ETSI TR 103 644 V1.2.1 (2020-09)

CYBER;
Observations from the SUCCESS project regarding smart meter security

Reference
RTR/CYBER-0059

Keywords
cybersecurity, smart meter

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Cyber security of Critical Infrastructure (CI) is a serious and ongoing challenge that affects electricity, gas and water production and distribution networks up to a regional scale. The significance of ***cyber-physical infrastructure security*** substantially differs from cyber security in general, because of the implications imposed by the topology configuration that obeys specific laws of physics, for example Kirchhoff's laws for electricity. For example, effective cyber security analysis of *energy distribution infrastructure* is done in conjunction with *application security in power systems* to prevent, mitigate, and tolerate cyber-attacks.

In the past, digital measurement equipment was networked over privately owned and isolated power lines only. Currently, Energy Infrastructures use common and standardized communication protocols for *bi-directional communication*, including 5G and Internet protocols. In new scenario, previously unknown networked agents can interact with remote nodes of critical infrastructure. This fact has substantially changed the perception of cyber infrastructure security aspects in all business scenarios, including the metering one. As an effect, utility companies in general - and energy utilities specifically - require better safety measures, improved security, and highly reliable data protection.

In the past, digital equipment was designed, manufactured, and deployed to end users in order to enable desired business scenarios: it was a business dictating the functional specifications to lead the technology developments. For example, when electro-mechanical energy meters were replaced by the new-generation ones, the deployment country-wide of so called "smart" electronic energy meters it was driven by the requirement of *enabling remote reading* of metering data collections for billing purposes. On competitive mass-markets, the price of standard smart meters has been progressively reduced which ownership is retained by utility companies. As well as the price of the smart meters is low, it is unlikely that a manufacturer will be able to implement highly sophisticated cybersecurity measures in a cheap mass-market device because the extent of security of a machine relies on cost aspects. For this reason, the energy utilities have continued to consider smart meters as part of their infrastructure.

After the advent and widespread of Internet of Things (IoT) and Machine-to-Machine (M2M) technologies, billions of legacy smart meters were refurbished and differently networked over new channels in order to support more advanced business scenario prospected by so-called "reference scenario for Smart Grid 2.0" [i.16] and [i.17]. As an effect of this, in energy metering business domain, energy utilities have started *demanding new functionalities*. Examples are:

1) near real time measurements;

2) better accurate demand-oriented measurements;

3) power and energy quality data;

4) energy flow control features.

It caused a substantial change in the socio-technological latter of Smart Grid. Like any other Industrial Control System (ICS) slowly refurbished and gradually re-developed over past three decades, a metering infrastructure offering flow control functionalities contains software agents and mechanical relays deputed to execute remotely issued control sequences. At one side, the cybersecurity imposes the use of cryptography and other identity management techniques. At another side, the interoperability requirement in standard communication protocols imposes the network-wide communication between agents [i.8]. Moreover, the industrial control protocols impose the real time delay-less communication, which might conflict with some requirements dictated by the security protocols [i.9]. As a result, critical energy infrastructures host several differently dated classes of digital equipment that can be operated by using large number of different specifications. It opens up the possibility of cyber-attacks and manipulations of power and/or energy demand.

The corpus of scientific literature has amply documented the above evidences by proposing ad hoc counter-measures, but truly harmonized solution could be achieved thanks to the international standardization only. At one side, business companies will be invited to invest more money in order to update their digital measurement equipment by making it more safe and secure. At another side, the International Community challenges introducing an additional security layer in order to cope with anomalies/crimes affecting inter-utility and cross-country.

It appears evident that fulfilling functional requirements imposed by legacy business is not enough in a new technology scenario. For this reason, SUCCESS added a non-functional security requirement in order to evolve pre-existing electronic digital metering equipment. In data communication perspective, Smart Meters are low-cost IoT devices. To allow them to be better protected, new measurement devices can incorporate edge-based Security Agents (edge-SecA) deputed to trace and monitor the network traffic originated by remote Control Agents in new scenarios of next-generation Smart Grid (currently Smart Grid 2.0 [i.16]). As such, it is suggested to follow a common standard about the above-mentioned security-oriented feature in order to allow coordinated and homogeneous implementations of the security measures in the next-generation Multi-Agent Control System countrywide, Region-wide, and world-wide.

In the belief that the improved *security monitoring features* enable quicker risk management response, SUCCESS team challenged to standardize the *cooperative defence* against staged cyber-attacks since it represents a risk hedging measure that complements other risk-mitigation (whenever possible) features in critical infrastructures.

1 Scope

The present document is a report of the findings of the SUCCESS H2020 project with respect to the security of Smart Meters. The present document applies only to the SUCCESS environment, but extrapolates the recommendations to a wider view of security of Smart Meters. The present document therefore may be used to sponsor future work in smart meter security.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] "Functional reference architecture for communications in smart metering systems, CEN/CLC/ETSI/TR 50572".

[i.2] ETSI TS 104 001:"Open Smart Grid Protocol (OSGP); Smart Metering/Smart Grid Communication Protocol".

[i.3] ETSI TR 102 691: "Machine-to-Machine communications (M2M); Smart Metering Use Cases".

[i.4] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.5] "Secure Architecture for Industrial Control Systems".

NOTE: Available at https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

[i.6] "Next Generation Real-Time Smart Meters for ICT Based Assessment of Grid Data Inconsistencies".

NOTE: Available at https://www.mdpi.com/1996-1073/10/7/857.

[i.7] "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains".

NOTE: Available at https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[i.8] "European Commission's directive EU COM (2006) 786".

NOTE: Available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

[i.9] "European Parliament's report 2018/2088(INI), Report on a comprehensive European industrial policy on artificial intelligence and robotics".

NOTE: Available at http://www.europarl.europa.eu/doceo/document/A-8-2019-0019_EN.pdf.

[i.10] "European Commission's Directive 2006/42/EC, Machinery Directive".

NOTE: Available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF.

[i.11] "European Commission's Directive 2014/35/EU, Low Voltage Directive".

[i.12] "Syncretic Use of Smart Meters for Power Quality Monitoring in Emerging Networks".

NOTE: Available at https://ieeexplore.ieee.org/abstract/document/7536160.

[i.13] "Secure Architecture for Industrial Control Systems".

NOTE: Available at https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

[i.14] "NOBEL GRID" Project website.

NOTE: Available at https://nobelgrid.eu/.

[i.15] "IEEE Standards Interpretations for IEEE Std 1588™-2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

NOTE: Available at https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/interpretations/1588-2008_interp.pdf.

[i.16] "The Smart Grid: Enabling Energy Efficiency and Demand Response", Fairmont Press, C.W. Gellings, 2009.

[i.17] OpenADR 2.0: "Demand Response Program Implementation Guide".

NOTE: Available at https://www.openadr.org/assets/openadr_drprogramguide_1_1.pdf.

[i.18] "Next Generation Smart Meter", (V3) (final).

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/700416_deliverable_D3.9.pdf.

[i.19] "Solution Architecture and Solution Description" (V3).

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/700416_deliverable_D4.3.pdf.

[i.20] "Innovative approach to data privacy for energy services".

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/700416_deliverable_D4.10.pdf.

[i.21] "Information Security Management Components and Documentation".

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/700416_deliverable_D3_4.pdf.

[i.22] "Big Data in Critical Infrastructures Security Monitoring: Challenges and Opportunities", CoRR, vol. abs/1405.0325, (03 July 2014).

NOTE: Available at https://arxiv.org/abs/1405.0325.

[i.23] "Information Security Management Components and Documentation", (V3).

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/700416_deliverable_D3.6.pdf.

[i.24] "Description of Available Components for SW Functions, Infrastructure and Related Documentation", (V.3).

NOTE: Available at https://success-energy.eu/files/success/Content/Library/Deliverables/SUCCESS_D4.6_v28.pdf.

[i.25] "Cyber Kill Chain Defender for Smart Meters, Complex, Intelligent, and Software Intensive Systems", pp 386-397, (2019).

NOTE: Available at https://link.springer.com/chapter/10.1007/978-3-319-93659-8_34.

[i.26] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

NOTE: Available at https://tools.ietf.org/html/rfc3748.

[i.27] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol", (V1.2).

NOTE: Available at https://tools.ietf.org/html/rfc5246.

[i.28] "OAuth 2.0".

NOTE: Available at https://oauth.net/2/.

[i.29] IEEE EBCCSP (2017): "Secured Event-based Smart Meter".

NOTE: Available at https://ieeexplore.ieee.org/document/8022818.

[i.30] "On the security of SSL/TLS-enabled applications".

NOTE: Available at https://www.sciencedirect.com/science/article/pii/S2210832714000039.

[i.31] "The importance of a security, education, training and awareness program".

NOTE: Available at http://www.infosecwriters.com/Papers/SHight_SETA.pdf.

[i.32] "Critical Infrastructure Protection Review", (a report).

NOTE: Available at https://www.criticalinfrastructureprotectionreview.com/.

[i.33] "Reference Incident Classification Taxonomy".

NOTE: Available at https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

[i.34] "Lightweight Machine to Machine Technical Specification".

NOTE: Available at http://www.openmobilealliance.org/release/LightweightM2M/V1_0-20170208-A/OMA-TS-LightweightM2M-V1_0-20170208-A.pdf.

[i.35] IEC 61850: "Communication networks and systems for power utility automation".

NOTE: Available at https://webstore.iec.ch/publication/6028.

[i.36] IEC TS 62351-6: "Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850".

NOTE: Available at https://webstore.iec.ch/publication/6909.

[i.37] IEC 61850-9-2:2011 - "Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3".

NOTE: Available at https://webstore.iec.ch/publication/6023.

[i.38] "OASIS MQTT", (V5.0).

NOTE: Available at https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf.

[i.39] IEC 62056-1-0:2014 - "Electricity metering data exchange - The DLMS/COSEM suite - Part 1-0: Smart metering standardisation framework".

NOTE: Available at https://webstore.iec.ch/publication/6397.

[i.40] IEC TS 62056-1-1:2016 - "Electricity metering data exchange - The DLMS/COSEM suite - Part 1-1: Template for DLMS/COSEM communication profile standards".

NOTE: Available at https://webstore.iec.ch/publication/24735.

[i.41] IEEE 1588-2008™: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

NOTE: Available at https://standards.ieee.org/standard/1588-2008.html.

[i.42] GDPR (Reg. EU 679/2016).

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT.

[i.43] IEC TR 61850-90-5:2012: "Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118".

NOTE: Available at https://webstore.iec.ch/publication/6026.

[i.44] IEC/IEEE 61850-9-3:2016: "Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation".

NOTE: Available at https://webstore.iec.ch/publication/24998.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Complex System (CS): system composed of a big number of components, which can interact - individually or in groups - with each other

NOTE: The collective behaviour of parts of a CS entails emergence of properties that can hardly be inferred from properties of the parts. Some examples of distinct properties in a CS that arise from these relationships are: non-linearity, spontaneous order, feedback loops, adaptation. CS is a kind of network where the nodes represent the components and the links their interactions. The behaviour of CS might become uncertain due to different kinds of interactions between their parts or between a given system and its environment, for example dependencies, competitions, or relationships. After Aristotle, the CS is a system in which the whole is more than the sum of its parts.

composability: capability to select and assemble system components in various combinations into valid system to satisfy specific user requirements

NOTE: Composability is a system design principle that deals with the inter-relationships of components. The essential features of composability are: modularity (self-contained property) that allows deploying components independently and memoryless property that allows atomic transactions.

Critical Infrastructure (CI): infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population

NOTE: Examples include power plants, drinking water, hospitals and train lines.

cyber physical sub-systems: cyber-physical systems, which exhibit the features of systems of systems and can comprise components, which by themselves are not cyber-physical, e.g. computer systems which manage the overall system that consists of coupled cyber-physical subsystems, or a communication infrastructure

Cyber Physical System (CPS): integration of computation with physical processes

NOTE: CPS are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. In a CPS, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioural modalities, and interacting with each other in many ways that change with context. In other definition, CPS is defined as transformative technologies for managing interconnected systems between its physical assets and computational capabilities.

GRID: common term referring to an electricity transmission and distribution system

integratability: property of a system capable of undergoing integration or of being integrated

interoperability: ability of a system to exchange information between components and their aggregations (subsystems) and make use of information

Metering Infrastructure (MI): wide-area system deployed to support a number of business scenarios in which an actor offers the energy-containing commodity and the energy services and other actors consumes them

NOTE: Advanced Metering Infrastructure (AMI) contains different digital equipment: Smart Meters, Metering Concentrators, Automated Meter Reading (AMR), Metering Data Collection & Management sub-systems and more. MI and its constituents are part of Smart Grid.

Power Application (PA): collection of operational control functions necessary to maintain stability within the physical power system

Smart Grid (SG): supply network (principally electricity network) that intelligently integrates the behavior and actions of all users connected to it - generators, consumers and those that do both - in order to efficiently ensure a more sustainable, economic and secure electricity supply

Smart Meter (SM): meter with additional functionalities one of which is data communication

Supporting Infrastructure (SI): cyber infrastructure including software, hardware, and communication networks

System of Systems (SoS): viewing of multiple, dispersed, independent systems in context as part of a larger, more complex system

NOTE: A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
API	Application Programming Interface
BR-GW	BReakout GateWay
CA	Certificate Authority
CI	Critical Infrastructure
CI-SAN	Critical Infrastructure Security Analytics Network
CI-SOC	Critical Infrastructure Security Operations Centres
CKC	Cyber Kill Chain
COSEM	COmpanion Specification for Energy Metering
CPP	Country Privacy Profile
CPS	Cyber-Physical Systems
CPU	Central Process Unit
CRC	Cyclic Redundancy Check

CS	Cyber Security
CSA	Central Security Agent
CSMS	Cyber-Security Monitoring Solution
DCS	Data Centric Security
DFT	Discrete Fourier Transform
DLMS	Device Language Message Specification
DoS	Denial of Service
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assesment
DSF	Demand Side Flexibility
DSO	Distribution System Operator
DSS	Decision Support System
DV	Double Virtualization
EAP	Extensible Authentication Protocol
ENISA	European Network and Information Security Agency
ESCO	Energy Service Company
FPGA	Field-Programmable Gate Array
GBA	Generic Bootstrapping Architecture
GDPR	General Data Protection Regulation
GOOSE	Generic Object Oriented Substation Events
GPIO	General Purpose Input/Output
GPS	Global Positioning System
GSE	Generic Substation Events
HMI	Human-Machine Interface
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control Systems
ICT	Information & Communication Technology
IoT	Internet of Things
IP	Internet Protocol
ISGT	Innovative Smart Grid Technologies
ISO	Internation Standardization Organisation
IT	Information Technologies
IT/OT	Information Technologies/Operational Technology
KMM	Key Management Module
LAN	Local Area Network
LCPMU	Low Cost PMU
LPA	Local PUF Agent
LV	Low Voltage
LwM2M	Lightweight Machine to Machine
MAC	Message Authentication Code
MAS	Multi-Agent System
MDMS	Metering Data Management System
MI	Metering Infrastructure
MitM	Man-in-the-Middle attack
MQTT	Message Queue Telemetry Transport
NAN	Neighbor Awareness Networking
NORM	Next-generation Open Real time smart Meter
NORM-SMG	Next generation Open Real time smart Meter - Smart Meter Gateway
NTP	Network Time Protocol
OS	Operation Systems
OSGP	Open Smart Grid Protocol
OSI	Open Standards Institute
PA	Power Application
PMU	Phase Measurement Unit
PP	Privacy Profiles
PPS	Pulse Per Second
PS	Physical Security
PTP	Precision Time Protocol
PUF	Physically Unclonable Function
RAM	Random Access Memory
RBAC	Role Based Access Control

REST	Representational State Transfer
ROCOF	Rate Of Change Of Frequency
SA	Security Analytics
SAA	Security Administration Agent
SbD	Security by Design
SCADA	Supervisory control And Data Acquisition
SDC	Security Data Concentrator
SDN	Software Defined Networking
SecA	Security Agent; edge-based or cloud-based (edge-SecA, cloud-SecA)
SG	Smart Grid
SHA-256	Secure Hash Algorithm - 256
SI	Supporting Infrastructure
SM	Smart Meter
SMDC	Smart Metering Data Concentrators
SMG	Smart Meter Gateway
SMM	Smart Metrology Meter
SMX	Smart Meter eXtension
SOC	Security Operations Centre
SUCCESS	SecUring CritiCal Energy infraStructureS
TEC	Transactive Energy Control
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSO	Transmission and System Operator
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UPP	User Privacy Profile
USM	Unbundled Smart Meter
UUID	Unique Universal IDentifier
VLAN	Virtual Local Access Network
VPN	Virtual Private Network
WAMS	Wide-Area Monitoring System

4 Security Monitoring Framework and its Components

4.1 Introduction to the Security Monitoring Framework

4.1.1 Overall architecture

The present document proposes a new Security Monitoring Architecture for metering infrastructures. This architecture was initially created by the EU-funded SUCCESS (Horizon-2020) project and is generalized in the present document. The Security Monitoring Architecture proposes a two-level Cyber-Security Monitoring Solution (2-level CSMS) as depicted in Figure 1. It aims at making the critical infrastructure of a cyber-physical system more secure and more reliable by embedding security functionality as part of the system of systems. Such an approach allows to continue enabling a business functionality while continuously tracking the utilization of said functionality by any remote networked agent.

