# ETSI TR 103 644 V1.1.1 (2019-12)


**CYBER;**
**Increasing smart meter security**

Reference

DTR/CYBER-0037

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



***Important notice***

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

# 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 gives some indications for increasing Smart Meters security, based on the outcomes of the SUCCESS H2020 project, with a focus on the cyber security aspects of the smart meters. The present document provides an overview of the Security Monitoring Framework architecture including threat detection and countermeasures. It includes design aspects regarding the cyber security of the smart meters, and the privacy by design concept.

# 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.

# 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 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.

**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

**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 energy meter:** device to measure the energy consumption data and make these data available for Smart service provider and the local application server, mostly operating in two-way communications device in reliable manner with a set of management functions

**Smart Grid (SG):** achieved by overlaying the power systems infrastructure with communications infrastructure

NOTE: Smart Grid (SG) is a wide-area energy - energy that comes from any vector and/or commodity - distribution network based on *digital technology* (1) that is *used* (2) to supply energy-containing commodity to consumers via *two-way digital communication* (3). SG is a system of systems, a superposition of different systems that contains an *information network* (a) and a physical commodity *distribution network* (b). Smart Grid is an example of Cyber Physical System.

**Smart Meter (SM):** electronic/digital device that measures the consumption data

NOTE: Meters can act as measurement- or data concentrator- devices. Metering data referrers to any energy-containing commodity including electricity, gas, heat, water, and similar. SM is part of Smart Grid.

**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. 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 |
| 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 |
| 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.