Vaasan yliopisto
UNIVERSITY OF VAASA

Technical Report TR 3.2

IEC 62351
Data and Communication Security: Power Systems Management and Associated Information Exchange

Mike Mekkanen
10th August 2021

Vaasa 2021

Programme for Sustainable Growth and Jobs

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Disclaimer

This document is for informational purposes only and is not meant to replace current technical reports and/or standards from key authority organizations. Furthermore, the job was completed by analyzing and studying current IEC authority organization standards and reports. Finally, due to the ongoing nature of this project, changes may occur between this version and the final release.

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Contents

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Abbreviations

ACSE	Association Control Service Element
AE	Authenticated Encryption
APDU	Application Protocol Data Unit
API	Application Programming interface
BER	Basic Encoding Rules
CA	Certification Authority
CBC	Cipher Block Chaining
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DHE	Ephemeral Diffie-Hellman
E2E	End-to-End
ECDHE	Elliptic Curve Ephemeral Diffie-Hellman
EnvPDU	Environment Protocol Data Unit
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Keyed-hash Message Authentication Code
ICCP	linter-Control Centre Communications Protocol
ICV	Integrity Check Value
lPsec	internet Protocol security
JID	Jabber identifier
MAC	Message Authentication Code
MMS	Manufacturing Message Specification
OCSP	Online Certificate Status Protocol
PDU	Protocol Data Unit
PDV	Presentation Data Value
PPDU	Presentation Protocol Data Unit
PTPDU	Protected Protocol Data Unit
SecPDU	Security Protocol Data Unit
SPDU	Session Protocol Data Unit
TASE.2	Telecontrol Application Service Element 2
TPDU	Transport Protocol Data Unit
UTC	Coordinated Universal Time
VPN	Virtual Private Network
XER	XML Encoding Rules
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	XML Schema Definition

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Executive Summary

Electric utilities are boosting their digitization and connectivity, to increase operational efficiency and satisfy consumer requirements in real time. This aim is accomplished through combining/using ICT (Information and Communication Technology) and standards. While incorporating these innovative technologies/standards into the energy framework have become one of the most important components of the energy framework's profiles and allow for/enables interconnectivity, it also raises cyber security concerns by increasing attack surfaces.

In addition, the deregulated market has created new threats, such as data about a competitor's assets and system activity, which might be beneficial, and obtaining such information could be a possibility.

Furthermore, critical infrastructure attacks have grown dramatically in recent years. These cyberattacks have advanced to the point where they may have had far-reaching consequences and unforeseen societal consequences. As a result, the World Economic Forum has classified cyberattacks on critical infrastructure as one of the top five global risks.

As a result, utilities are increasingly looking into ways to improve the cyber security of their networks, industrial controls, and business continuity to improve ES cyber resiliency. The IEC 62351 standard describes how to provide cybersecurity to an ES environment to protect it. IEC 62351 defines, among other things, the use of innovative cyber security IT technologies/tools that are suited for essential ES needs, such as IEC 62351-4 provides security for MMS protocol, IEC 62351-6 provides security for IEC 61850 communication protocols etc. The purpose of this report is to highlight and investigate these enhancements in ES cyber security in accordance with the IEC 62351 specifications.

However, these enhancements/recommendations are left to the end users/companies to assess their feasibility/suitability for their systems/networks. As a result, businesses must have in-depth knowledge of their systems and networks, as well as identify potential attack vectors and define protection procedures to mitigate the risk from the potential highest attack vectors.

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

Scope

This report's scope is concerned with the technical, information security for power system operational, and management surfaces that serve as the basis for securing the power system communication protocols defined by IEC TC 57. Specifically, the IEC 608705 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Here in this report, we consider the IEC 61850 series. Seeks to emphasis and discuss the end-to-end security issues concern with the use and adoption of IEC 62351 security standard for IEC 61850 compliant power system entities.

Here we consider the IEC 61850 Generic Object-Oriented Substation Event (GOOSE), Sample Value (SV) and Manufacturing Message Specification (MMS) protocols and means that be utilized by the modern IEDs within the horizontal and vertical for inter/intra power system communication.

Objective

The goal of this report is to highlight the IEC 62351 series, recommendations, and guidelines (classified/allocated on “How” group standards) to improve end-to-end cybersecurity for the IEC TC 57 communication profile. These improvements can be attained by introducing various mechanisms and techniques that are appropriate for and fulfill the power system operation requirements. The introduced IEC 62351 actions were identified as the obvious first steps in securing power system control operations and should include all cybersecurity issues such as security policies, security enforcement, intrusion detection, internal system and application health, and all broader security needs.

Audience

The report focuses on those who work/interest from both industry and academia in the design and development of energy systems operation control associated information exchange-data and communications security. Personnel who are being targeted include:

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

- System integrator, developers, configurators, researchers and who assess energy system communication.
- Policy makers, administrators, project designers, and network analysts
- OT/IT network security personnel
- Expert insights on securing and monitoring power systems

Document Structure

The report begins with general backgrounds to power system and digital power system communication standard defined by IEC TC 57 specifically IEC 61850 constructed data model, then moves on to its goal by explaining the IEC 62351 mechanisms and techniques for power system operation control associated information exchange-data and communications security. Following that, a comprehensive section on cyber physical security goals in energy system environment is provided, followed by an explanation of the distinction between cyber physical security, information security, and focuses on threat analysis, describing vulnerabilities, threats, and attacks. The following section describe the IEC 62351-4 Data and communication security - Profiles including MMS and derivatives, as it aims to secure the MMS protocol-based A-profile and T-profile. Finally, IEC 62351-6 Security for IEC 61850, it concerned with the IEC 61850 protocols such as GOOSE, SV, and IEC 61850 MMS protection based on adding the extension filed to enhance the cyber security of the IEC 61850 communication protocols.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

1 Introduction

Electric utilities worldwide are expanding their digitization and interconnection to acquire functional efficiencies and fulfill in real-time costumers demands. This objective is accomplished by combining/using information communication system ICT and standards which is gets quite possibly the most critical pieces of energy frameworks productive activity. While even the emerging catting edge ICT and standards to energy framework is permitting/facilitating with interconnections, it does, however, raise concerns about cyber security by increasing the attack surfaces.

Moreover, the deregulated market has introduced new threats, like data on a contender's assets and the action of his system, which can be supportive, and the getting of such information could be a potential reality.

Attacks on critical infrastructures have increased significantly in recent years. These cyberattacks have become so sophisticated that they may have resulted in major consequences and unanticipated society impacts, e.g., power outages as in Ukraine in both 2015 and 2016. Terrorism has also become a more visible threat. To that end, cyber threats to the power system are now recognized as critical threats to the safe functioning of societies, economic stability, and business continuity. As such, cyberattacks on critical infrastructure are listed as one of the top five global risks by the World Economic Forum.

