

Giovanna.Dondossola@rse-web.it

PCS_ResTest@rse-web.it