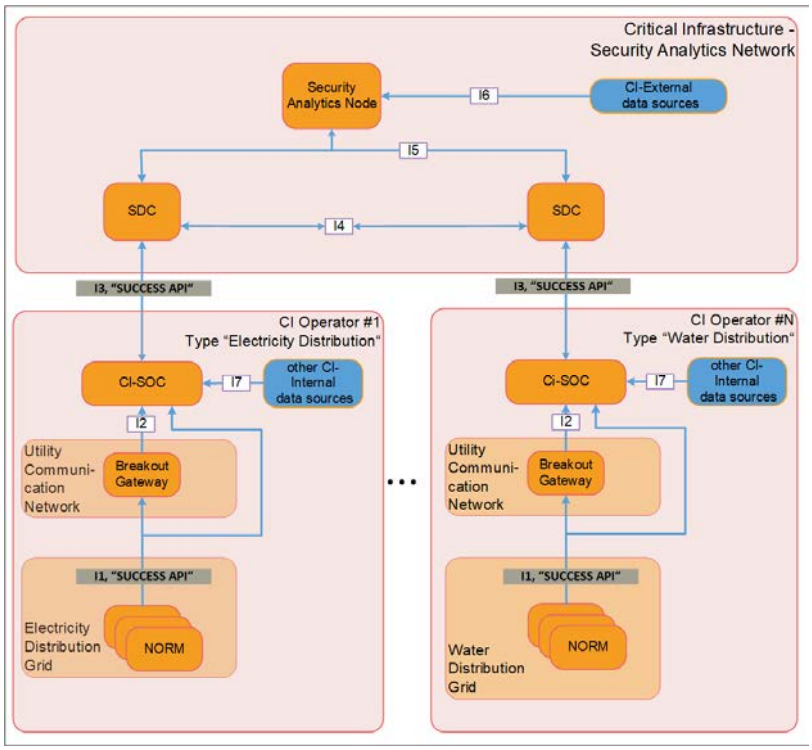

Figure 1: Security Monitoring Framework [i.19]

One level of the said system is designed for the *individual* Critical Infrastructure operator as presented in Figure 1. Another level of the same system is set at a regional level to integrate and share knowledge among *the universe of all* the operators [i.4], [i.19]. The two individual levels are interconnected with each other through the so-called SUCCESS API. Hence, the proposed solution *enables monitoring for cyber-security incidents* on two levels. Firstly, security monitoring is performed at the Critical Infrastructure level, typically it is a DSO business actor when considering energy business, a *Critical Infrastructure Security Operations Centre* (CI-SOC) monitors the field equipment, communications infrastructures and any other relevant data sources of a Critical Infrastructure, trying to detect security incidents. Any *detected event being recognized as an incident* can indicate to proper countermeasures being initiated by the CI-SOC. Secondly, the monitored information regarding identified incidents and countermeasures, are sent by CI-SOC *to the second level* in the SUCCESS Security Monitoring Framework. This level, called the *Critical Infrastructure Security Analytics Network* (CI-SAN), serves as a regional network for exchanging security incidents and countermeasures information.

Additionally, as CI-SAN is an infrastructure capable of monitoring the cyber-security of the various Critical Infrastructures present in different countries, it represents an extensive view of the critical infrastructures (CI) security status.

As a way to have regional coverage, CI-SAN is designed as a system with two hierarchical levels, which consist of distributed instances:

- The Security Data Concentrator (SDC) represents the lower level which carries out information gathering across local instances.
- The Security Analytics Node (SA Node) represents the upper level analysing the information coming from instances at regional, national or international level.

It is possible to have a correspondence of the possible coverage areas of the upper and lower levels which denote that the instances' layout in the lower and upper levels can be designed to consider and face local, regional and national conditions. Thus, a regional security analytics network is made up of both levels in CI-SAN containing a set of distributed instances.

The SDC instances, on the lower level of the CI-SAN, collect information coming from the Critical Infrastructures in the local areas where they are located. This information is collected not only from the Critical Infrastructures but also from other local information sources. Furthermore, each SecA Node instance on the upper level of the CI-SAN collects information coming from the SDC instances pertaining to its area and from other sources. The information collected by each SecA Node instance is used to identify security incidents by analysing those data for patterns related to cyber-attacks or physical attacks. Then, this information about the security incidents is both shared, through the SDCs, between the SecA Nodes and alert Critical Infrastructure operators (e.g. DSOs or TSOs in the case of the electrical grid critical infrastructure).

SUCCESS has developed a secure Smart Meter Gateway called Next-generation Open Real time smart Meter (NORM), which offers to the customers secure services. Accordingly, SUCCESS's method to threat and countermeasure analysis id focused on the vulnerabilities that could come directly from the Smart Meters and their associated architecture. In the SUCCESS architecture, data to the CI-SOC is provisioned by the NORM. CI-SOC provisions its local SDC instances with information on grid status and possible countermeasures.

SUCCESS has developed the Breakout Gateway (BR-GW), which represents a new mobile communications network function. It carries out the mobile core network functionality on an edge cloud system situated at the eNodeB (5G mobile systems' radio base station). The BR-GW performs also distributed edge processing, by allowing distributed automation functionality to be performed at the edge of the power network. Furthermore, real-time countermeasures to cyber-attacks can be executed by the BR-GW.

The security incidents detection and the countermeasures application in SUCCESS are implemented in a hierarchical approach ensuring defence-in-depth. CI-SAN is on the top of the detection pyramid, it detects security incidents. Because of the impact of the possible consequences, CI-SAN warrants a conscious decision from the responsible authorities, and does not itself automatically start countermeasures, but will send a broadcast alert to all parties involved about the possibility of a cyber-attack happening and will inform the CI-SOC, which can begin the proper countermeasures. Both the Critical Infrastructure Security Operations Centre (CI-SOC) and the Breakout Gateway (BR-GW) have a more limited sphere of action, however, they are able to autonomously initiate countermeasures.

The SUCCESS security Monitoring Framework, shown in Figure 1, is made up of multiple components. A distributed security monitoring solution represents the core of it, used for monitoring the DSO network and its events using Critical Infrastructure Security Operations Centres (CI-SOC), at the DSO level. The CI-SOC is in charge of analysing the legacy traffic, signalling and state information reaching the DSO as well as information reporting from the network components on anomalous behaviour. The SUCCESS components NORM and BR-GW send this additional information. The BR-GW is co-located with the 3GPP base station and analyses the integrity of traffic at the edge of the 3GPP access network. BR-GW can use Data-Centric Security (DCS) to verify the message integrity and analyse client devices' traffic patterns. The NORM component represents a Smart Meter Gateway, it gathers grid measurements from the Smart Meters or Phasor Measurement Units (PMU) and sends them to the CI-SOC via the BR-GW. Virtual Private Network (VPN) and Physically Unclonable Function (PUF) technologies are used by NORM to have secure communications with BR-GW and CI-SOC.

The SUCCESS API (I1 and I3 in Figure 1) enable information exchange between Critical Infrastructure level and regional level in the Critical Infrastructure Security Analytics Network. The SUCCESS API consist of the following interfaces:

- Interfaces I-1 (between NORM and CI-SOC or BR-GW).
- Interfaces I-3 (between CI-SOC and SDC).

The SUCCESS API enables the information exchange about:

1) detection of a security incident;
2) countermeasures triggering and advising; and
3) additional payload between the SUCCESS components.

Payload data represent grid status dat (acquired by NORM) or the IT infrastructure data (acquired by e.g. firewall log files). Critical Infrastructure operators are meant to use the SUCCESS API. Allowing interoperability of different components and flexible, downstream implementation of additional threats and countermeasures is the main purpose of the SUCCESS API. The data exchanged on the API are restricted and subject to security controls, thus no data related to private persons are exchanged on the SUCCESS API. All the sensitive data are anonymized and private data protected.

The SUCCESS API provides unified definitions of how grid-state data can be made available by the DSOs, in the case of the Distribution Grid critical infrastructure. By analysing and comparing these data at different levels can reveal anomalies, which can be caused by physical, or cyber-attacks. Consequently, the holistic security approach of SUCCESS is implemented by the communication via the SUCCESS API, which includes multiple tiers for the detection of a security incident and the start of countermeasures.

4.1.2 Critical Infrastructure Security Operations Centre (CI-SOC)

4.1.2.1 Introduction

The *security of* critical infrastructure is different compared with the cyber-security in computer systems mainly because of the complexity (since any CI is a materialization of a complex system). The key issue depends on different kinds of interactions between parts or between a given system and its environment, an aspect that might cause an uncertain behaviour of the entire critical infrastructure due to dependencies, competitions, or relationships [i.8], [i.9] and [i.10]. The elimination of the factors that can make the CI vulnerable and susceptible to cyber misuse, along with the enhancement of the overall robustness, represent the main challenge regarding *cyber security of critical infrastructures.* Thus, the implementation of techniques that are able to ensure the reliability, performance and manageability of critical infrastructures represent the aim of cyber security systems.

The state of the art literature acknowledged these concerns and established compliance requirements to enforce baseline cybersecurity efforts [i.32] throughout the bulk power system. Current events have shown attackers using increasingly sophisticated attacks against Industrial Control Systems while numerous countries have acknowledged that cyber-attacks have targeted their critical infrastructures.

SUCCESS considered security of critical infrastructure as the *functional composition of* the following:

1) the physical components and control applications;

2) the cyber infrastructures required to support necessary planning, operational, and market functions;

3) the correlation between cyber-attacks and the resulting physical system impacts; and

4) the countermeasures to mitigate risks to critical infrastructure as a whole from cyber threats.

For Smart Grid, the *cyber sub-systems*, consisting of electronic field devices, communication networks, substation automation systems, and control centres, are embedded throughout the physical grid for efficient and reliable generation, transmission, and distribution of power. The control centre(s) is responsible for real-time monitoring, control, and operational decision making. There is an operator that performs coordination between power utilities, and dispatch commands to their control centres. Utilities that participate in power markets also interact with other actors supporting market functions based on real-time power generation, transmission, demand management and more. As such, the present document addresses the *coupling between* the power control applications (1) and cyber systems (2), including *composability aspects* in complex systems.

CI-SOC protects critical infrastructures from cyber-attacks by identifying threats and countermeasures by creating a list of mitigation actions. Thus CI-SOC represents a real-time decision support system that protects the Neighbour Awareness Networking (NAN) assets of the smart grid by extracting, from detected and already mitigated threats, tailored countermeasures. Its main operation s based on real-time and historical data processing. These data are gathered from smart meters and PMU devices across the local area of DSO that belongs to a given local area. CI-SOC supports a regional strategy for the threat detection supplying to the CI-SAN component information from DSOs across region and enabling it to obtain information that cannot be deduces from local level. An internal repository with a set of countermeasures and solutions from both real-time situations and from the literature to give an overview of the options to deal with the identified cyber threats that occur to the smart grid is uses by CI-SOC.

CI-SOC represents a scalable, reliable and robust tool able to detect cyber and physical threats that may affect the Smart Grid. It is designed to mitigate these threats in an effective way through the identification of proper countermeasures. CI-SOC matches and correlates possible new and old threats with the most suitable security actions and countermeasures related to the specific application scenario of the Neighbour Awareness Networking (NAN) level smart devices. As a result, the CI-SOC has three main functionalities:

1) threats monitoring and detecting;

2) identification of the most appropriate countermeasures;

3) provision a threat monitoring and detection intuitive user interface.

These functionalities enable the CI-SOC to identify and execute countermeasures against the threats related to the devices placed on customer premises or in public spaces. The principal goal is to guarantee the security Smart Meters and their communications with the DSOs and other relevant actors. Real-time possible threats that can invalidate a smart grid at NAN level can be detected by CI-SOC. It detects and identifies a possible ongoing attack, by using innovative algorithms, to an electrical device, smart meter or any other items placed in NAN, providing a set of the main suitable countermeasures, among those available, able to face and mitigate the impact of such attacks. Figure 2 shows the CI-SOC principal conceptual components and their main relationships.

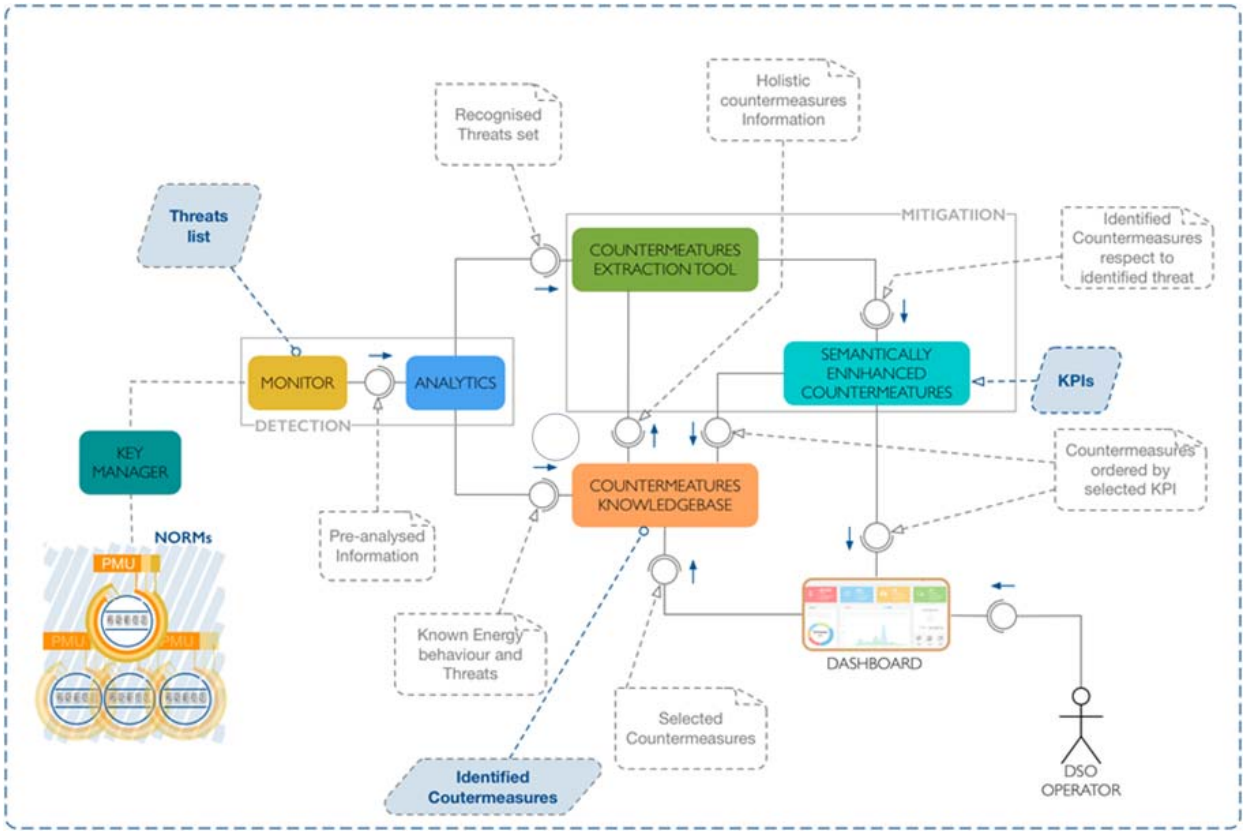

Figure 2: CI-SOC Conceptual Architecture [i.21]

The data coming from the smart meter are captured by the **monitor** and after a preliminary analysis, the pre-analysed data are sent to the analytic tool.