Nowadays utilities are evaluating options for enhancing the cyber security of their networks, industrials controls and business continuity to improve cyber resiliency. Having real-time visibility into cyber security attacks, risks, and incidents is one from the fundamental security best practice. However, there was no such technology/solution that could provide such visibility for large, heterogeneous, high availability (HA) industrial systems, as well as offer 100% protection-system security.

Currently, various groups and committees, such as NIST, EPRI, IEEE, IEC etc., are working to develop recommendations, guidelines, solutions, and standards to improve the cyber security and operational reliability of energy systems. These developments are left to end users/companies to assess their feasibility/suitability for their sys-

tems/networks. As a result, businesses must have in-depth knowledge of their systems and networks, as well as identify potential attack vectors and define protection procedures to mitigate the risk of these attack vectors. In case cyber-breach is recognized, usage of the developed security steps is characterized to stop/eliminate this attack from exposure and moderate their impacts. Finally return to the normal operation, learn from the past events, and attempt to anticipate them in future.

1.1 Motivation

The transition of utilities to smart grid by adding a communication infrastructure to the existing energy system infrastructure provides many benefits, but it also expands the attack surfaces for threat agents seeking to disrupt power grid operations. Previously, the common approach to cybersecurity for energy systems was security through obscurity. It was assumed that potential attackers lacked the motivation and specialized knowledge needed to carry out a successful cyberattack which is nowadays considered ineffective approach. As a result, utilities must rely on truly effective security measures. At this point the goal of the IEC 62351 standard is to provide recommendations to improve the cyber-security of energy systems, by introducing cryptographic measures, monitoring capabilities, user management, and other features. Due to the contrasts between traditional IT networks and the Operations Technology (OT) networks utilized in the energy grids, existing security measures typically used for IT networks should be adjusted to react to threats pointed explicitly at energy networks. IEC 62351 achieves this by executing security measures while considering the context of energy systems, such as the specific communication protocols previously designed by the IEC and adapted to this environment. Because the IEC 62351 standard was only recently published, it has not yet been widely adopted by manufacturers or the subject of extensive research. It is therefore critical to investigate their effectiveness/capabilities in more depth by emphasizing the recommendations/guidelines provided by the standard.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

2 Energy Grid Cyber Security Goals

The three main goals of energy system cybersecurity have been revised and are usually availability, integrity, and confidentiality. Because the energy system is made up of both IT and OT systems, and its operation is heavily reliant on OT. Technologies in the OT environment have different requirements and constraints when applying security measures. In addition to these, IEC 62351 additionally focuses on non-repudiation, authentication, and authorization among its objectives. Each of these terms, as well as the threats associated with them, is defined below.

2.1 ES cybersecurity protection triangle

2.1.1 Availability

The first element of the ES cybersecurity protection triangle is availability. It is considered the most important security criterion in smart grid because the loss of availability means disruption of operation/access to information in ES. It is defined as ensuring that the ES is operational in a timely manner and that authorized access to information/operation parameters is granted. A high-availability system is ready to complete/operate its functionality in an acceptable amount of time and to be accessed by a legitimate user at any time is needed. At this point as dictated by performance requirements, attacks against ES availability include, Denial-of-Service (DoS), degradation-of-service, delay, and other assaults can all be used against ES availability. These many threats could cause the ES's availability to be reduced or lost by blocking, delaying, or fabricating information flow over the network. As a result, the network's ability to control the ES's operators will be disabled. Figure 1 depicts the IT versus OT cybersecurity goals and related priorities.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

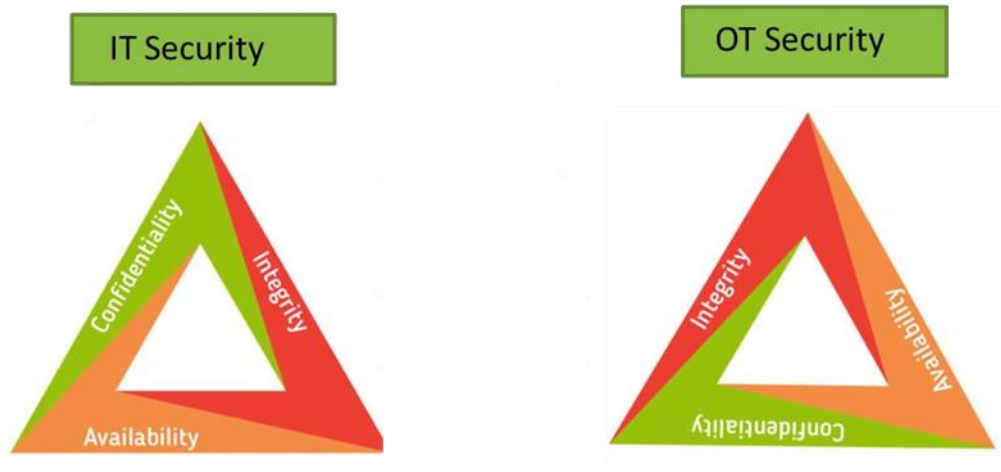

Figure 1. IT versus OT cybersecurity protection goals priorities, Omicron training course reference

2.1.2 Integrity

Integrity refers to the consistency and assurance that data/information is accurate and safeguarded from unauthorized change or destruction. In addition, the data/information is always available to the appropriate people when they need it, and the system/data can be trusted. As a result, integrity aims to prevent unauthorized writing of information. Hash functions are frequently used to achieve this. A hash function turns any length of data into a unique, tiny "hash" value of a specific length. Recalculating the hash of a certain input should always yield the same hash; if it does not, the input has been tampered with and should not be trusted. Integrity attacks entail altering data in some way, such as changing the contents of files or databases. Re-sending previously sent packets (replay), injecting forged packets into the network, or changing existing packets after introducing a Man-in-the-Middle (MitM) attack which is one from the integrity attack examples in networks. e.g., an adversary could intelligently modify power injection or consumption readings by relaying them from the power meters/flow to the controller/state estimator, resulting in an immoral condition or state (overloaded, blackout, etc.). To sustain the integrity, both nonrepudiation and authenticity of information are essential in which that will be addressed next.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

2.1.3 Confidentiality

The term "confidentiality" refers to ensuring that only authorized people/applications have access to the data. Encryption and the distribution of the decryption key to only approved entities, individuals, or processes are two ways to secure confidential data. Confidentiality is required to safeguard not only data but also credentials that must be kept secret to meet the other security objectives. Sniffing network packets, stealing sensitive data from a file or database on an end device, guessing encryption keys, and gathering intelligence on a system through scanning or eavesdropping are all examples of confidentiality attacks. For instance, data traded between a client and different substances, e.g., meter control, metering use, and charging data, should be secret and protected; otherwise, the client's data could be controlled, altered, or utilized for other hurtful purposes. Figure 1 demonstrates how the ES protection triangle's confidentiality appears in the last position. Because most ESs information, such as the single line diagram of the ES network, which could include information such as how much power each DG generates, how much power a specific load consumes, and so on, is likely to be public and available online, it is not particularly sensitive in an ES network.

2.1.4 Non-repudiation

The term "non-repudiation" refers to a method that anticipating stockholders from denying their past activities or claiming activities that did not really happen. In other words, non-repudiation guarantees that stockholders cannot stow away or distort records of their actions. This property is significant for reviewing after a security event to guarantee that the log files are dependable. Digital signatures can give a level of non-repudiation just as uprightness and confirmation for specific messages, as Digital signatures must be figured by the legitimate holder of a private key that is not imparted to different entities.

2.2 Authentication

The term "authentication" refers to the mechanisms that verify an entity's identification. Entity authentication is used to guarantee that entities are who or what they claim to be, keys, passwords, certificates, and biometrics that are unique to each entity

are a typical way to do so. Only the legitimate entity should know and be able to present the correct credentials, hence this ensures authentication. In addition, Digital signatures such as Rivest-Shamir-Adleman (RSA) and Message Authentication Codes (MACs) are employed. These strategies allow one to generate a tiny message value that can only be computed by the key's legal holder. Authentication is impossible if the authenticator is not reliable. It also generally depends on the credentials' security, since a hacker who gets them can at that point imitate another entity.

2.3 Authorization

The term "authorization" refers to a method that verifies an entity's privileges and limits its access to only authorized entities. In other words, the system must allow entities with the proper role or rights to perform actions while also preventing entities without those rights from performing actions. Authorization is a key requirement for the other security goals, as it distinguishes the real (authorized) entities from others. It is worth noting that authorization requires authentication.

2.4 Energy System New Opportunities and Potential Threats

The modern power system is a complex bulk of power and communication units that must all be linked to keep track of the world's rapidly expanding economies and populations. Were, the PS must be more resilient to address these issues. ICT features incorporated into the power system are one of the primary techniques to supporting PS resiliency. As a results Utilities have been forced to retrofit, upgrade, and update the legacy PSs and look at ways of efficient utilization, which increase interest in innovative solutions. Few years ago, managing of the power system infrastructure was only the main focused and took all utilities’ attention. That lack view has been changed based on the concept of two infrastructures must be managed, the energy system infrastructure and the communication information system infrastructure as illustrated in Figure 2.

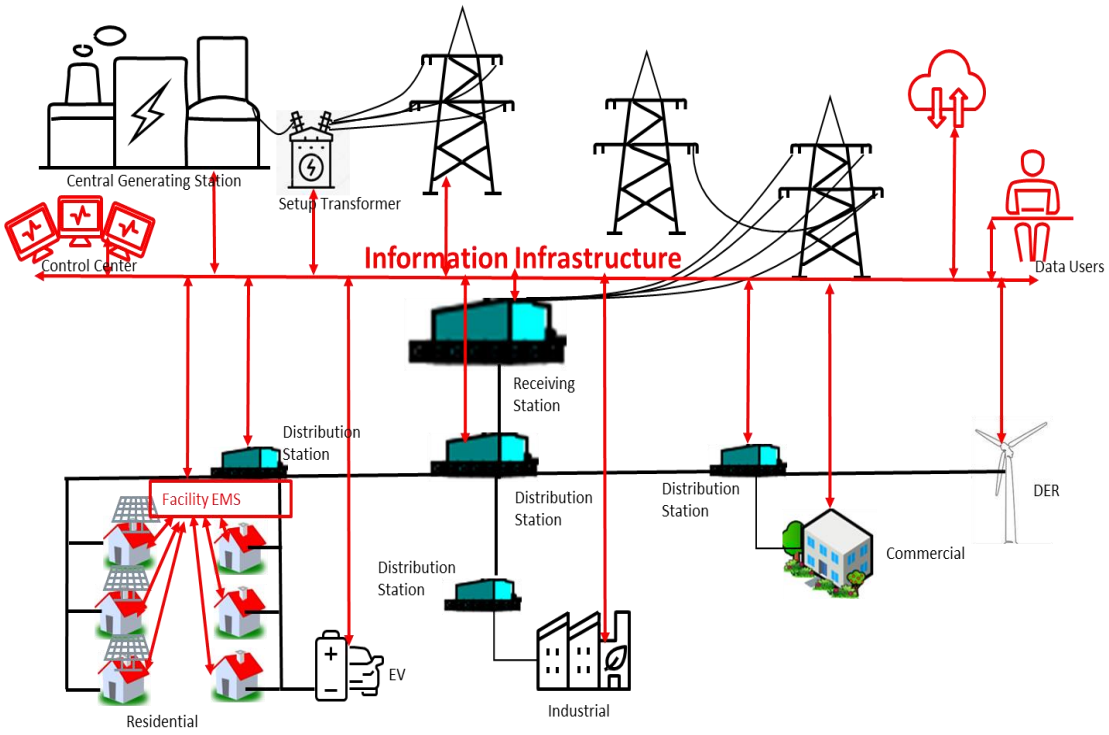

Figure 2. ICT for the existing energy system, IEC cyber security session reference

Furthermore, utilities may have many substations, which are crucial for realizing the PS's efficiency and adaptability strategy. The voltage and current of the energy flowing on incoming power lines are transformed by them. Figure 3 is an example of a single-line diagram from IEC 61850-5 depicting the primary equipment of a distribution substation. The digital substation incorporates IEDs that are interconnected via a communication network in addition to the primary instruments. Figure 4 shows a communication network that was installed to the D2-1 distribution substation that linked all the distributed monitoring, control, and protection IEDs as an example.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