The **analytic tool** is in charge of analysing the data concerning the threats identified.

The **countermeasure extraction tool** selects all possible appropriate countermeasures for each identified threat, once some threats are detected.

The **countermeasure knowledgebase** contains the list of countermeasures to use. This component is a very intelligent repository: each time a countermeasure is selected taking into account the several indicators including resilience time and out-of-service time, it enriches the information about the countermeasures identified learning from the previous SUCCESS system reactions and improving its knowledge through machine-learning mechanisms.

The **semantically enhanced countermeasure tool** ranks them according to KPIs, once the suitable countermeasures are identified. Therefore, the DSO operator can select the appropriate indicators and decide which countermeasure applies:

- The CI-SOC system offers the DSO an instrument able to detect smart grid cyber-physical threats - and also enables the application of suitable mitigation measures supporting the coordination, control and communication mechanisms of the various countermeasures procedures. CI-SOC is able to monitor and analyse a variety of different NORM components for the real-time analysis of the different smart grid NAN assets but it also has the ability to provide and receive information from the upper regional level supporting the possibility to detect a threat not only on local level but also on regional level. Considering the entire Security Monitoring Architecture it interacts with different devices, exchanging information. CI-SOC principal functionalities are summarized as follows: NORM communication - this functionality is used to set up communication with NORM, relying both on software and hardware security protocols, to provision energy-related information. This operation entails the analysis of local phases and voltages related to different types of Distributed Energy Resources (DERs) infrastructure behind each NORM. In order to assure secure communication with the CI-SOC NORM encompasses two different security layers:

  - the first one based on standard channel encryption techniques; and
  - the second one based on hardware cryptographic operations.

  As the CI SOC and administrator have access to the trusted zone of Smart Meter Gateway (SMG) which operates both as communication and functional gateway, they require a higher security level. These encryption and cryptographic operations are coordinated by the Security Agent (SecA) which is also in charge of pre-processing and formatting messages to be delivered to CI-SOC via MQTT communication protocol. The SecA pre-processed messages can include all the important information for CI-SOC to:

  - verify data integrity;
  - decrypt message;
  - detect potential threats by analysing received values.

- Monitor and analysis: in order to monitor and analyse the pre-processed data at NORM level and as well as to provide threat detection - the CI-SOC creates an enumeration of risks. A threat Modelling and Analysis of new threats is created based on correlation between the risks and the attack trees -coming from the ENISA taxonomy [i.33]. The threat modelling is the principal input required to allow the CI-SOC threat detection and proper match, enabled by the Countermeasure extraction tool.

- Countermeasure application: A match between detected threats and appropriate countermeasure mitigation actions can be achieved using the countermeasure extraction tool. It offers a list of possible countermeasures to be further analysed using the semantically enhanced countermeasures module for the most appropriate countermeasure to apply. A corresponding countermeasure strategy action is assigned to every threat semantically represented.

4.1.2.2 CI-SOC and NORM

In the smart grid scenario, the principal data source for the CI- SOC is the Next-generation Open Real-time smart Meter (NORM) which is a device designed on the concept of the Unbundled Smart Meter (USM). It offers smart meter, low-cost Phasor Measurement Unit (PMU) and cyber-security through an enhanced Smart Metering Gateway (SMG). NORM represents the prosumer's interface to the grid, and assists the distribution security monitoring centres, to face the higher-level cyber-security threats, allowing both secure grid operations and complex market activities. A set of well-established steps that are built upon mainly SUCCESS outcomes, is where the synergic work between NORM and CI-SOC in detection of threats and application of appropriate countermeasure rely on. The data from Security Agent running on NORM are retrieved by the monitoring part of CI-SOC which analyse them in search of suspicious behaviour. NORM security is guarantee with a double layer based on both hardware and software (PUF security and OpenVPN). A probable set of threats is assigned by means of threat categorization model and implemented in CI-SOC, once the identification of a suspicious behaviour is made. CI-SOC sorts the threats from the highest to the lowest risk. By following this type of prioritization, the risk mitigation is done through a list of strategies and countermeasure to be applied both in manual and automatic mode. It involves also a process of evaluation of the impact that they pose in the threat mitigation. Then the identified countermeasure is applied and recorded in the CI-SOC. The application to the detected threats is memorized in a repository that is incrementally populated with the used countermeasures.

4.1.2.3 CI-SOC Modules

The following modules compose the CI-SOC:

- **Key Management module** [i.21] has an enabling role: without incurring in excess of communications overhead implied by common authentication approaches (e.g. OAuth 2.0 [i.28], etc.), it allows the identity management of the NORM devices in an efficient and effective way. The Physical Unclonable Functions (PUF), which is a hardware security function attached to a physical system, is employed at NORM level. The PUF guarantees that a bearer is as unique as the PUF construction characteristics are. Its functionality solely depends on their specific hardware characteristics, which guarantees the uniqueness of the PUFs. In conclusion, given a Challenge string, the PUF generates a unique (supposedly random) Response string. Additionally, the same PUF generates different Response strings to different Challenge strings. Thus, given a large set of previously known triads of type <Bearer, Challenge, Response>, an identity management system can confirm if a Bearer is legitimate. The key management mechanism keeps track of all the active <NORM, Challenge, Response> triads in order to achieve the high-level of control granularity and guarantee effective and secure identity management at all times. By ensuring that only NORMs that succeed in enfolding the correct response for the active challenge are allowed to access SUCCESS APIs, resources and functionality, it acts as a gateway.

Figure 3 represents the high-level architecture of the Key Management module.

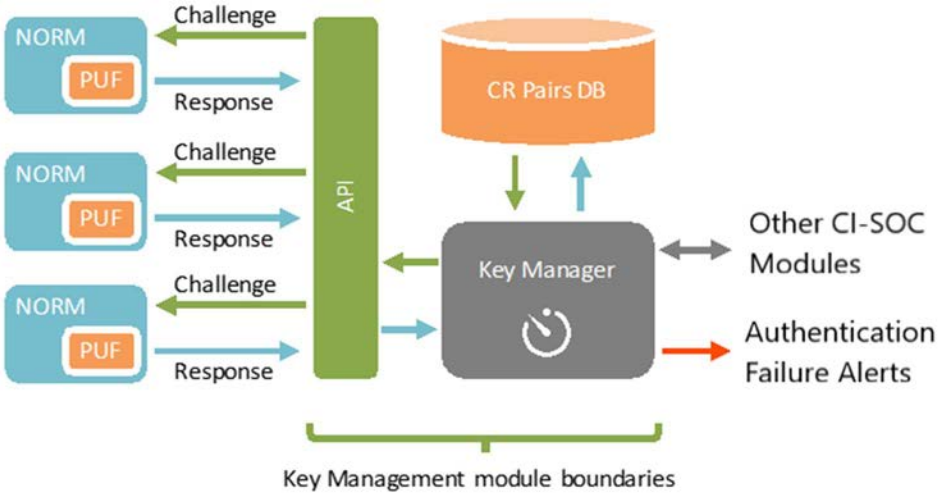

Figure 3: Key Management module high-level architecture [i.21], [i.23]

- The Key Management module is composed of three principal sub-modules, specifically the API, the Key Manager and the Challenge-Response pairs database. Anytime a message to the CI-SOC is sent from a NORM device, it is able also to provide its ID, the active Challenge and the Response string related to that active Challenge, as those are defined by the Key Management module and communicated to the NORM. The Challenge strings are frequently updated by the Key Manager, at all NORM devices (emulating the token refresh functionality used in OAuth 2.0 [i.28]). The updates frequency is parametrized. A new Challenge will be communicated to the NORM, anytime it fails to pass the Key Manager identity validation processes. If the identity validation is not passed also by the new Response, an alarm will be activated to point out that either the specific NORM has been changed, or the communications channel has been breached and the data reported by the NORM have been tampered.

- **Monitor module** deals with the first two points of the flow: *Selection of data* and *Pre-processing of data set.* The data from NORM devices are collected and a pre-processing of data is done considering the threats list. The challenge is represented by finding means of obtaining information from low voltage (LV) networks with available monitoring system data [i.11], given that monitoring all the substations and feeders in the distribution system is hardly feasible. The reliance on low-level measurements represents the innovation introduced by SUCCESS. Where low level measurements are considered data streams coming from smart meters (NORM/SMG) located either at customers' premises or at distribution substation points. Therefore, the smart meters are able to send data to different databases in parallel.

- **Analytics module** is a tool for multi-criteria analysis of data and detection of *spatiotemporal patterns* in order to identify threats and select an appropriate countermeasure optimally. To allow the early threat identification and then select the appropriate countermeasure the Analytics module uses one of some concrete and fully-fledged algorithmic techniques: Anomaly detection/Outlier detection.

- The CI-SOC implements a data [i.21] analytics engine that is able to monitor the incoming data flows from the various edge devices (including and with a focus on NORMs), relying on the threat models generated and the threat classification procedures defined. This allows the detection of behaviour patterns, the attack detection and classification based on the system's expected normality and data handling occur accordingly. A series of chained processing tasks are involved in the data analysis process. These tasks include data clustering and subsequent projection to estimated values as well as event triggering in the case an anomaly, specifically, is detected a significant deviation of the actual data values as compared to the expected ones.

- Anomaly detection referred to as outlier detection, represent the identification of items or events, which substantially differ from an expected pattern. The identified patterns are known as anomalies and often result in critical and actionable information in different application domains. In intrusion detection, anomalous events are not necessarily rare, but unexpected - such as bursts in activity. Many outlier detection methods (unsupervised methods) will fail on such data, as well as this kind of pattern does not comply with the common statistical definition of an outlier as a rare object, unless this data has been aggregated appropriately. The micro clusters formed by these patterns can be detected by a cluster analysis algorithm, instead. Figure 4 presents the outliers extraction from a trend process on a data set. A hybrid approach is considered within SUCCESS, as a way analyse different scenarios. The objective of anomaly detection is to extract the Neighbour Awareness Networking (NAN) operation irregularities.

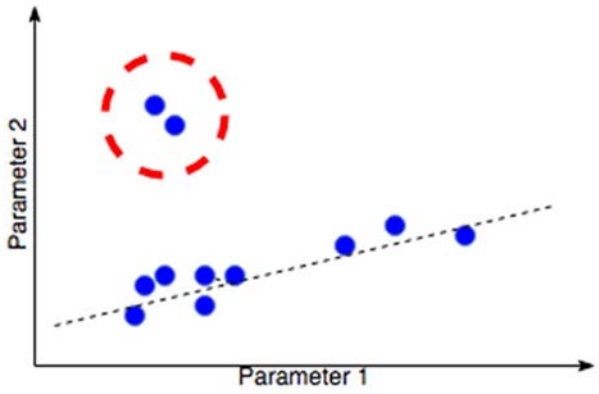

Figure 4: Extraction of Outliers from a Trend Process on a Dataset of Events [i.21]

In order to be able to have data reporting referred to clusters based on their overall behaviour in terms of reporting frequency and values reported, the clustering step is necessary to be undertaken. The clustering enables not only to execute additional clustered analytics procedures on top of similar data but also to identify suspicious behaviours, specifically by reporting that they substantially differ from the expected reporting behaviour.

The employment of attack graphs can be also considered as a supplementary approach for anomaly/intrusion detection, besides the common clustering approach, which considers events rather than reported values. The attack graphs consider sequences of timestamped, recorded events that when detected on pre-defined sequences, allow classifying an attack as active, in contrast to the clustering processes which act upon the collected data and can detect relevant outliers (i.e. suspicious behaviours). The attack graphs-based approach has the advantage that based on the tree/graph unfolding, is able to analyse subtrees of possible attack vectors and identify and treat prior to classifying the attack as active, besides classifying events as active attack-triggering entities.

Figure 5 and Figure 6 illustrate a representative graph-based attack model.

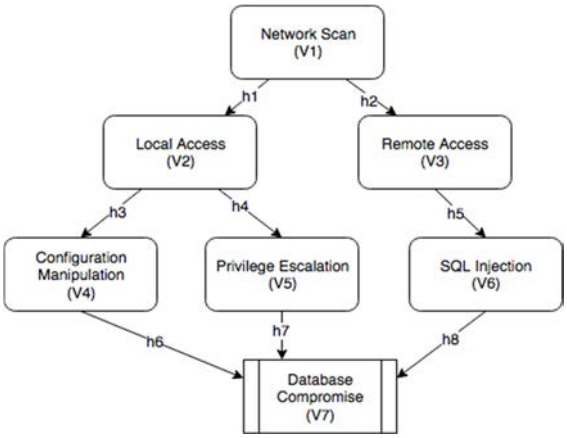

Figure 5: Example graph-based attack model [i.22]

The Analytics module [i.21], in order to assure fast reaction upon anomaly detection, will notify immediately both the Monitor Module (also providing information about the potentially malicious nodes and the data suspected as anomalous) and the CI-SOC Dashboard - to select the proper countermeasures and notify the CI-SOC administrators, respectively. Figure 6 presents the Analytics module architecture high-level overview.

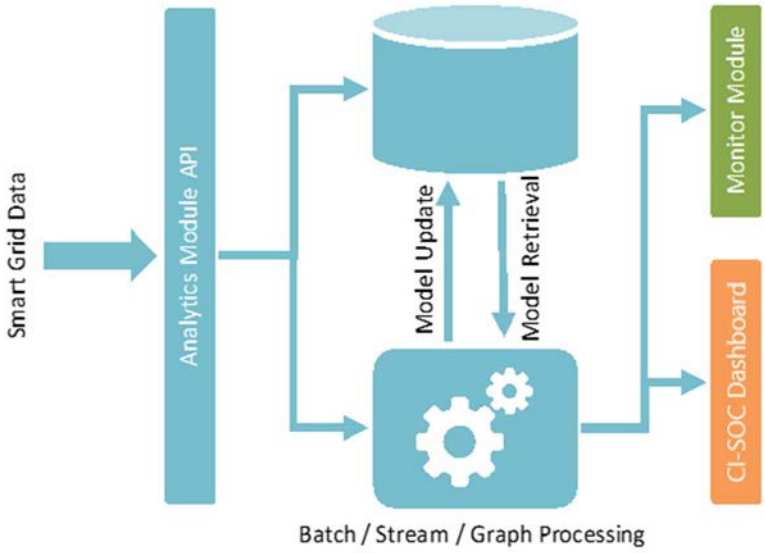

Figure 6: The high-level functional architecture of the Analytics module [i.21]

- **The Countermeasures Extraction Tool** purpose is to evaluate the effect of each of the selected countermeasures against the information security objectives, including availability, integrity, privacy/confidentiality, by selecting a set of the most suitable countermeasures. This tool employs several ad-hoc algorithms as a way to completely cover the whole real-time selection of the most appropriate countermeasures [i.21].

- **Semantically Enhanced Countermeasures** is in charge of providing meta-information in order to enable the definition of the impact of an identified security incident. This will enable the overall business operation of the DSO secured by SUCCESS, to efficiently implement the online threat classification and risk management algorithms [i.21]. This tool is responsible for performing the identification and matching of cutting-edge countermeasures against new and old threats associated to smart meters and electrical devices at NAN (Neighbour Awareness Networking) level.