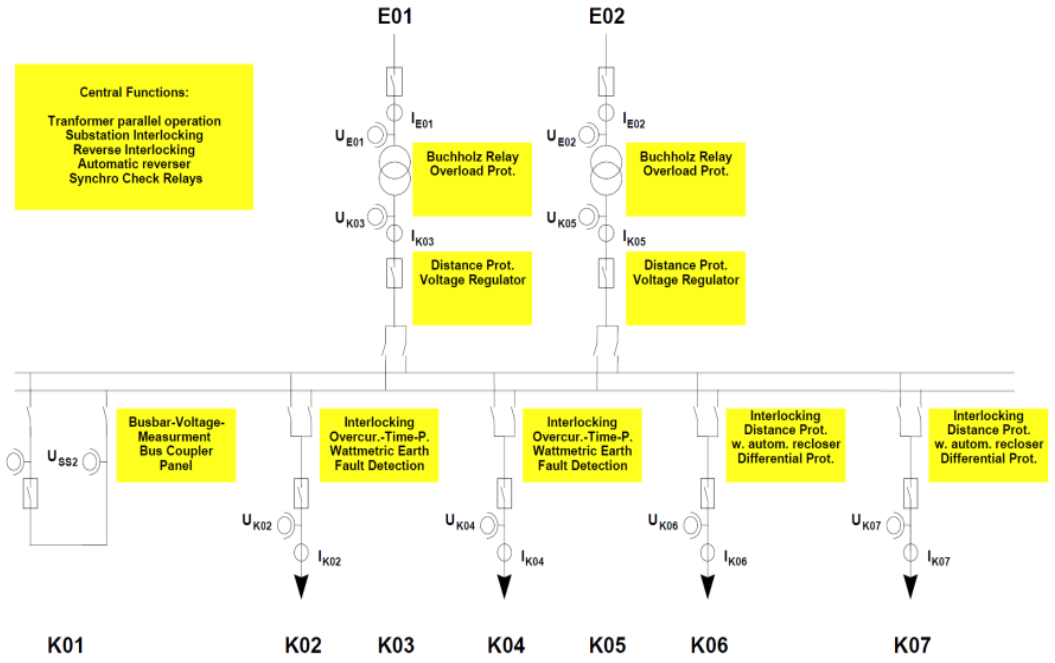

Figure 3. Example substation D2-1 according to IEC 61850. IEC standard

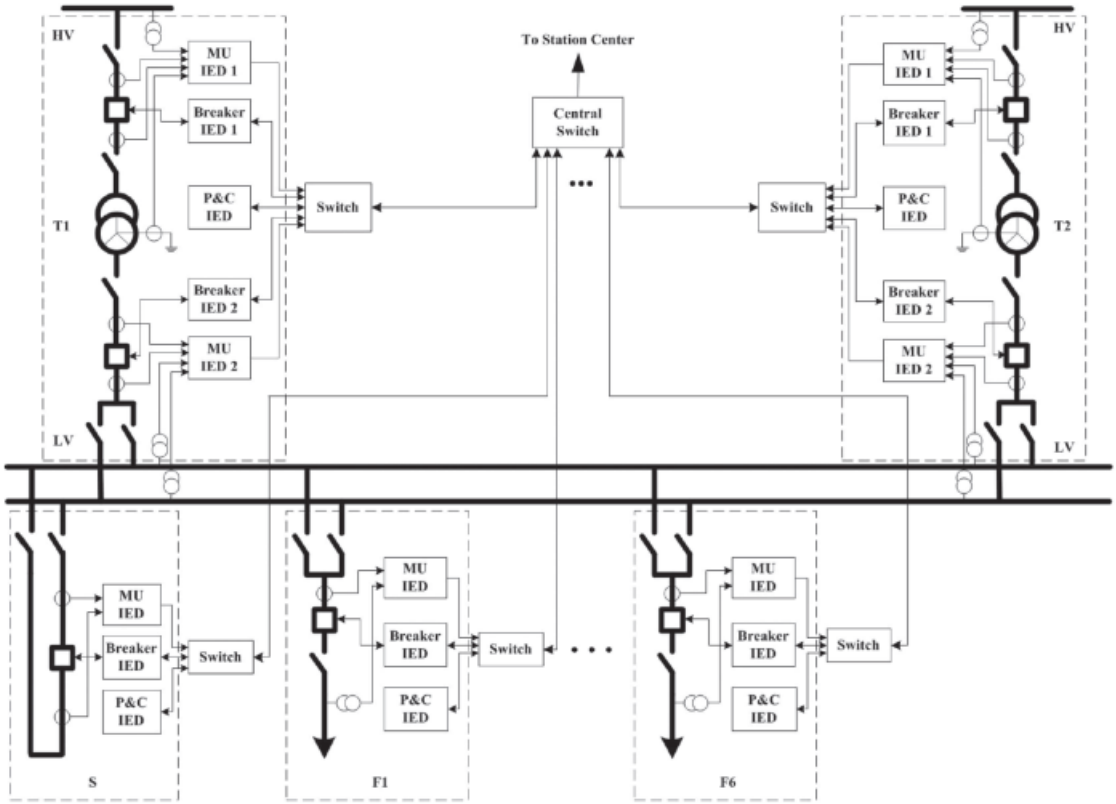

Figure 4. Example substation D2-1 with communication system based on IEC 61850

Therefore, modern power system currently facing number of developments one from many goals is to provide efficient utilization of the state-of-the-art technologies and standards and assuring PS security, resiliency. Security/resiliency, assign to the ability of the power system to except a certain level of risks, develop a cyber-security procedure for the highest risk vector (detection and protection), recover, return to normal operation, and survive attacks disturbances without interrupting services to the clients. As a result, although integrating state-of-the-art technologies and standards into power systems has many advantages, it also increases the risk of cyberattacks on these new digital IEDs, particularly if the system's communication network is accessible remotely via Internet. Furthermore, electricity systems are already exposed to existing risks such as natural disasters, utility staff errors, and deliberate electrical equipment sabotage. At this stage, currently PS is becoming more appealing to hackers, and press headlines highlight multiple incidents of cyber-attacks against Industrial Control Systems (ICS), for instance Ukraine’s power system attacks. In these attacks the Ukraine’s power system is targeted on two different attacks, both of which occurred in 2015 and 2016. The first Attack involved a sophisticated cyber-attack that caused a power outage for more than 200,000 people. Hackers deployed a Trojan that installed and infected one of the remotely linked PC, opened breakers using unauthorized commands, and then used the KillDisk malware to kill the SCADA system and block the communication links, limiting access to the power system and hindering recovery efforts. Whereas, on the second attack, CrashOverride, trojan, was used to carry out the attack. This malware has a wide range of capabilities, including monitoring networks for information, spoofing ICS commands, launching DoS attacks to disrupt communications or turn off devices, and wiping devices altogether. This CrashOverride, Trojan is considered as one off the more sophisticated attack as it is the first malware that targeted the IEC 61850 communication protocols. These attacks, among others, underline the need of safeguarding the PS and the IEC 61850 communication protocols (more information about the IEC 61850 in report TR3.1), given that sophisticated threats have already been developed specifically for these environments.

3 IEC 62351 Standard for ES Cyber Security

IEC 62351, first edition was released by the International Electrotechnical Commission (IEC) in 2007 with the titled "Power systems management and associated information exchange - Data and communications security,". The standard aims to strengthen cybersecurity in PS control operations, as the scope of IEC 61850 does not include cybersecurity. In addition, there is an ever-increasing threat against critical infrastructures and protecting of the PS from the increasing threats faces substantial challenges both institutional and technical from the following major trends:

- Greater integration with a range of corporate organizations is required.
- Expanded utilize of open systems-based frameworks that will create the future power system
- The necessity for existing or "legacy" systems to be properly integrated with future systems
- Integrated distributed computing systems are becoming more sophisticated and complicated.
- Threats are getting more sophisticated, and they are being launched by hostile communities, that may be supported by organizations or nations.

As a result of the challenges, the IEC is being prompted to draft a new cybersecurity standard. This standard's major purpose is to “Undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues.” [62351-1]

The IEC 62351 is divided into several parts, as below.

- IEC TS 62351-1 Communication network and system security - Introduction to security issues: it covers cyberattacks and how the standard is supposed to address them
- IEC TS 62351-2 glossary of terms

- IEC 62351-3 Communication network and system security - Profiles including TCP/IP: Its goal is to protect TCP, which is utilized by MMS and other application protocols.
- IEC 62351-4 Data and communication security - Profiles including MMS and derivatives: as it aims to secure the MMS protocol
- IEC TS 62351-5 Security for IEC 60870-5 and derivatives: as it concerned with IEC 60870-5 standard communication protocols
- IEC 62351-6 Security for IEC 61850: it concerned with the IEC 61850 protocols such as GOOSE, SV, and IEC 61850 MMS protection.
- IEC 62351-7 Network and System Management (NSM) data object models: focuses on end-to-end security monitoring of the Network and System Management (NSM)
- IEC 62351-8 Role-based access control for power system management: its role is based access control for power system management (RBAC) focus on access and control human and automated agent access to data objects in power systems.
- IEC 62351-9 Cyber security key management for power system equipment: Specifies how to use safety-critical parameters such as passwords and encryption keys correctly and safely.
- IEC TR 62351-10 Security architecture guidelines: security architectures for the entire IT infrastructure are explained. Identifying essential communication architectural nodes, such as the substation control center and substation automation
- IEC 62351-11 Security for XML documents: The original XML content is embedded into an XML container. XML data access control and date of issue X.509 signature for XML data authenticity Encryption of data is an option.
- IEC TR 62351-12 Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems: It addresses resilience needs with the purpose of improving the safety, dependability, power quality, and other operational elements of DER systems with high penetrations,

based on the concepts and hierarchical design outlined in the Smart Grid interoperability guidelines.

- IEC TR 62351-13 Guidelines on security topics to be covered in standards and specifications: provides guidelines on what security topics should be included in standards and specifications. These guidelines should be utilized as a checklist for the mix of standards and specifications used in system implementations.
- IEC TR 62351-90-1 Guidelines for handling role-based access control in power systems; role-based access control (RBAC), as described in IEC TS 62351-8, is used to control the access of users and automated agents to data objects in power systems. The primary goal of this document is to create a standardized way for defining and engineering bespoke roles, as well as the role-to-right mappings and infrastructure support required to use these custom roles in power systems.
- IEC TR 62351-90-2 Deep packet inspection of encrypted communications: It focuses on the illustration, needs and requirement to perform Deep Packet Inspection (DPI) on IEC 62351-secured communication channels utilizing state-of-the-art DPI techniques that may be used to several types of channels and set their boundaries.
- IEC TR 62351-90-3 Guidelines for network and system management: provides guidelines for effectively managing both IT and OT data in terms of monitoring, classification, and correlations to derive any useful conclusions about the state of the power system. Additionally, to provide a broad monitoring framework based on the analysis of data received from various IT and OT systems via network management, traffic inspection, system activity readings, these data analysis should include filtering and correlation methods.
- IEC TS 62351-100-1 Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7: presents data and communication security test cases for various communication and control elements. The purpose is to promote interoperability by establishing a common technique for testing protocol implementations to ensure that a device meets the standard's requirements.

- IEC TS 62351-100-3 Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP: describes test cases of data and communication security. The purpose is to verify that a device fulfils the requirement of IEC 62351-3.

On this study we will focusing on the parts IEC 62351 (1, 4, and 6) that are relevant to IEC 61850 communication protocols.

3.1 IEC TS 62351-1 Communication network and system security - Introduction to security issues

IEC TS 62351-1 focuses, among other things, about the different PS potential cyberattacks and how the standard is designed to solve them as an introduction to security challenges. Figure 5 depicts some of the potential PS cyber-attacks, demonstrating how the same sort of attack can frequently be found in other cyber threats. Because of this network of potential attacks, there is no single way to achieve a certain security requirement: each of the sorts of attacks that pose a specific threat must be considered. In addition, a "chain of attacks," in which a series of attacks, involving multiple assets and occurring over time, can also be used to realize a given threat.

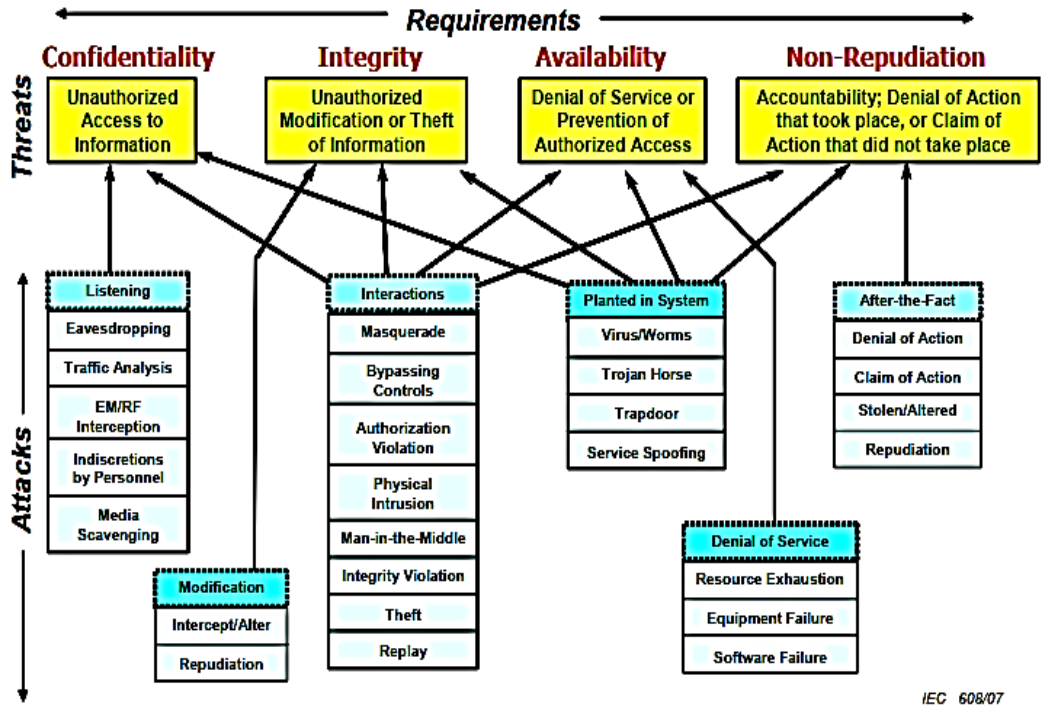

Figure 5. Security requirements, threats, and attacks

Part 1 also defined and classified cyber security into 4 groups, each of which necessitates security measures to achieve “end-to-end” security; securing only one category is usually insufficient. As a result, these security measures should be carefully integrated with one another and applied as a bulk of cyber security strategy to minimize inadvertent vulnerabilities. Figure 6 depicts the security categories, as well as the typical threats and the available countermeasures that must be used.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