- **Countermeasure knowledge database** purpose is to make the countermeasures available [i.21] for forthcoming application of the regional tools. This component will be populated in an incremental way and at operation phase, it will be a repository for the suggested and used countermeasures.

- **Dashboard** is a DSS (Decision Support System) for the DSO operators enabling the application of countermeasures concerning the detected threat [i.21]. Its objective is the impact assessment of every chosen countermeasure that permits to identify the most likely type of attack, in real-time. This tool presents an essential role in the identification and selection of the countermeasure to apply. Accordingly, it is important to consider the selection of the best techniques to be used in a given condition or situation. Anyhow, the inefficient usage of visualization techniques can produce inaccurate or even erroneous results, generated by graphic representation mistakes.

4.2 Security Aspects

4.2.1 Introduction

As described in clause 4.1, the SUCCESS' threat detection model is *cooperative*. However, all the *information exchanged* between entities in the smart grid can be considered sensitive. The sensitivity levels can vary from end-user privacy concerns to business and operation critical information. In many architectures the two principal of protection mechanisms considered are integrity and confidentiality protection Similarly to the information sensitivity, also the protection levels provided by integrity and confidentiality protection may vary. Security considered as a disconnected tool/add-on in specific protocols, components, and architecture descriptions does not take into account the consequences of compositions or interactions. Security improvements start with the specific protocol selections, it is embedded in the architecture components, and is implemented in compliance with scrutinized processes and operating procedures.

Security functions necessary to enable secure communication and the physical security measures necessary to secure the network components against physical threats to the equipment are both considered part of the basic network security. Can be classified as physical threats malicious attacks that have as objective to disrupt service by destroying the network components as well as other causes of equipment malfunction such as natural phenomena or component malfunction.

Similarly to many critical systems, also smart grid communication mechanism needs protection against modification. A considerable part of the information flow can be privacy sensitive and usually demands protection to contrast unauthorized access to the exchanged information. The data can reveal either information related to the end-user and his behaviour, directly or based on data analysis. The information also is related to financial transactions, so their modification could result in a financial loss for either party. Furthermore, the security requirements *can expand beyond the communication event*, and in many situations, establish supplementary security requirements for data storage and handling. Besides the information exchanged between the smart meter at the client's premises and the network, also the nodes inside the power infrastructure exchange information with high security requirements. This information consists of management of the nodes within the network, statistics reporting as well as other network state information.

4.2.2 Communications Security

A cooperative networked security system can offer adequate *Identity Management* features. The devices identity represent the basis for communications security, which comprises an identifier and an associated credential [i.2]. A public key certificate as the identifier and the associated private key as the credential can be an example of this. Moreover, symmetric key-based credentials are feasible, where the identifier is a device identity such as the 128 bit Universally Unique Identifier (UUID) and the corresponding credential is a secret key. In this specific situation, it is crucial to have a sufficiently strong key, which means a long enough and random key.

The symmetric approaches have the disadvantage that the same key cannot be reused towards multiple peers/services. This is due to the fact that as the probability of a key being jeopardized increases and at the same time the effect of it is theoretically amplified directly based on the number of entities sharing the same secret key. The SUCCESS approach to the identification and authentication the NORM devices is based on Physically Unclonable Function (PUF) and the uniqueness of the key provided by the CI-SOC component's key management module. The devices need to be aware of the services/peers they need to communicate with as well as their identities, once the identities are in place. Sometimes, it may be sufficient to recognize as a trusted peer any peer with a certificate from a trusted Certificate Authority (CA), while in other cases can be trusted only specific identifiers. Moreover, distinct peers/services may have various levels of trust, or certain types of information with certain identified peers/services can be shared by the device.

This is established through authorization policies and access control. The configuration of this information can be done directly to the devices or securely over the network by using some device management protocol such as LwM2M [i.34]. It is necessary that during the connection between peers, the device can authenticate the peer before interacting with it [i.3]. During this process, the device has the confirmation that the identity of the peer is trusted and it can interact with it. Normally, likewise, the peer needs to authenticate the device, resulting in mutual authentication, which is based on the strong identities used by the devices.

A typical authentication protocol is the Extensible Authentication Protocol (EAP) [i.26]. It is principally used for access authentication, such as a device demanding access from an access point or gateway but it can be also used for other types of authentication. Multiple different authentication methods and credential types are supported by EAP. The setup of Transport Layer Security (TLS) [i.27] with both client side and server-side certificates represent another common example of mutual authentication. If the device has 3GPP credentials, by leveraging the Generic Bootstrapping Architecture (GBA), it is also possible to use the credentials for authentication and key-agreement with the service.

Eventually, the device can initiate interacting with the peer/server, after successful authentication. At this point, the level of security required by the communication is defined by the security policy. The access network might itself offer secured access, can be one methodology. In another methodology, the communication protection can be done end-to-end instead of hop-by-hop. A default choice in many cases is the confidentiality protection, i.e. encryption, especially in the smart grid scenarios. In many cases, nonetheless, encrypted data without integrity protection can be modified on the path by an attacker without being detected by the receiver [i.29], where usually, the attacker can only make some random alterations of the plaintext, but the exact change is not chosen. The more plaintext the attacker knows the more he can target the change to a particular part of it. However, the receiver can occasionally notice these types of attacks, if the plaintext has a well-defined format and expected value ranges (e.g. reported temperature or power consumption), as well as the random alterations, may result in unrealistic values or corrupted message formats. Explicit integrity protection can be used, e.g. by applying keyed hashes, MACs or digital signatures. Replay protection is another characteristic that the protocols themselves provide in many cases. If protocols are not offering this feature explicitly, one can consider adding it. Communication security protocols include (D)TLS, object security and IPsec [i.30]. Depending on requirements different algorithms and cypher suites can be selected for all of them. Usually, the key material used to secure communication is either based on the authentication keys or negotiated as part of the authentication process.

Through the application of these concepts of having a strong identity, appropriate access control and end-to-end authentication and encryption requirements, it is possible to achieve a good base level of security and many threats (e.g. man-in-the-middle, eavesdropping and data injection attacks) can be effectively prevented.

4.2.3 Physical Security

Smart Grid is a nation-wide cyber-physical system originated by Legacy distribution networks being gradually updated. As such, it was subject of long evolutionary developments operated by many business actors. Nowadays, it is a big, complex, and interconnected heterogeneous system that utilizes different generations/versions of equipment. The co-presence of different versions of software and the utilization of differently aged hardware poses several interoperability, general security, safety, and data privacy issues.

The physical security of the smart grid nodes is another major part of the smart grid security. Some nodes are placed at customer premises to which the customer might have direct access, and some of the infrastructure nodes are placed in remote unmanned locations. In fact, the protection is needed not only by the node itself but also by its power supply and communication capabilities, because disabling any of them would make the node inaccessible as well.

The node physical protection can include blocking unauthorized access to them as well as sensors for perimeter breaches detection. The sensors can be used for the site as well as for the node itself, e.g. with sensors detecting the device's enclosure opening.

Besides signalling device enclosure breaches, the device could store a state associated to this. This state could be stored in hardware secured memory, e.g.in a Trusted Platform Module (TPM), in order to protect it against tampering. Using a remote attestation service, the state of the node can then be queried remotely, and the state stored in the TPM would be part of the node's state. The TPM could also be used to store the node's credentials and other critical security parameters to prevent an attacker from copying/cloning them. Furthermore, other hardware-secured modules can be used to store credentials (e.g. Universal Integrated Circuit Card (UICC)).

4.2.4 Double Virtualization

In order to secure the Smart Grid, in conjunction with well-known security mechanisms, such as strong authentication and communications security, in SUCCESS, have also been defined and used some more recent and even new security concepts. For the purpose of separating data from functionality Double Virtualization (DV) is used, and enables moving data between different physical devices independently from each other. This can be particularly useful a device is under cyber-attack as the functionality can be transferred to another physical host, helping to keep the system up and running.

Double virtualization has been implemented in SUCCESS, as a flexible solution dedicated to power and communication grids, based on separating of applications from their data and implementing the functionality related to the application and data parts in the edge cloud on different Virtual Machines.

4.2.5 Other Security Measures

The human factor plays an important role in shaping the security panorama of cyber-physical systems. There have to be taken into account two important aspects, firstly having well-educated personnel acquainted with the underlying systems and secondly having adequate security policies for how they can behave and access data and nodes in the network [i.31]. This can be associated with non-repudiation logs providing as well.

It is also important to establish countermeasures in advance to address potential security threats and accidents that can be detected. This also requires the ability to detect such accidents, which implies the monitoring of the network and its nodes. The network-monitoring centre gathers node and network state information and actions and reports any abnormal behaviour to the administrator. This could be for instance an update of a node firmware without being scheduled in the system, which could indicate a node attack. The administrator investigates the cause on the bases of these alerts and potentially performs countermeasures to fix the problems and mitigate their impact on the network.

In fact, it is possible to maintain in all nodes up-to-date software, such as OS, firmware and applications. Hardening of the software might also be a good preventive measure for the most critical nodes. However, in order to defend against network and malware types of attacks, in the nodes and network can be installed anti-virus programs, firewalls and likely Deep Packet Inspection (DPI), if plain text messages are available (which might be the case in the breakout gateway).

In order to isolate the nodes and the smart grid network from the public networks, as well as node internal functions from each other, can also be used other isolation methods, such as virtualization and SDN. Probable software bugs can be removed, by promptly applying updates, eliminating known vulnerabilities. Alternatively, it is possible to upgrade the cypher suites and security algorithms in use at a given time if it is discovered that they have some weaknesses or have been breached.

It is possible to duplicate the most critical nodes in the network for resilience. So, the network can be able to continue functioning even when a node is not available even in case of malfunction, attacks or accidents. This can be done by using the backup node that can manage the critical functions of the disabled node.

4.3 Threat Detection and Countermeasures

4.3.1 Introduction

In general, all Security Frameworks include intrusion/threat detection functions. In SUCCESS, the threat detection model is cooperative. The overall approach to security in SUCCESS is trust-but-verify. There are several networked agents contributing to measure and to classify (1) a threat by using the context information (2) and the computations of metrics performed by SecAs.

The CI-SOC, and in some cases the BR-GW, can activate pre-defined countermeasures to the identified incidents when threats are recognized and a security incident occurs. The response needs to be immediate, in some situations, i.e. autonomous reaction by the system, while other countermeasures might need a human operator or administrator to authorize the countermeasure action. Cyber-security related incidents but also some physical security related incidents, and identification of the associated countermeasures, are the main focus in SUCCESS. An exhaustive approach to threat detection is carried out on three levels: BR-GW conduct controls on data communications integrity, CI-SOC controls only the grid data while CI-SAN controls both at other locally available data (e.g. computer logs) and analyses over a wide area making it possible to elaborate information correlation in order to gain further insight. The way countermeasures are applied, reflect the three-level approach implementing countermeasures across a wide area is something that needs manual control by a grid operator. Therefore, while CI-SAN alerts the grid operator of incidents and the operator is responsible for implementing the countermeasures, CI-SOC can implement countermeasures autonomously in its local area and BR-GW can implement countermeasures for the data communications which are handled by the given virtual BR-GW instance. BR-GW, CI-SOC and CI-SAN share and co-ordinated information regarding detected incidents and implemented countermeasures.

4.3.2 List of security incidents and outline of countermeasures

4.3.2.1 Purdue Model and Cyber Kill Chain

In a Smart Grid scenario, Smart Meters can also be used for flow control purposes in real time. It represents a new threat formerly known as Cyber Kill Chain (CKC) in other classes of Industrial Control Systems. CKC [i.7] is a way to understand the sequence of events involved in an external attack on an organization's IT environment. Conversely, to those well-protected systems, Smart Meters are low-cost IoT devices ubiquitously distributed over large geographical areas with limited protection. One of the deficiencies in the above-mentioned context is the incapacity to analyze the communication patterns between networked energy flow control agents.

The Purdue Model [i.5] identifies five zones and six levels of operations as shown in Figure 7.

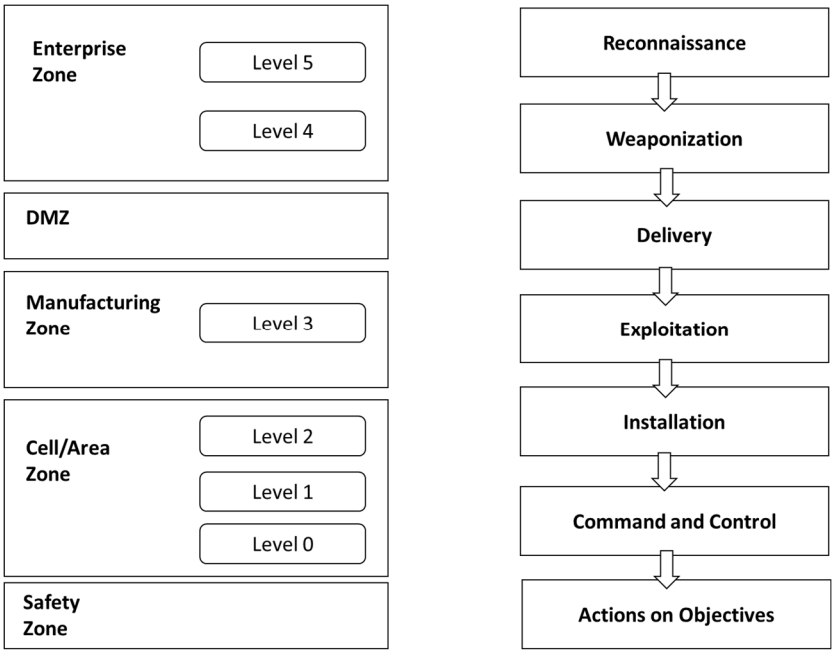

Figure 7: Purdue Model and Cyber Kill Chain [i.5]

- Enterprise Zone - This zone includes the services, systems and applications in Levels 4 and 5 that are normally managed and operated by the IT organization. In Level 5 (Enterprise) resides the IT infrastructure and enterprise applications (e.g. VPN remote access, Internet access services). Due to the high risks, that it would bring, systems in the Enterprise zone and the ICS environment do not communicate directly; instead, that is the Demilitarized Zone is used to communicate with the ICS environment. Level 4 (Site Business Planning and Logistics) includes the principal enterprise IT systems that include operational and maintenance management, e-mail, phone and printing services and inventory management.

- Manufacturing Zone - Level 3 (Site Manufacturing Operations and Control) includes systems in charge of managing the control plant operations to produce the desired product. Systems in Level 3 communicate with the systems in Enterprise Zone through a Demilitarized Zone and can communicate with systems in Levels 1 and 0.

- Cell/Area Zone - Level 2 (Manufacturing Operations) are included in this level the manufacturing operations equipment for a production area (e.g. Human Machine Interfaces (HMI), Alarms/Alert systems, Control room workstations). The systems from this Level can communicate directly to the Level 1 systems and through the a Demilitarized Zone with the systems of Enterprise and Manufacturing zones. Level 1 (Basic Control) in this level are comprised all the process control equipment (e.g. Distributed Control Systems, Programmable Logic Controllers, and Remote Terminal Units) that receive input from Level 0 devices, that are responsible for continuous, sequence, batch and discrete control. Level 0 (hardware devices) in this level are includes all the hardware equipment that control the manufacturing process and are controlled by the Level 1 devices.

- Safety Zone - in this zone reside all the monitoring systems that process information, bring the systems into established security levels and alert the operators about the risk condition.

Currently Smart Meters are not offering any data traffic analysis tools to detect anomalous communication patterns compatible with the Cyber Kill Chain (CKC) attack. Smart meters with the (remote) load flow control functionality fall into the wider category of ICS.

The ICS, like the ones used in energy distribution, have very specific cyber-security challenges due to the physical nature of the systems, their real-time requirements and the specific protocols in use, often derived by legacy applications that were designed before the introduction of networks -not taking in consideration the problem involved by the interconnection of systems. Those ICS are vulnerable to the CKC. CKC is a well-known model for mapping unauthorized introductions in computer networks by external malicious actors. The original model is divided in 7 sequential phases that range from the initial reconnaissance of the attack surface up to the final accomplishment of the intended goals. Each step in the CKC can be targeted with specific defence mechanisms to reduce the probability of successful intrusion and impact of damages carried out by intruders.

The first step in the CKC is called Reconnaissance. In this phase, the attackers try to collect as much information as possible of the attack targets in order to identify the attack surface and the possible breach points. The next steps are already involving the active exploitation of the vulnerabilities identified and selected in the first step. It is therefore very important to identify a potential threat as soon as possible in order to react as quickly as possible by applying mitigation procedures. In general, reconnaissance includes the collection of any piece of intelligence that can help attackers to gain unauthorized access to the systems. This includes information such as operator's identities, mail addresses, customer's and supplier's names and so on. This allows for example sophisticated targeted attacks of social engineering against human operators.

4.3.2.2 Cyber-security related incidents

By combining the basic security configuration and measures with active attack detection and mitigation, which complement each other, is possible to achieve defence in depth, and make it more difficult for the attacker to succeed. Network and nodes monitoring is the basic requirement to identify security incidents.

The effective monitoring of the power grid can only be done through the communications network monitoring, in order that the monitored network is a hybrid comprising both the power grid and the communication network. The given network thus contains both the power grid and the communication network and the nodes contains the power grid equipment and communication network equipment.

The ideal case is that attack attempts are identified, and blocked, as they happen, e.g. when an attacker tries to gain access to a node in the system. This means that the node itself has to raise an alarm when it notices things such as an intrusion attempt, multiple failed login attempts, port scans, etc., which gets the attention of security personnel that, can monitor the situation and take actions if needed. Ways to minimize the attack surface include hardening the nodes, requiring all software being installed be signed, and using a hardware root of trust, which can verify signed software, detect modifications to the system, etc. Periodic remote attestation could also be performed to verify the state of the nodes. These precautions are good (but not guaranteed) ways of tackling hackers, while they are less efficient against insider attacks by attackers who have some level of authorized access to the nodes/system.

If an attacker gains *undetected access* to a node, indications of their presence can include devices that do not react or not perform as expected, e.g. exceptions to regular communication patterns or message type and content. Nonetheless, the root cause incident detection might not be straightforward as well as multiple threats could result in similar type of outcomes, such as a node not answering due to a physical attack, a network-based attack/hack on the node (e.g. Denial of Service (DoS) attack) or on the network itself, or a natural disaster or accident that has damaged the node or made it useless. Of course, sometimes what is identified as an incident turns out to be a regular operation, i.e. a false positive. Some incidents might require immediate action while full analysis might not be feasible in that timescale. Defensive strategy can be prepared but not disclosed at the same time in order to preserve its efficiency (the effect of surprise). Hence, it makes sense to perform analysis and verification of an incident before reacting to it in order to materialize a readiness to defend.

Once a security accident has been identified and confirmed, it can be mitigated by adopting a pre-defined protocol, comprising a number of steps or parts. This is referred to as a countermeasure, which is used to react to the accident and minimize the impact of the incident. The present document details the multiple incidents and the countermeasures that can be used to resolve the situation.

The selection of the countermeasures is done based on the exact nature of the security incident and is organized as an aggregation of atomic actions. Typically, countermeasures are carried out sequentially, depending on the particular nature of the incident.

Normally, the set of security incidents is more generically specified and is not expected to be modified so often, while the related countermeasures might be revised over time. The cyber-attacks are constantly evolving, thus potentially requiring evolved countermeasures as well, but their effect on ICT systems, such as converged IT/OT systems, (as defined by the security incident) remains unchanged, e.g. loss of service. Hence, the present document addresses the incidents instead of the use of particular countermeasures. The specified countermeasures can be considered as a model and might, in many situations, need to be modified for the specific incident at hand. This implies that the countermeasure inventory will increase over time as new changes of the incidents occur and appropriate countermeasures are identified.

How fast an attack is detected depends a lot on how the attacker behaves. An attacker that gains credentials to a system but just monitors it is less likely to be detected promptly compared to an attacker that just modifies messages on the path without proper credentials. The latter can be detected immediately as the modified messages will not pass integrity checks.

Assuming a system, which is applying proper security protocols and configurations, an attacker, could still potentially gain access to the system through hacking, social engineering, or through a disgruntled employee. The attacker could then use the gained access for performing malicious activities, e.g. a Man-in-the-Middle (MitM) attack in order to disrupt the system, monitor traffic, or even modify it. Detecting a security incident can optimally happen before the actual attack (MitM attack in our example) is launched, i.e. when the attacker tries to gain access to the system. However, this might not always be possible; if the attacker is good enough, he might find a vulnerability in the system that lets him gain access without the system/detection system noticing it. The next phase where the attack could be detected is when the attacker uses the system, e.g. by acting as a Man-in-the-Middle (MitM). However, detection of this activity is not trivial, and it might go on undetected for a very long time. A Man-in-the-Middle (MitM) attack is not an example of a security incident for which a countermeasure is defined, rather it is defined for the sub attacks needed for applying a MitM attack, e.g. physically breaching the casing of a device, which could be part of the setup phase of the attack where the attacker gains access to the system or noticing strange type of data being communicated in the system, which might be due to an attacker modifying the traffic as a MitM.

The term "device" is intended to be interpreted as any physical device in the system, such as NORM, running a (potentially virtualized) function, or as any part of a larger system that either sends, receives or manages communication.

Table 1 and Table 2 both include countermeasures for cyber security and physical security incidents, and give a high-level overview of the countermeasures to be applied when the corresponding incident is detected.

Table 1: Cyber-security related incidents and countermeasures [i.24]

Incident Label	Incident Description	Countermeasure
CS-1	Device behaving suspiciously	1. Move the data or applications to another physical/logical zone 2. Perform remote attestation to verify device state 3. If state is OK, red-flag the device: a. Temporarily disconnect device from the grid b. Investigate
CS-2	Remote attestation fails (after step 2 of CS-1 above)	1. Disconnect device from the grid. 2. Send maintenance unit to location 3. Reset/Reinstall device & re-bootstrap (new credentials & revoke old ones)
CS-3	Unauthorized messages	1. Identify device or network segment where data is originating from 2. If device, perform CS-1 3. If network segment, it means there is an unauthorized node in the network segment 4. Isolate network segment 5. Investigate
CS-4	Virus detected in device	1. Re-deploy VMs running on device 2. Isolate device/functions from network 3. Enable backup device if available 4. Reinstall device to remove malware 5. Verify peers not infected 6. Update malware definitions in all nodes as soon as possible
CS-5	DoS suspicions	1. Block DoS traffic at edge of network by updating firewall rules and using SDN for re-routing DoS traffic 2. Move VMs running on targeted node to other location 3. Enable backup node if available 4. Do load-balancing if possible 5. Analyse suspected DoS traffic, verify attack
CS-6	Security algorithm deemed insecure	1. Remotely configure affected nodes to deprecate insecure algorithm and enable alternative algorithm 2. Optionally select and review proper alternative algorithm

Table 2: Physical security related incidents and countermeasures [i.24]

Incident Label	Incident Description	Countermeasure
PS-1	Perimeter breached	1. Send security personnel to the location to investigate and repair breach (infrastructure device)
PS-2	Device casing breached	1. Send security personnel to the location to investigate and repair breach (infrastructure device) 2. Perform remote attestation of device state 3. Send maintenance unit to location: a. Reset device & re-bootstrap (new credentials & revoke old ones) b. Repair device or c. Replace device
PS-3	Communication link unavailable	1. Re-configure network to route device via secondary access (if available) 2. If secondary access not available: Move data and/or applications to another physical/logical zone 3. Send maintenance unit to location to: a. Reset network connection & unit b. Repair network connection & unit or c. Replace network connection unit

Incident Label	Incident Description	Countermeasure
PS-4	Device power unavailable	1. Enable backup power 2. At least if 1) not possible: Move data and/or applications to another physical/logical zone 3. Send maintenance unit to location to: a. Reset power supply unit b. Repair power supply unit or c. Replace power-supply unit
PS-5	Device Unavailable	1. Enable backup node if available 2. Move data and/or applications to another physical/logical zone (to backup node if available) 3. Send maintenance unit to location to: a. Reset device b. Repair device or c. Replace device

The countermeasures provided are generic countermeasures for a particular incident type. These countermeasures, however, act as a model and can be customized to the real use-cases and particular incidents.

In order to have a better understanding of security incidents on a regional level, they all can also be propagated upwards to CI-SOC. This implies sending any pertinent information related to the incident to the CI-SOC so that the SecA Node can correlate potential distributed attacks in a wide area, as well as providing information to DSOs regarding individual current or recent incidents. The DSOs can thus be prepared and learn about probably future incident types and patterns.

5 Cyber Security for Smart Meters

5.1 Introduction to the smart meter security

Several classes of smart meters exist: interval- energy meters, pulse-based meters, event-driven meters, meters with flow control capacity, demand-oriented meters, meters with different sub-metering options, hybrid meters embedding relays for control purposes, hybrid meters with real time PMUs, and more.

An energy distribution business is enabled by the Advanced Metering Infrastructure (AMI) and the telecommunication that links smart meters, metering concentrators, and other components of the Metering Data Management System (MDMS). The data formats, security measures, and protocols related to the smart meter security in initial AMI deployments were proprietary. It means that the former security principle was "security protected by obscurity".

Due to the difficulties in obtaining secure communication introduced by the adoption of proprietary methods and because of interoperability constraints, the industry moved towards common standards (e.g. for smart meters ETSI TS 104 001 [i.2], IEC 62056 (DLMS/COSEM IEC 62056-1-0:2014 [i.39], IEC 62056-1-1:2016 [i.40] and for the interoperability of smart grids IEC 61850 [i.35]). Considering the architecture of NORM (see Figure 9) which comprises the Smart Metrology Meter (SMM, which is a market existing meter compliant to DLMS/COSEM IEC 62056-1-0:2014 [i.39]), the Low Cost PMU (the compliance of NORM to the IEC 61850 [i.35] standard is considered, particularly to the IEC 61850-90-5 [i.43] related to the PMU, the IEC 61850-9-3 [i.44] related to the PTP profile for power utility automation), and the Smart Meter Gateway (SMG, which coordinates simultaneously the local measurement equipment and the communication with all external actors which implies its compliance to the aforementioned standards).

Standard smart meters are demanded to store a key used that is used to encrypt and generate Message Authentication Codes (MAC), and the passwords that are used in the smart meter to provide different access privileges in specific tables. A secure mechanism is necessary to protect these keys and passwords. Applying such a methodology in the AMI needs a (better) scalable, efficient, and robust key management scheme capable of supporting a very large number of smart meters and supporting smart meter authentication as well. Smart meters are susceptible to man-in-the-middle attacks if a strong authentication mechanism is not implemented. The utility server can be convinced by an attacker, to communicate with a legitimate smart meter and can cause damages.

The secure end-to-end communication between utility servers and smart meters is a necessary prerequisite for the AMI's overall security. Before reaching the destination, the messages exchanged between the utility servers and smart meters travel through multiple hops. The routing nodes role can be played by the collector nodes and, sometimes smart meters.

Therefore, a message between the utility server and a smart meter can pass across one or more collector nodes and other smart meters. Different communication protocols can be used by different hops.

EXAMPLE: The utility servers and collector nodes hop can use a 3G network while the collector nodes and smart meters hop can use a radio link. As compromised/malicious intermediate nodes cannot be trusted for the confidentiality and integrity of the messages, though most of these communication protocols foresee link level security, this is not strong enough to protect messages exchanged between the utility servers and smart meters.

End-to-end message level security is important to protect messages from against attacks through the communication channels and intermediate nodes.

In AMI, the data in uplink transmission from smart meters to the MDMS includes **secret information**, for example, the power usage of a household, a data that represents a flow of monetary units. Those data will be collected by the MDMS and be further applied to determine the power generation commitment and the contractual usage of renewable energy. The control data in downlink transmission involves the price and tariff information, yet another monetary flow, which affects the demand side response and finally lead to a more efficient power grid. In AMI, each smart meter needs to be available and be treated equally in the network since fairness needs to be applied to each of the customers. Traditional communication networks do not emphasize availability for each node let alone fairness. The deployment of smart meters to households is deterministic and well ordered since the buildings are in fixed positions. The wireless nodes in traditional networks are usually deployed randomly and redundantly. The uplink transmission and downlink transmission in AMI are asymmetric where the uplink transmission consists of different data from each smart meter to the MDMS and the most of the downlink transmissions are in broadcast mode. In traditional communication networks, the uplink or downlink can even barely be distinguished.

Several smart meters come with the real time energy **flow control** features. NORM aggregates through its Smart Meter Gateway (SMG) the data from two different local measuring equipment: the Smart Metrology Meter and the Low Cost Phase Measurement Unit (PMU). This data integration allows NORM to enable both smart metering and hard real-time smart grid functionalities. In several communication protocols used to support this kind of business operations, and the IEC 61850 [i.35] in the smart grid gives an example, the messages need to be transmitted within 4 milliseconds and so that encryption or other security measures which affect transmission rates are not acceptable. Consequently, the only security measure included is authentication. In the IEC 62351-6 [i.36] example, the protocol provides a mechanism for digitally signing the messages that need minimal compute requirements for these profiles. The Virtual LAN (VLAN) high-speed profiles used for GOOSE, GSE, and IEC 61850-9-2 [i.37], they have performance requirements (e.g. 4 milliseconds or less) that prohibit the use of full encryption. As an effect, a big number of smart meters that use a CRC based Message Authentication Code/Seal to provide integrity, operate in insufficiently secured environment, a factor suggesting an increased vulnerability. Many smart meters are installed and left unattended for very long periods of time and are operated from remote locations over public communication channels. In near future, smart meters will enable Transactive Energy Control (TEC) operations on behalf of the actual energy users. Therefore, given the practical impossibility to completely secure smart meters, the changing energy business scenario suggests rethinking a way of using the protocols to fit the uniqueness of AMI.

In general, Wide-Area Monitoring Systems (WAMS) employ PMUs to collect measurements and estimates about the **system states**. Newer smart meters - and the SUCCESS NORM gives an example - include the **metering & PMU** mix of functionalities. It opens to the time-specific "undetectable" attacks. SUCCESS has provided a methodology for mitigating undetectable attacks through providing algorithms for optimal security investments in secure time synchronization and for optimal deployment of additional PMUs.

The nation-wide ubiquitous deployment of smart meters - being delivered to the end users and left **unattended** for extremely long periods of time - has an important security implication. The SMM is vulnerable because the firmware can be replaced by unknown actors. For this reason, has been implemented a hardware-based security feature, Physical Unclonable Functions (PUFs) implemented on a Field-Programmable Gate Array (FPGA) board. Hardware-based security is used for purposes of authentication and encryption at data messages level.

The utilization of **fleets of smart meters** in WAMS context requires GPS-precise time synchronization or its equivalents, for example the use of the Network Time Protocol (NTP) or the Prevision Time Protocol (PTP) [i.15]. In heterogeneous use scenario, co-existence of multiple clock synchronization sources, e.g. GPS and network-based ones, it exposes to clock synchronization attacks. However, the knowledge about system configuration, it makes also possible implementing a detection logic against clock synchronization attacks. The PTP module can synchronize the CPU time base with a much higher accuracy than the NTP can. PTP is defined in the IEEE 1588-2008 [i.41] and on local area networks or on low latency mobile networks (e.g. 5G), it achieves clock accuracy in the microsecond range or better, making it suitable for high precision measurements such as PMU requires. PTP's core principles are analogous to that of the NTP protocol, where computers and other devices that have a clock are connected in a network and create a hierarchy of time sources where time is distributed from top to bottom. Typically, the devices at the top are synchronized to a specific common time source (e.g. a GPS receiver timing signal, or an atomic clock). For the purpose to measure the offset of their clocks, periodically, the devices "below" exchange timestamps with their time sources. The clocks are constantly calibrated to adjust random variations in their rate (because of effects such as thermal changes) and to lessen the detected offset.