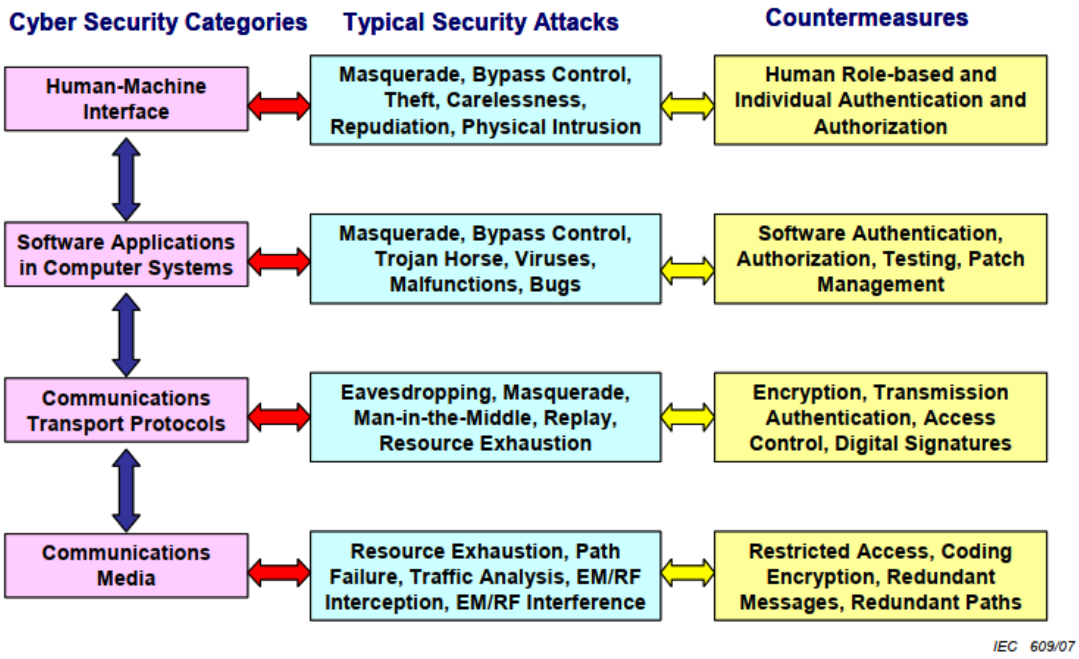

Figure 6. Security categories, typical attacks, and common countermeasures

At this stage, it is important to remember that not all security countermeasures are required or preferred for all systems all the time. This would be a massive overkill that would render the system unusable or extremely slow. As a result, the first step is to determine which countermeasures are appropriate for demands. Figure 7 depicts a broad overview of all countermeasures, for the defined four cyber security require-ments.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

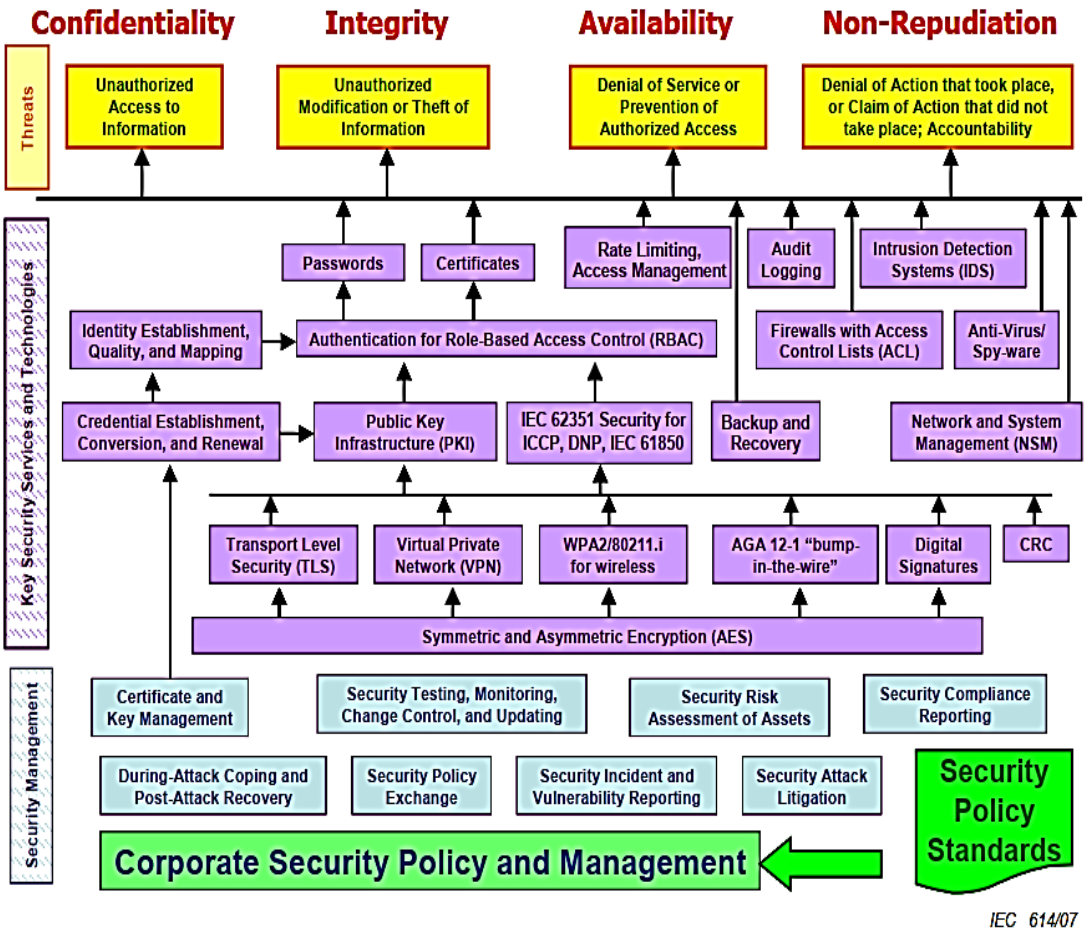

Figure 7. Security requirements, threats, countermeasures, and management in general.

Along with the overall security vision Figure 7 shows also the four security requirements indicated on top and the basic security threats shown below each requirement. The essential security services and technologies used to combat these risks are displayed in the boxes directly below the threats, with arrows indicating which technologies and services support the security measures above them. Security management and security policies, which form the foundation for all security measures, are at the bottom, below the security services and technologies.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

3.1.1 Objective of IEC 62351-1

In the past, security requirements were analyzed using both enterprise-based and technology/threat-based analysis methodologies. Within the first method it will begin by applying a set of security measures to the entire enterprise. While the second method applying a set of technologies to all systems. Both strategies have obvious drawbacks. Since for instance, the enterprise-based method an enterprise may encompass more than one business entity and is continuously evolving and changing where a single set of security policies and technologies cannot be deployed. Whereas the drawbacks for the Technology/Threat-based analysis that presume a static security measure based on today's technology may limit future adoption of more advanced security technologies. As a result, any security choice necessitates a great deal of coordination and tends to break down the problem into smaller areas of security analysis and management. Depending on the use cases three alternative approaches have been utilized. These are.