It is worth noting that to take full advantage of PTP the hardware timestamping capability is strongly recommended, although even in absence of that resource it is possible to mitigate the jitter of resulting instantaneous offset from the master clock by adopting "robust" digital filter (higher time constants and order filter), in the controller that mediates the tick rate adjustment. This increased stability will be obtained at the cost of a slower convergence, but in the context of Phasor Measurement Unit (PMU) application it is acceptable. Under those conditions, the final target is to keep the overall uncertainty below 1 μs.

After a **composition** of different system components in a complex system, e.g. Smart Grid, smart meters do interact network-wide with each other and with their respective peers. The intended topology and the intended **logic of interaction** are not sharp because they **evolve over time** due to the evolution of business specifications. Like any ICS, different Legacy versions of software agent **co-exist, interact, and interoperate** in a complex system for a long while. The wired topology of a physical system could be invariant or *slowly changing* over time, but the updates of interaction's logics occurs *more frequently*. It forms a system of systems **running at different velocities**. As an effect, the bifurcations (in system states) are possible. As such, the probability of so-called blue-sky catastrophe cannot be excluded. To mitigate, SUCCESS adds ad-hoc observer deputed to care about the effects of interactions that includes Security Agents (SecA) tracing patterns of communication between actors and verifying their identities. The SMG includes new functionalities of the Security Agent potentially useful to perform intelligence-based analysis of the data communication patterns.

The interoperability definition according IEEE is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged". This definition originates several implications for the interoperability requirements of the smart grid. First, the infrastructure has to **allow information exchanging** from senders to receivers (the capacity to exchange bits and bytes). Second, the participating solutions' implementations need to be able to **make sense of the information** provided. Therefore, it assesses the usage of common symbols, protocols, and implementation specific interpretations. A frequently neglected or underrated aspect is the theoretical consistency of solutions to make sure that the implementation of specific interpretations in each system is theoretically consistent within the context of the common operation. **The information** can **always (at any time) be used** by the receiving system the way it was meant by the sending system.

The integrability, interoperability, and composability challenges are discussed above. Integrability deals with the physical/technical connection domains between systems, which comprise hardware and firmware, protocols, networks, etc. Interoperability deals with the interoperations software and implementation details of; it involves data elements exchange via interfaces, the middleware usage, mapping to common information exchange models, etc. Composability deals with the modelling level issues. The underlying models represent determined abstractions of reality used for the conceptualization being implemented by the resulting systems. Altogether, do challenge the adoption of Security by Design.

5.2 Design Principles

Security by Design (SbD) is a well-known methodology - and design principle - to software and hardware development that needs to make systems as vulnerability free and resistant to attack as possible. This can be done through the application of measures like continuous testing, authentication safeguards and adherence to best programming practices. The SbD considers security performance as a horizontal component in product design for networking appliances and not generally networked objects. Less rigid models including security through obscurity, security through minority and security through obsolescence contrast with the SbD model. In critical metering infrastructure, the SbD concept exhibits three different aspects to focus on.

Let us assume that smart meters are used for real time flow control in a WAMS/SCADA/ICS context. The main aspect concerns the security of the Phasor Measurement Unit (PMU) time synchronization component because the importance of time synchronization security is two-fold:

1) the time synchronization security issue is particularly difficult, and in the context of PMUs has not been fully understood;

2) it is foreseen to use PMU data for different applications in future power systems, hence, its security, including that of time synchronization, is essential.

Traditionally the security of PMU time synchronization is ensured using **technical solutions** and the **detection of anomalies** is based on detection algorithms that consider technical information only. At the same time, data validity in power systems is usually verified using state estimation based on a physical model of the system. By combining the two, a powerful solution was developed for time synchronization anomaly detection.

The second aspect on Securing Smart Meters is their metrology part affected by the vulnerability of **uncontrolled firmware updates**, which has been mitigated by introducing PUF.

The third aspect regards the **interoperability** interfaces between meters and the infrastructure. It includes the analysis of the data traffic between the controllers and the actuators.

The aforementioned principles can be used in two extremely different contexts, specifically development - and reuse - ones. During development, in order to ensure that the resulting system will be interoperable, **prescriptive norms** are required. During reuse, in order to allow evaluating whether a legacy system can be used in a new operational context or not **descriptive metrics** are required When legacy systems have to be modified to migrate towards new (improved security) solutions, both contexts are connected.

5.3 Separation of Functionalities

Deployed Smart Meters (SM) deliver a set of functionalities required by a domain-specific business scenario. Traditional SMs are high-precision measurement devices calibrated in accredited centres in order to support financial transactions, e.g. billing operations [i.1]. SM includes an embedded architecture for *calibrated metrology* and some other (additional) functionalities. Flexibility in terms of local functionalities of the meter, is difficult and sometimes impossible to achieve, as any new function needs a recompiled firmware version inside the meter. New metrology approval from accredited calibration authority would then be automatically necessary for each new version or for each minor update.

In the new smart grid paradigm, the needed business functions can evolve quicker compared with the conventional time assigned for new generations of Smart Meters being planned to be replaced. A complete cycle for the replacement of calibrated/certified Smart Meters is currently estimated at approximately 10 years. In other words, only minimal functionality - if any - it can be added to the existing Smart Meters during those 10 years because of the need to re-certify any addition.

The unbundling of meter functionalities in two different parts is a systematic process, which has been first presented in the conference IEEE ISGT 2011 [i.12] in Manchester and then developed in the H2020 project NOBEL GRID [i.14] is presented in Figure 8. To overcome these limitations, the Unbundled Smart Meter (USM) architecture was designed in order to maintain a clear separation between:

a) The business logic and multi-actor communication part, named Smart Meter eXtension (SMX), which can act also as a Smart Meter Gateway.

b) The metrology part, named Smart Metrology Meter (SMM, being legally enforced by metrology approval and its related billing data security aspects (which include physical seals).

Figure 8 shows main features of the SMM and SMX. As the SMM part can remain unchanged for the whole life of the SM, the initial investment in this legally binding part is protected from being obsolete. However, the SMX is a powerful machine to cover all flexibility needed for communication with various actors and for implementing flexible functionalities. This part is not rigid and is expected to support many upgrades and new functionalities and services, thus being exposed to cyber-attacks. In this respect, data security is an essential feature that needs to be managed in a multi-actor environment and able to communicate on public IP networks.

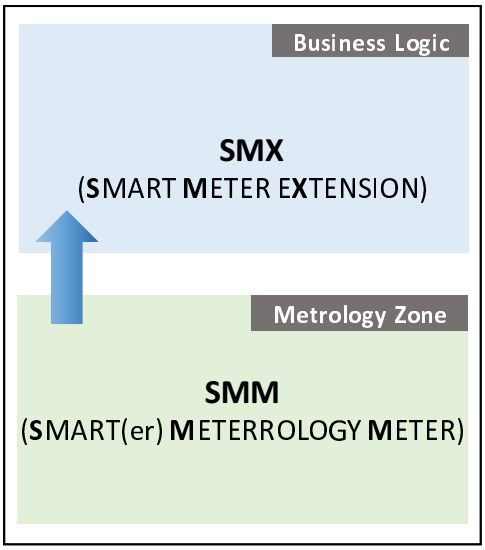

Figure 8: Unbundled Smart Meter (USM) [i.18]

Based on the Unbundled Smart Meter (USM) architecture, Next Generation Open Real Time Smart Meter (NORM) [i.18] goes further and adds a supplementary module, a low-cost Phasor Measurement Unit (PMU), which represents the data second source for the SMX, besides the existing Smart Metrology Meter data. Being the extension (SMX) more complex and asking for additional functions, it becomes a "Smart Meter Gateway" (SMG). The NORM parts are presented in Figure 9.

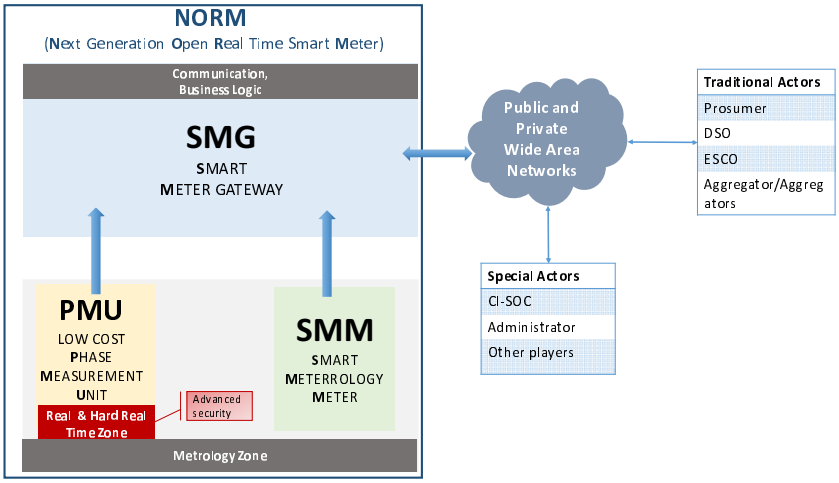

Figure 9: NORM unbundled concept [i.18]

In Figure 9 it can be seen that NORM is made up of three components, and that the smart metrology meter part is now enriched by the low cost PMU (LCPMU). The vulnerable parts are the metrology component SMM, the PMU component and the algorithms running on the SMG.

5.4 Smart Meter Gateway

5.4.1 Main functionalities

The most important subsystem of NORM is represented by Smart Meter Gateway (SMG) as it coordinates simultaneously the local measurement equipment and the communication with all external actors. The SMG's most important aspects are:

- it is the device concentrating the data coming from the metrology meter and the low cost PMU (LCPMU);

- it uses meter and PMU particular protocols for data access and storage in a real-time database followed by a persistent storage of values based on daily logs of profiles;
- a database-centric architecture permits the interaction between data and all external actors only through a Role Based Access Control (RBAC) mechanism, which allows that only data specific to each actor is provided with that actor;
- based on a high cyber-security model leveraging PUF technology, it implements the multi-user/multi-protocol simultaneous communication with all external actors; and
- it implements a local security agent, capable of collecting and transmitting to higher-level relevant and non-private data, which can be used to assess at CI-SOC, smooth out discrepancies which initiate corresponding counter-measures.

The SMG represents both the interoperability (1) and the network-edge-isolation (2) features. In one viewpoint, the utilization of SMG is an implementation of so-called trusted zone, a kind of shield that allows preventing intrusions. Compared with a limited computational power of a calibrated/certified metrology device, another vision considers the SMG as a kind of higher-power computation unit.

5.4.2 Database-centric architecture

Smart meter data can offer sharp insights into consumer energy use and consequently into users' habits at home.

NORM is based on a "database centric architecture". Any access of external actors qualified in SUCCESS Components can be only done by accessing the central database of NORM through two specific interfaces, which are incorporating Role Based Access Control (RBAC).

The Smart Meter Gateway (SMG) [i.18], in NORM architecture, serves as meter, as a PMU data acquisition device and as the only interface with public IP networks such as internet or local network-based e.g. on Wi-Fi™ connection to internet.

As shown in Figure 10, the SMG architecture has a database-centric approach and is originated from SMX developed in Nobel Grid.

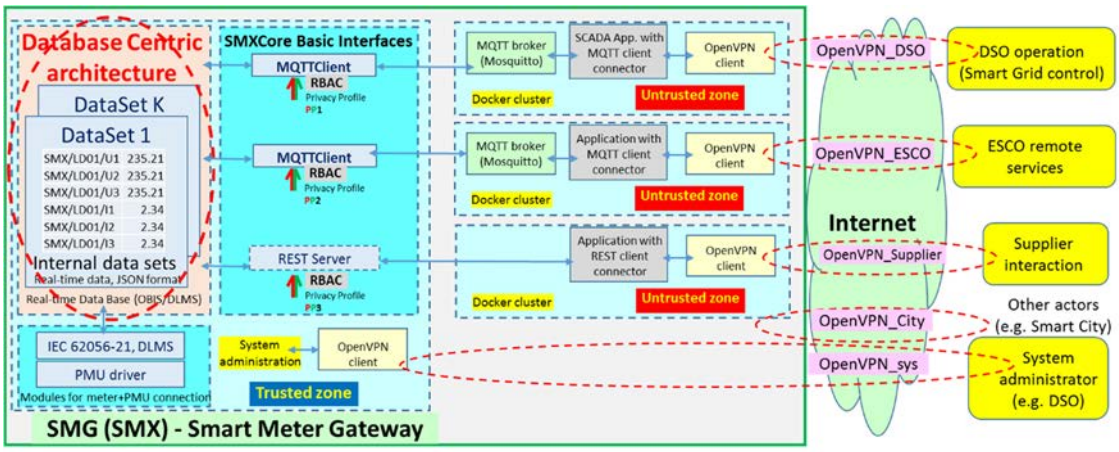

Figure 10: Database centric architecture [i.18]

In Figure 10 is indicated that all metering and PMU data is sent in the real-time database, in different datasets and that, the only way to connect with different external actors is accessing the database through MQTT and REST interfaces.

By using a Role based Access Control (RBAC) approach, which allows different data privacy policies to be applied to each actor, this data-centric architecture enables a strong control regarding the access of different actors to the data.

5.4.3 Data privacy profiles

Data privacy [i.18] represents an important legal issue. A different privacy policy can be established, depending on the type of metering point:

- for metering points serving citizen's houses or apartments, it implements personal data protection, therefore, collected data is subject to privacy assessment. This implemented also to prosumer's metering data, where renewable production, storage and consumption are "behind the meter";
- for metering points in the grid, it might be necessary to consider them as critical infrastructure data, although they can not be classified as personal data; and
- for metering points related to energy production, some data can be considered critical as well.

For this reason, NORM has to implement a so called "Privacy profile", which will be parameterized based on the type of metering point.

The database centric architecture usage entails that any connection of each external actor can be done only by accessing the database through MQTT [i.38], and REST interfaces [i.18]. These interfaces are already incorporating Role Based Access Control (RBAC) [i.18], and its implementation takes into account specific Privacy Profiles (PP) for each actor.

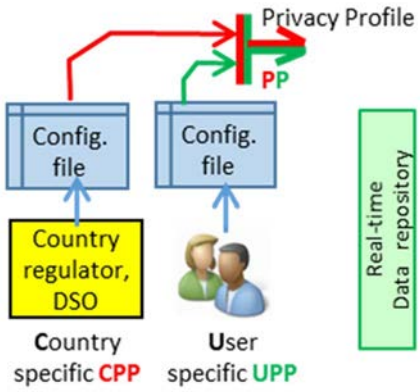

Figure 11: Privacy Profiles [i.18]

For example, in Figure 11, the PP1 privacy profile is a particular profile related to the DSO operation, implying that it can only be used to exchange data, which are allowed for DSO. Moreover, a specific OpenVPN [i.18] is used to communicate with the DSO and the whole SCADA application is considered as being in an untrusted zone, thus being sandboxed in a Docker cluster containing an MQTT broker, the SCADA app with IEC 61850 protocol [i.35], [i.18] and the OpenVPN client. This allows having a secure environment for the external communication to be kept with the DSO actor. The same policy of data access and communication is applied to any other actors (such as ESCO or supplier).

By using an OpenVPN client in the trusted zone, a special session can be obtained when communicating for system administration . It establishes an OpenVPN connection with the remote system administrator, which usually is also the DSO, but can be also another entity, which is entitled to make the NORM/SMG maintenance.

Privacy profiles PP1, ... PP3, etc. are a combination of data access policies that respect both:

- country specific rules (provided by national law, country regulatory authority and by the DSO), denominated Country Privacy Profile (CPP); and
- user specific rules, defined in User Privacy Profile UPP.

Priorities between DSO and user preferences, are defined in the country specific rules. For example, for measurements regarding the voltages, the DSO can have the right to read the data, without the user consent, however for the measurements regarding the active powers of the user consumption only the user has the right to give or not this rich content and privacy sensitive data to any actor (including for DSO).

Based on the specific laws and country regulator rules, PP structure can vary from country to country. In Figure 12 is shown the wider perspective of NORM interaction with different users and actors.

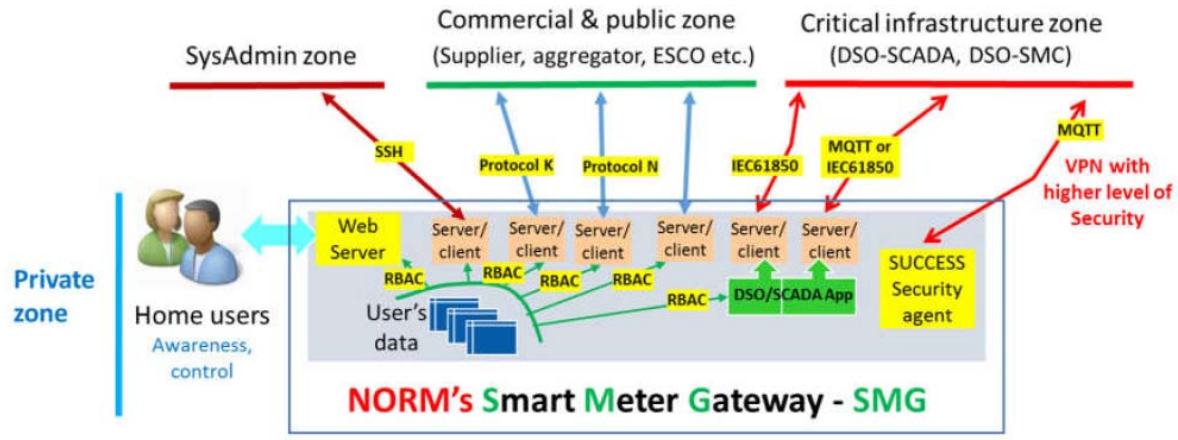

Figure 12: NORM-SMG and actors interaction through RBAC system [i.18]

5.5 Smart metrology Meter

The metrological part of NORM is represented by the Smart metrology meter (SMM) [i.18], which is considered as being a market existing meter, in the SUCCESS project, and is chosen as being a meter present in the sites of the demonstrators. SUCCESS does not focus on a new SMM, but on the new NORM architecture which, as already has been discussed is based on unbundling the different critical components.

The metrology feature of this part is crucial as well as it allows NORM to have the status of a Smart Meter, as long as it maintains the legal power of metrology. This allows the measurements to be used for billing purposes, thus being usable in case of legal disputes.

SMM can be certified by its own, as well as it acts as a legal black box containing un-modifiable data, without affecting the other NORM components.

The market existing meter is connected to SMG through a serial connection in the practical demonstration of NORM architecture. This represents the only feasible interaction way between SMM and SMG, based on standard protocols available for the meter, such as ETSI TS 104 001 [i.2] and Device Language Message specification and COmpanion Specification for Energy Metering (DLMS/COSEM) [i.39] and [i.40].

5.6 Low cost Phasor Measurement Unit (PMU)

Phasor Measurement Units (PMUs) [i.18] are new devices in the distribution network, mainly being used in the transmission system, operated by Transmission and System Operator (TSO). The concept of measuring of angles of voltages and currents on phases is basically based on the fact that there is a very good time synchronization between different PMUs. Due to this requirement, PMUs currently use GPS as the principal time synchronization source, which requires the GPS receiver to be mounted in a certain place in order to have full visibility of the the sky and satellites.

SUCCESS targeted the large implementation of basic PMU features in any smart meter of the low voltage distribution grid. This is done according to the following approach: only voltages are subject of PMU measurements (voltages phases are the most important for assessing active grid or microgrid functionality) and synchronization is done by combining high-speed IP-network and 5G connectivity.

In the PMU the absolute clock synchronization is obtained through GPS signal. This signal, however, can be spoofed. This vulnerability is mitigated in SUCCESS by adding the clock synchronization throughout data network, using the PTP protocol [i.41].

The project proposes the use of Precise Time Protocol (PTP) for the synchronization while being able to synchronize with a GPS module as well. In addition, a built-in feature offered by the PTP module is a Pulse per Second (PPS) generation on a GPIO, which gives a test point and a synchronization trigger source for the low-cost PMU analogue-to-digital converters.

The PPS signal and the PTP time reference are used by the phasor calculation algorithm to synchronize the data acquisition and timestamp the calculated phasors. The GPS PPS signal activates the sample acquisition every second. In order to calculate the frequency, the samples are digitally filtered and then elaborated by a zero-crossing algorithm. The samples are then sent to a block in order to calculate the Discrete Fourier Transform (DFT) and published via UDP.

The coexistence of multiple clock synchronization sources (GPS and data network) makes it possible to implement detection logic against such clock synchronization attacks. Local GPS synchronization is an additional source of synchronized clock, which brings more redundancy and better chance of detecting malicious synchronization. Thus, a local GPS device can be added to aid implementation of a syndicated detection of suspicious synchronization sources.

5.7 Physical Unclonable Function (PUF) component

5.7.1 Introduction to the Physical Unclonable Function

Smart meters are deployed to the premises of remote end users and left unattended. An unwanted risk comes from users opening the device and changing something, a condition to monitor and to report about. Physical Unclonable Functions (PUFs) [i.18] are defined as physical functions (often parallelized to one-way functions) represented on physical structures and can be easily evaluated/validated but can be hardly predicted. Being one-way functions, once given an input string (called challenge), PUFs typically produce a *unique* output string (called response). PUFs establish their operation on the uniqueness of their precise manufacturing process (leveraging their physical microstructure uniqueness). They are basically impossible to replicate and are, therefore used in applications with high security requirements as security/authentication mechanisms. In SUCCESS, a PUF tool is applied to the NORM context, as a way to offer authentication and encryption. The access to it through the different NORM components is simplified by a "local PUF agent", specifically a simple web service enabling RESTful access to the rest of the NORM components. PUF has a dual role in the overall NORM architecture:

1) provide a way to authenticate NORM against the CI-SOC, i.e. providing unique features and supporting PUF-based authentication; and

2) deliver on-demand encryption services to the different data services included in the overall SMG concept (e.g. the low-cost PMU or the metering services).

The service endpoint URLs over Secure HTTP (https), are offered by the local PUF agent and expose services related to:

1) bootstrapping the PUF functionality to the CI-SOC Key Management module;

2) authentication versus the CI-SOC Key Management module;

3) transmitted data encryption.

5.7.2 Bootstrapping services

It is very important, before a PUF deployment on a NORM, to have a large number of challenge-response pairs at the authentication server level (Key Management component of the CI-SOC). For this purpose, the PUF local agent offers a service that can communicate with an appointed CI-SOC Key Management module to carry out the bootstrapping as follows:

- The CI-SOC Key Management module's bootstrapping service is triggered by the local PUF agent, defining a number of expected challenges.

- The local PUF agent elaborates the response coming from the CI-SOC Key Management module (comprising a dictionary of challenges) and replies with a dictionary of responses.

In order to avoid the public exposure of the challenge-response pairs, the above procedure can be carried out in a controlled environment or at least in a non-field setting. When the bootstrapping is done at field settings, the above procedures can be executed only if the communication link is protected by encryption (e.g. VPN).

The PUF is ready for field use [i.18] after this bootstrapping procedure has been completed.

5.7.3 Authentication services

Once the bootstrapping procedure has been executed and the PUF-enabled NORM has been placed into service, the NORM can send authentication requests against the CI-SOC [i.18].

In the strong PUF implementation context, used in SUCCESS, each PUF can authenticate itself against a unique active challenge, depending on the node's the bootstrapping configuration regarding the number of challenge strings demanded by the local PUF agent. Theoretically, this challenge can only be used once, and then be cancelled, so a malicious third party cannot overhear and reuse it. Nevertheless, as the PUF-supported operations occur over encrypted (VPN) channels, in the context of SUCCESS, is attempted a re-usage of a challenge-response pair for a limited amount of time, specifically all requests that occur in the timeframe of a minute are related to the same challenge.

The PUF can authenticate itself to the CI-SOC Key Management module by giving its ID and a corresponding reply to the active PUF challenge. For this purpose, the local PUF agent keeps the active challenge in RAM. It manages the PUF authentication at any given time and periodically sends authentication requests. If there is no active challenge in RAM (e.g. in the case of a NORM reboot), a new challenge request is sent to the CI-SOC Key Management module. The CI-SOC Key Management module already offers a mechanism for communicating new challenges at pre-defined time intervals (e.g. every 1-hour or less, depending on constraints encountered during the developments), to registered PUF-enabled NORMs.

5.7.4 Encryption services

Considering that the bootstrapping and authentication processes function correctly, the local PUF agent [i.18] can provide AES-based encryption services to the different NORM modules pertaining to the SMG range. Regarding this, a RESTful API is exposed by the local PUF agent that the NORM modules can use to encrypt data POSTed to the service. The steps followed when is received such a request are as follows:

1) ensure that there is an active challenge in RAM:

   a) if this is not true, demand the CI-SOC Key Management module for a new challenge;

2) demand the PUF for a new encryption request, sending as input the active challenge and the data to be encrypted; and

3) receive the encrypted data from PUF and enclose them in the response to the original encryption request.

The PUF encryption mechanism is using the active challenge to generate an appropriate response, that will be used as the encryption key for the data encryption process. Since the CI-SOC Key Management module is aware of the envisioned responses to the batch of known challenges of all the PUFs, the data decryption (at the server side) is reasonably feasible.

It important to emphasize the fact that this encryption can operate together with the encrypted channels methodology (VPN) used by SUCCESS for the critical, security-related information sent to the CI-SOC by the NORM to, adding another security layer on top of the existing one. Therefore, even if a third party has physical access to the storage contents of NORM, hence also the VPN configuration/keys), the information transmitted from NORM to the CI-SOC can not be overheard.

5.8 Security Agents

The Smart Meter Security Agent (SecA) [i.18] is an instance of software in each edge, on each meter and in the cloud as DSO security agent and as a Regional Centre Security Agent. This design allows performing intelligence-based data traffic analysis in order to uncover a potential CKC attack.

The Security Agent can run in this trusted zone and can implement the following functionalities:

a) Collect non-confidential data such as frequency, voltages, angles of voltages and rate of change of frequency (ROCOF) - which are mainly grid data that can be measured by anyone.

b) Monitor data traffic with each external actor, including related to attempts to exchange data not allowed by each RBAC.

c) Monitor the health of applications and of critical files on local storage resources, by checking their hash value, the number of read-writes, the available free space and more.

d) Send non-confidential data which is relevant from cyber-security point of view to a higher level of security applications (to a CI-SOC or Critical Infrastructure Security Operations Centre), where data is correlated with other grid data received from other NORMs, in order to assess data inconsistencies. These inconsistencies can show cyber-attacks and compromised data sources, in order to trigger countermeasures.

SecA handles encryption and cryptographic tasks and formats messages in order to include all the relevant information:

- verify data integrity;
- decrypt messages;
- to identify possible threats, further inspect the received value.

Figure 13 provides a first view of the data monitoring and control approach by using SecA in the SMG communication with the higher level (CI-SOC).

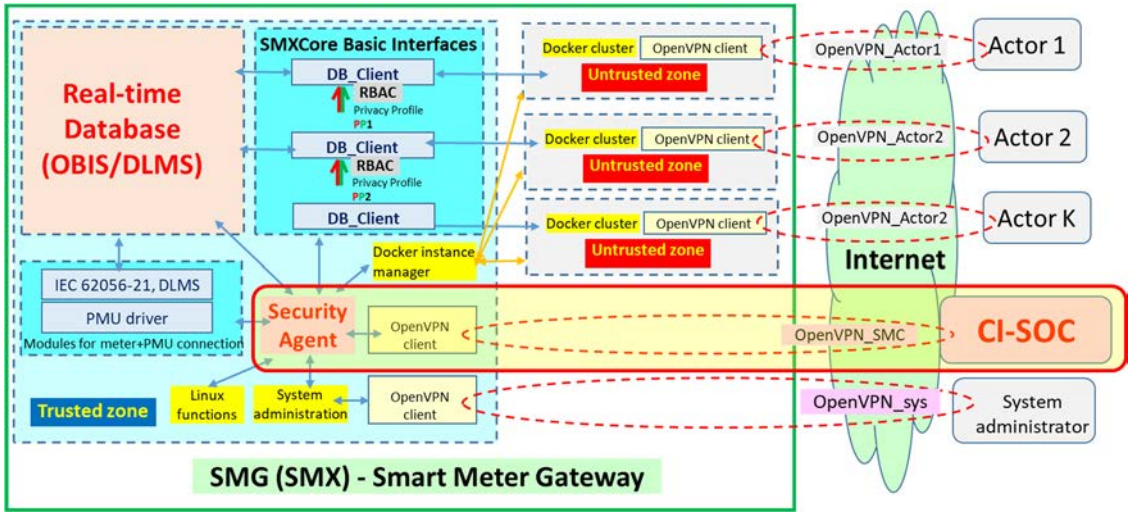

Figure 13: Security Agent in SMG [i.18]

The Security Agent module communicates with all relevant modules, specifically with the real-time database and with all communication interfaces, as well as with components in charge of the message encryption and hashing messages. From an architectural perspective, both "System Administrator" and "CI-SOC" are connected to the "Trusted zone", as being the only SMG element with the necessary rights to get access to configuring external applications.

A critical problem is the need to protect, where applicable, the *privacy of user data*, in compliance with Regional (European) laws and the energy authorities in different countries. The privacy concerns are important at the consumer level, but energy related grid data, which does not refer to particular clients or are aggregated data, are mostly data that can be used as it is for the CI Security Operation Centre.

The Security Agent collects and pre-processes measurement values coming from both smart meters and PMU, so that more information to elaborate are available to the CI-SOC. The Security Agent verifies the congruity of collected data after obtaining the identified measurements, by comparing values generated by smart meter and PMU.

Many important aspects of the SMG, are regularly verified by the Security Administration Agent (SAA), such as hash-codes of relevant parts of the software and of sensitive files like important configuration files.

A higher secure VPN, is used by SecA to exchange data with higher level (e.g. CI-SOC), where data is sent with enhanced PUF security encryption, which makes the channel used for cyber-security highly impenetrable compared to normal communication paths.

In the present solution, PUF can make authentic a NORM with regard to NORM identifier. Typically, a NORM is made up by PUF, SMG and SMM. Located inside the NORM, the Security Agent (SecA), guarantees the uniqueness and the indivisibility of the overall aggregate.

So, for each NORM made up by PUF, SMG and SMM, the SecA generates an identity (id). It generates a distinct id for every single NORM, considering three identifiers: PUF id, SMM id and SMG id. The SecA uses a function based on the SHA-256 algorithm to create a hash-based identity (Id).

The hash function is installed specifically in in SecA in NORM and SecA Driver in CI-SOC. When the NORM_id is detected by SecA Driver for the first time, it stores the id in its internal repository.