- Physical security perimeter: physical access to critical infrastructure is forbidden/controlled for instance e.g., cameras, walls, fences etc., these entities can be used for physically protecting assets.
- Electronic security perimeter: the logical boundaries applied at the edge of the connected critical infrastructure network to which access is restricted. This perimeter can be used to implement cyber-security measures.
- Security domain: define the areas within the enterprise with the same security perspective/requirements or at least under the control of the same entity. The security domain concept allows a set of resources to be managed independently.

3.1.2 Security Requirement/Measures and Impact on Power System operations

The modern power system is made up of electrical and cyber systems. Based on IT and OT features, these systems are integrated and connected to form a smart power system. In comparison to most other systems, the IT and OT technologies used in power systems necessitate distinct concentrations and security requirements. Since a result,

power system operations provide a unique set of security issues, as they are a combination of IT and OT, with OT being the primary mode of operation. This power system operation feature acquires many strict performance and reliability criteria that are less stringent in other sectors. Most current security measures are intended to protect IT systems from hackers who are connected to the worldwide network (Internet). The IT of the worldwide network environment is vastly different from the OT of power system operating environments. Thus, there is often a lack of awareness of security requirements and the potential influence of security measures on power system. For instance

- Anticipating an authorized users from accessing the SCDA to control substation seem to have more consequences than anticipating an authorized client from accessing his bank account. In this manner, the danger of denial-of-service in critical power system entities is distant more critical than other systems (e.g., power system control cannot be turned off or restarted as in other systems).
- Resources in power system entities e.g., communication channels, IEDs memory, CPU computing etc., are often limited which is not suitable for some of the overhead needed for certain security measures, such as encryption and key exchanges.
- Power system organizations are typically dispersed across wide geographical areas where communication infrastructure may be lacking. As a result, Key management, certificate revocation, and other security procedures become more complex to apply.
- Because many systems are linked through multi-drop communication channels, traditional industrial network security procedures are ineffective.
- Wireless communication's benefits and implementation are extensively utilized in different sectors; nevertheless, in power systems and based on the electromagnetic noisy environments, utilities must be incredibly careful where and for what purposes they use these wireless technologies. In addition, many wireless networks have security features that might raise the overhead.

.

3.1.3 Cyber Security Process

Cyber security for power systems accomplished by selecting a solution based on current technology and statically implementing it as is may prevent future adoption of more advanced security solutions. Thus IEC 62351 defined end-to-end PS cyber security as a dynamic continuous process that never stands still. To assist security processes, keep up with the demands that will be placed on the systems, ongoing work and education is required. Corporate security policies/security infrastructure will continue to evolve and compete with hostile organizations in terms of security. There are no communication-connected systems that are 100% secure by definition. Residual risk will always exist and must be considered and handled. As a result, continual awareness, and monitoring, as well as response to evolve/changes in the systems environment, are required to ensure security. Figure 8 depicts the IEC 62351 specified end-to-end PS cyber security process in continuous cycle, which consists of five high-level processes. The continuous cycle of the process is circular by nature, and there is a clear order to the process.

Figure 8. Overall security process continuous cycle, IEC standard

- Security Assessment- is the process of determining whether or not assets are secure, and the needed security resources, requirements based on the likelihood of an attack, the liability associated with successful attacks, and the costs of mitigating the risks and liabilities. The security needs analysis suggestions lead to the development of security policies, the acquisition of security-related products and services, and the execution of security processes. Periodic re-assessment is necessary to continuously evaluate the technological and political changes that may require. The re-assessment timeframe must be specified in policy for periodic review.
- Security Policy- The process of establishing policies for controlling, implementing, and deploying security inside a Security Domain is known as security policy generation. The security assessment's suggestions are evaluated, and procedures are created to guarantee that the recommendations are executed and maintained throughout time. The security strategy should be enshrined in a security plan that lays out the specific security measures to be implemented, the timeline for doing so, and the review mechanism for assessing the outcomes and revising the plan.
- Security Deployment- Purchase, installation, and testing of security products and services, as well as the execution of security policies and procedures defined throughout the security policy process, make up security deployment. Management processes that allow for intrusion detection and audit capabilities, should be implemented as part of the deployment component of the Security Policies.
- Security Training- Security threats, security technology, and corporate and regulatory regulations that affect security all require ongoing training. Security risks and technology are always adapting, need ongoing analysis and staff training to create and maintain the appropriate security architecture.
- Security Audit (monitoring) - Ultimately, every system that lacks complete 100% security must be monitored. Security auditing is the process of detecting security assaults, detecting security breaches, and evaluating the established security

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

infrastructure's performance. The idea of an audit, on the other hand, is often applied to post-event/incursion activities. As with active security infrastructures, the Security Domain concept necessitates continuous monitoring. As a result, the auditing procedure must be improved.

3.2 IEC 62351-4 Data and communication security - Profiles including MMS and derivatives

IEC 62351-4 standard, which was first published in 2007, has been withdrawn, and the part IEC 62351-4, 2018 standard is a developed and expanded version of the previous one and replace it. IEC 62351-4, 2018 expand the scope of previous version to support applications at both the transport and application layers. Since in IEC 62351-4, 2007 previous version primarily had a limited support at the application layer for authentication during handshake for the Manufacturing Message Specification (MMS) based applications.

3.2.1 IEC 62351-4 objective

IEC 62351-4, 2018 proposes security for the A-Profile (i.e., application-level security) as well as for the transport T-Profile based TCP/IP- by means of represents of a set of mandatory and optional security specifications to be applied to enhance the security for OSI different layers communication protocols. Figure 9 presents the OSI stuck model and different layers protocols.

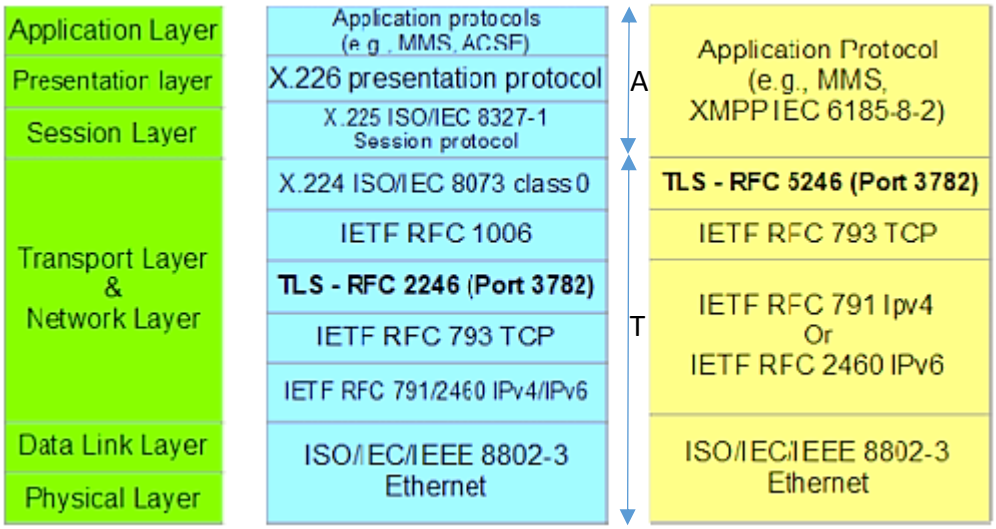

Figure 9. OSI Protocol stack model for compatible and native T-security specifications for MMS messages.