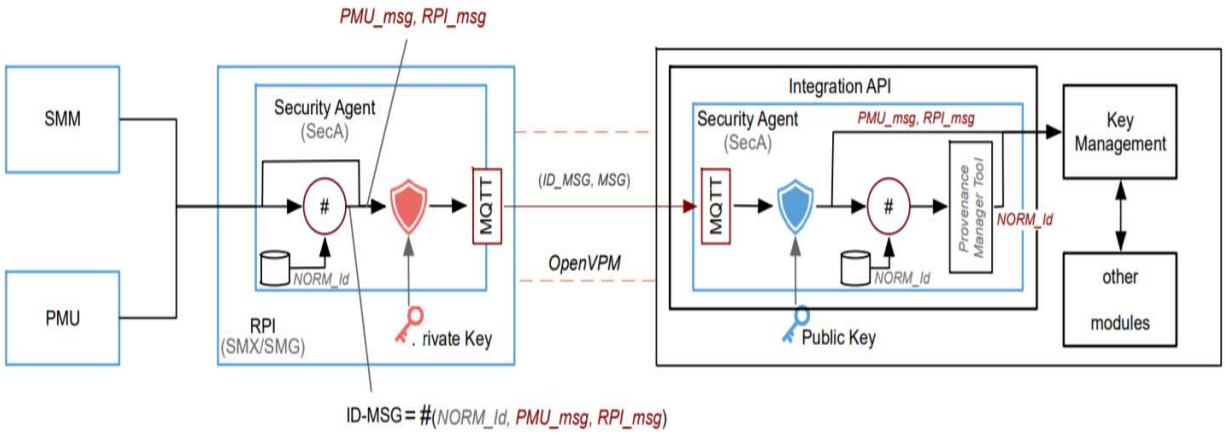

Figure 14: Security Agent architecture [i.18]

Regarding this, a PUF will be identified as a new element if it is removed from a given NORM and associated to another.

It is necessary to encrypt the message to make the communication between NORM and CI-SOC more secure. The local PUF agent on NORM executes this encryption. Then the encrypted message is sent to CI-SOC by the SecA finally via MQTT message. The CI-SOC then decrypts the received message by communicating with the Key Management Module (KMM) to obtain information relevant for its elaboration, i.e. voltages and frequencies.

In addition in each message is included a hash, generated by the Data Centric Security agent, based on the NORM following data:

- "norm_ip": IP address of the NORM;
- "request_id": alpha-numeric id of the hash request;
- "request_ts": timestamp when the hash is requested;
- "norm_data": encrypted NORM data.

A certificate and a hash are created by the DCS and sent back to the Security Agent. Both hash and the request id are then included as `hashed_data` in the message that is sent to CI-SOC. These values are then used by the CI-SOC to verify data integrity by interacting with the Breakout Gateway. This approach offers the possibility to detect every type of intrusion between NORM and CI-SOC; if the data integrity verification fails, a threat is issued and then will be applied an appropriate countermeasure.

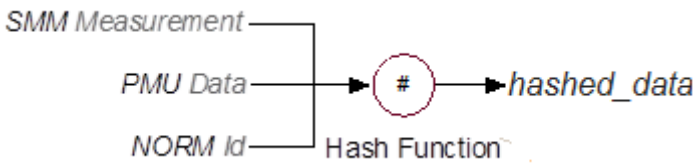

Figure 15: hashed_data generation [i.18]

On top of that, the Security Agent can verify firewall rules set in the NORM, principally following a CI-SOC request. If this check fails, by the interaction with the local PUF agent on NORM (LPA), can be applied appropriate countermeasures.

5.9 Intelligence based data driven analysis of the communication patterns between meters

In TEC scenario, a smart meter locally measures the Demand Side Flexibility (DSF) of a user, receives a price signal from an operator, and takes a decision about materializing an ancillary balancing service against an amount of money. It is absolutely normal that a smart meter interacts with a data concentrator and/or a remote broker/aggregator agent. It is also normal to replace a metering data concentrator for any reason. Therefore, a meter alone cannot perform identity management. An unencrypted communication scenario offers a chance to an attacker to simulate the broker/aggregator agent, especially because of interoperability conditions implemented in communication protocols. There are no obvious ways to increase the security. To implement risk-hedging functionality, smart meters can be able to detect any change in the data communication patterns and to report it to an agent capable to distinguish between a legal and illegal operations.

New defensive functionality can be implemented in each smart meter by reconfiguring the network card component in a way to intercept all data communication messages and to make a data log. Over a long time-horizon, a smart meter can inspect all data packets in order to elaborate descriptive statistics about the common data pattern(s). After each change and each change can be considered as a suspicious case, smart meter can report to a cloud-based Security Agent.

Because there is no apparent difference between being polled once only by a remote actor and between a scanning attempt in which the same remote actor poll several but many smart meters, the early detection of a (staged) cyber-attack can be enacted by the cloud-based Security Agent.

Since the Security Agents are available in all layers of Smart metering infrastructures, they can be used to analyse the communication patterns affecting the Smart Meters. For example, an individual Smart Meter cannot detect a scanning attempt, while the networked agent can analyse a set of information about requests received by many meters to conclude about the same originator interacting with many meters from the same network.

The network-based intelligence allows the detection of the reconnaissance stage of the CKC.

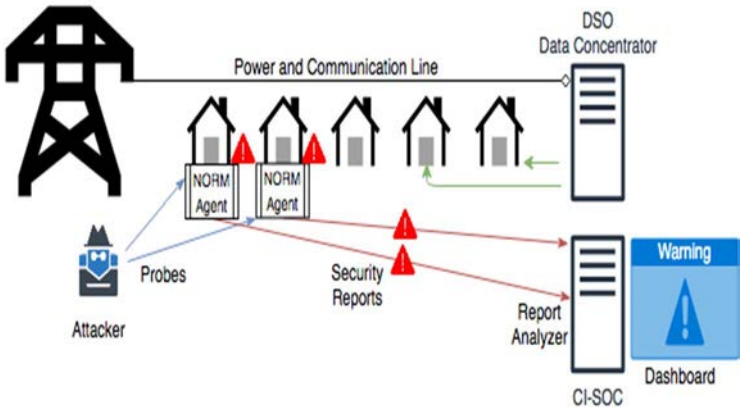

Figure 16: Distributed and Collaborative Agent-Based system [i.25]

This defence strategy is based on the early discovery of the Reconnaissance activity. There can be several alternative technical implementations.

In the first variant, a Security Agent (SecA) is installed for networks traffic monitoring purpose (cloud-computing approach). In the second variant, the same role can be assigned to the SMs (edge-computing approach). In the third variant, the intelligence can be distributed between one or few centralized SecAs and the ubiquitous SMs (a mix between cloud- and edge- computing).

A single SM electronic device cannot distinguish between "normal" network probing and coordinated reconnaissance activities by itself. However, multiple devices can collaborate in reporting about the abnormal network traffic to a Central Security Agent (CSA). This CSA has a global view of the security state of its network of reference.

In normal operational scenario, SMs interacts with the known Smart Metering Data Concentrators (SMDC) only. The master-slave relationship between the peers in a Multi-Agent System (MAS) dictates an intended behavioural model in an ICS scenario. However, the network can be re-configured dynamically. In such a case, SMs are not necessarily informed in advance about a change going to happen. As a result, the changed topology/roles are not necessarily clues of an attack but as an interplay between SMs and unidentified remote peers - potential attackers - can be dangerous, so it can be carefully monitored by someone. For an actively protected power network, the distributed devices (NORM) implement passive network sensors that listen for unsolicited traffic coming from unknown sources. Different levels of information can be analysed in order to discover suspicious traffic, depending on the considered OSI layer.

At device level are considered mainly layers up to Network Layer, implementing in fact a shallow packet inspection. This is necessary to keep a low usage of resources, which are usually limited in similar devices. This information is used for a first local distinction between expected and unexpected requests.

Information about upper layer 4 (Transport Layer- ISO/OSI) is also reported to the Central Security Agent depicted inside the box CI-SOC (Figure 16), so that it can better relate multiple network traces. This security by design concept combines approaches developed in the power systems and in the IT sectors into a joint attack detection and mitigation scheme.

5.10 Grid data consistency assessment

Another criterion for being able to detect cyber-threats, especially for detecting false data injection, is the assessment of grid data at CI-SOC level. Grid data such as frequency and voltage, being transmitted by the NORM agent to CI-SOC, can be analysed in terms of data consistency. Such preliminary analysis is presented in the paper [i.6], but more assessments have since been made using frequency measured in different metering points and applying statistical methods.

The main threats are related to cyber-penetration at the level of the smart meter, which can bring manipulation of the grid data through false data injection at the lowest acquisition level. Wrong data acquired from the meters can affect several functionalities at the grid control level, which can threaten major functionalities such as grid stability, power quality, e.g. voltage levels as well as microgrid functionalities, thus needing detection in order to apply countermeasures. In this context the focus is on the assessment of data, which has no private aspects, meaning data related to grid, such as voltage level and voltage phases obtained from PMUs and grid frequency are part of a privacy by design approach. While voltage can differ between metering points, frequency in the same area can have a very good similarity, forming a dataset, which needs to be consistent. NORM acquires from the meter part the most important real-time data, which is available on the communication interface.

In this scenario, the local advanced measurement information of NORM is provided to a specialized Critical Infrastructure Security Operations Centre (CI-SOC), which can be used to monitor consistency of grid data across the network in order to address false data injection threats, without jeopardizing the end-customer privacy during its regular services activity. Non-privacy intrusive methods of consistency assessment are possible in parallel with other activities performed by NORM. This case is particularly interesting because it gives solutions for relying on both secure grid operation as well as enabled free market of services, while determining significant savings in investment costs, thanks to a dual or multiple use of available information, which is assessed for inconsistency in parallel with normal communication of NORM with various actors. As cyber-security concerns are killing factors for all these activities, the NORM security-by-design approach intends to reduce risks and allows for more secure actor activity, in an ICT enabled environment.

5.11 NORM Security Administration Agent

The SUCCESS Security Administration Agent (SAA) [i.18] represents a component that periodically verifies some crucial elements of the SMG, such as hash-codes of important parts of the software and of critical files (e.g. essential configuration files like the Privacy Profile files). A highly secure VPN is used by the Security Administration Agent to exchange data with a higher level (e.g. the administrator in the BR-GW). Data sent through the secure VPN has enhanced PUF security encryption, which makes the channel used for cyber-security completely impenetrable compared to normal communication paths.

6 Privacy by Design in Smart Meters

SUCCESS Project has well implemented those best practices in technical solutions, called "privacy-by-design" solutions [i.20], whose purpose was also to enhance the protection of personal data of end-users and energy operator physical persons. Specifically, SUCCESS was based on identifying and solving cyber-threats for smart grids and this can be for sure the best way to protect "metering data", in compliance with the Data Integrity principle.

In the following clause is given a short summary of the **privacy-by-design solutions** as applied in the context of SUCCESS [i.20]. Therefore, a list of the implemented SUCCESS solutions follows:

- **Utility level data anonymization** which, based on the *relative* and *subjective* concept of anonymity executes a process of data *de-personalization* before they leave the user-level.
- A **Role Based Access Control System (RBAC)** helps end-users to decide which category of subjects (based on their roles) can access their data, when, how, and how long. This is compliant to the *principle of transparency* (the data owner is fully aware of who can access his/her data) and with the purpose of ensuring him/her a minimum level of *control on the processing* of his/her personal data.
- **The sharing only network data (and not consumption data)**, to avoid the personal data transmission above the utility level.
- **A "database centric architecture"**, used to prohibit any access by external entities without going through the NORM central database. The access to this database can be achieved only via MQTT-based interfaces implementing RBAC.
- **A system that allows the DSO to access only specific data, after the end-users approval**. This is important to be conform with the principle of data-minimization and to ensure to the end-user a minimum level of control on his/her data.
- **As a way of protecting the communication with the DSO and also with all other actors** (e.g. ESCO or energy supplier): a VPN is used for the data communication with the particular DSO and the whole SCADA application is sandboxed in a Docker cluster comprising an MQTT broker, the SCADA application with IEC 61850 [i.35], [i.20] protocol, and the VPN client.
- **A "User Privacy Profile" UPP** system, which entitles any particular qualified actor within the SUCCESS Components to access data. This approach is implemented in order to comply with:
  - Specific National laws related to the smart grid's maintenance and also with the public security rules regarding the energy sector.
  - Particular instructions provided through the UPP by the end-users.
  - Data protection framework, specifically art. 6 of the GDPR (Reg. EU 679/2016 [i.42]).
- **"SMXCore"**, an MQTT oriented Open Source/Open Access platform used to provide each end-user (data subject/owner) with the opportunity to access his/her own particular user account on this platform. This platform allows end-users to:
  - access personal data regarding not only user's data energy consumption data, etc.;
  - privacy profiles access control (allow and deny);
  - revise certain data previously submitted to the DSO (e.g. identification data like name, id code, home/building information, etc.);
  - read intentions and any other relevant information about the data processing (according to art. 15, GDPR);
  - control the personal data flow through the platform.
- The prospect of exercising the right to delete and the portability rights through a particular request to the DSO Data Protection Officer.

- The opportunity for NORM users to specify a particular time period when data can be shared. Consequently, the period of the data flow from NORM to DSO or other possible smart grid system subjects or components can be pre-set "by-design".
- A "double virtualization" system, comprising two separated layers, specifically a data-layer (storing all personal data) and a functionality-layer. This separation represents a sort of data minimization and can enhances disaster recovery. In case of an attack targeting a single layer, its efficiency will be limited as the other layer will not be compromised and all the critical entities will be migrated to the other layer.
- A Double Virtualization (DV) technology represents a procedure for both grid and functionality data backup.

In addition, the Smart Meter designed within SUCCESS (called "NORM") collects personal data but does not share them with other components/agents/operators: there is an automated tool (called Role Based Access Control System) through which end-users can decide who (which kind of subjects based on their roles) can access their data, when, how and how long. In general, however, just network data (and not consumption data) are shared, so there is no flow of personal data beyond the Utility level.

Another important solution is that access to data are controlled and logged, but since those logs are personal data (of the physical operator of the Energy Service), there is a system of anonymization of all data before leaving the Utility level.

In addition, to enhance security of data all information is stored in a Cloud (Smart meter Gateway), but this "virtualization of data" (called "double virtualization") is divided into two parts: a Data Layer and a Functionality Layer. Data Layer (where all personal data are stored) is totally separated from the Functionality Layer. This is a form of data minimization, though enhancing disaster recovery solutions.

Table 3: Comparison between Privacy Principles, best practices for the energy services and privacy-by-design solutions developed in SUCCESS [i.20]

Privacy Principles	Best Practices in theory in the Energy Sector	Best Practices in practice in the Energy Sector	Privacy-by-design solution in SUCCESS
Data integrity	Data access controls; Prevention of unauthorized disclosures; Pseudonymization	Metering Data Protection	Cyber-threats analysis
Data minimization; Purpose Limitation	Avoiding unnecessary use of personal data	Anonymization of Metering Data	NORM and RBAC System
Data storage Limitation	Aggregating data as much as possible	Aggregating data as much as possible	'Double Virtualization'
Lawfulness, fairness, Accountability	Continuous assessment of data processing purposes and of the respect of users' rights	Anticipated and continuous DPIA	Three-steps test DPIA

7 Conclusions

Concerning electronic (IoT) metering devices of any kind, those pervasively shaping the deployments of Smart Grid nation-wide, the present document considers them as crucial part responsible for the vulnerability of the entire complex system-of-systems. Because of the lower costs, and because of the intrinsic contradiction between the grid-wide interoperability (bi-directional communication) and the security in ICS and other CPS, the present document suggests standardization of the additional security-oriented components recently added to the system of system [i.20].

Since novel smart meters are designed to implement the enabling role of forthcoming business operations, the addition of security requirements appears natural.

The present document has proposed an addition of a Multi-Agent System - a layer hosting edge-SecA and cloud-SecA - in order to perform data traffic monitoring and the intelligent based identity management aimed to improve the security of critical infrastructure.

The Security by Design - and its constituent's - concepts can be used in two very different contexts, namely development - and reuse - ones. During development, **prescriptive norms** are needed to ensure that the resulting system will be interoperable. During reuse, **descriptive metrics** are required to allow evaluating whether a legacy system can be used in a new operational context or not. Both contexts are connected when legacy systems are changed in order to migrate towards new (improved security) solutions. As such, the ETSI standardization process is a tool to ensure the intended quality of regional critical infrastructure.

History

Document history		
V1.1.1	December 2019	Publication
V1.2.1	September 2020	Publication