The IEC 62351-4 2018, enhanced integrity and authentication specification/requirements are developed to support the handshake and data transfer phases. It also provides security end-to-end (E2E) with zero or more intermediary entities, as well as shared key management and data transfer encryption at the application layer. Finally, it supports application protocols that are implemented using other protocol stacks, such as e.g., an internet protocol suite. This protection is now extended to application protocols that use XML encoding.

- A-Profile Application Profile Security. For the three upper layers OSI reference model security specification, entities peer-to-peer should be authenticated through certificate based during association establishment. In the association request, a device will provide an X.509 certificate, as well as a timestamp and a signature on the timestamp using the specified certificate. If the timestamp does not deviate by more than 10 minutes from the local time, the receiving device will check it and accept it. Furthermore, a device will not receive a message with a timestamp that has been viewed within the last 10 minutes.
- T-Profile Transport Profile Security. For the four lower layers OSI reference model security transport layer security (TLS) e.g., transport control protocol (TCP). The standard describes how to use different TCP port for secure connections between Transport layer TCP protocol and the ISO Transport Service. Further defined are the TLS cipher suites that should be supported and how to handle certificate revocation.

Summery for security communication aspects is discussed and described in Table 1., based on the A-profile and T-profile constraint.

Table 1. Relationship between security and security measure combinations

Application Security	Application Profile	None	A-Security Profile	E2E security without encryption	E2E security without encryption	E2E security with encryption	E2E security with encryption
Transport Security	none	TLS	TLS	none	TLS	none	TLS
Note	Note1	Note2		Note3		Note4	

For the application of the T-security, TLS is expected to be used as specified in 6 3 for the OSI operational environment. For other environments, TLS usage is outside the scope of this document and specified by the referencing standard.

Note l: Using the A-security profile alone without TLS results in a non-secure system

Note 2: Using TLS with or without the A-security profile gives a reasonable security assuming that all other security measures are observed, including use of TLS cipher suits and that the communication is peer-to-peer without intermediate entities. in addition to the authentication provided by TLS, the use of the A-security profile allows for authentication at the application layer of application entities

Note 3: Using E2E security without encryption with or without TLS provides for mutual authentication and end-to-end integrity protection and thus reasonable security providing that confidentiality is not required and that other security measures are observed. Use of TLS fulfils confidentiality (encryption) an integrity protection on transport layer hops should the E2E security be compromised

Note 4: As for note 3 with addition of end-to-end encryption (confidentiality).

3.2.2 IEC 62351-4 Compatibility and Native modes

The IEC 62351-4 standard provides two mutually incompatible modes of operation, namely, compatibility and native modes.

- The compatibility mode is a mode of operation that is compatible with both the IEC TS 62351-4 specified A-profile and T-profile communication profiles. According to the T-profile specifications a set of cipher suits is used that claim conformance to IEC TS 62351-4. This cipher suits are specified and shall support the TLS_RSA_WITH_AES_128_CBC SHA2S6 as a minimum. In addition, the standard defined a set of cipher suite (they originate from different IETF RFC 2246) and it is recommended be considered for use and it is presented in Annex A Table 1. Whereas the application security specification for A-profile is given by MMS abstract syntax which is defined in 24.11 of ISO 9506:2003
- The native mode is a mode of operation that recognized as the major addition of the IEC 62351-4 standard. It offers the extended support for TLS security as specified as in TLS_RSA_WITH_AES_128_CBC SHA2S6 as a minimum. In addi-

tion, the standard defined a set of cipher suite (they originate from different IETF RFC 5246) and it is recommended be considered for use and it is presented in Annex A Table 2. Furthermore, it allows for end-to-end security between two application entities with zero or more intermediate application entities as we discussed within next sections.

IEC TS 62351-4 specified for implementing and using port 3782 instead of the usual port 102 for the TLS transport layer connection. Hence, the secure MMS messages use the port 3782 at the transport layer as shown in Figure 10.

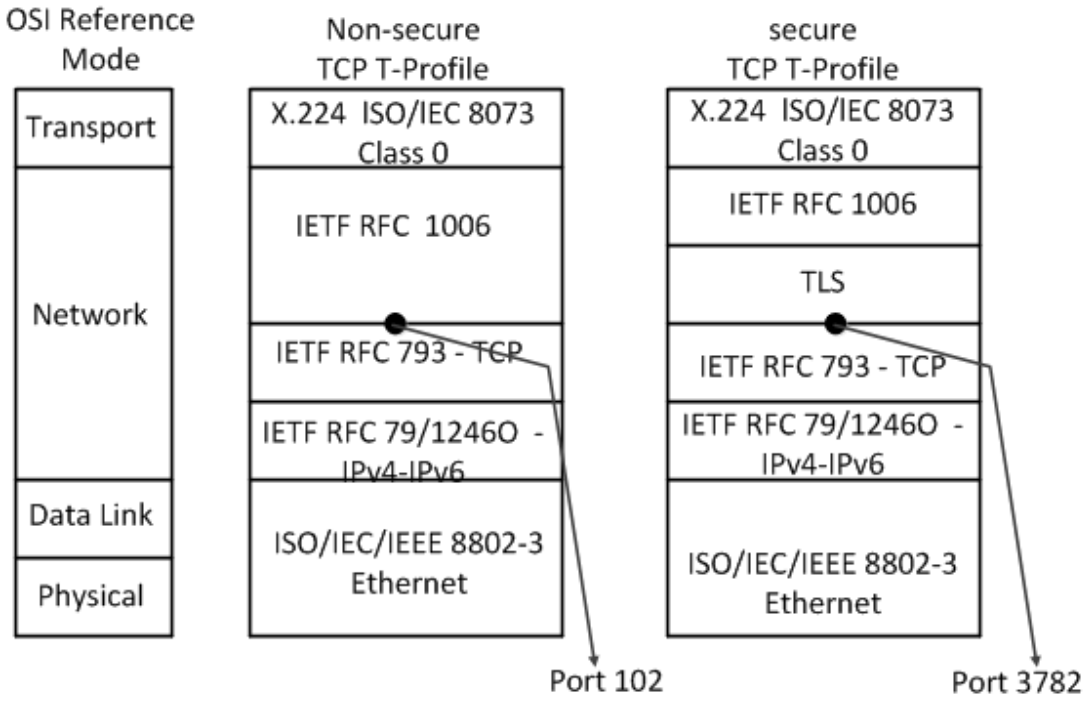

Figure 10. T-profiles without and with TLS protection

3.2.3 End-to-End Application Security Model

In diverse operating environments, E2E security standards at the application layer are utilized. It describes how to safeguard different application protocols by using peer authentication, message integrity, and confidentiality throughout both the association setup and data transfer phases as seen in Figure 11.

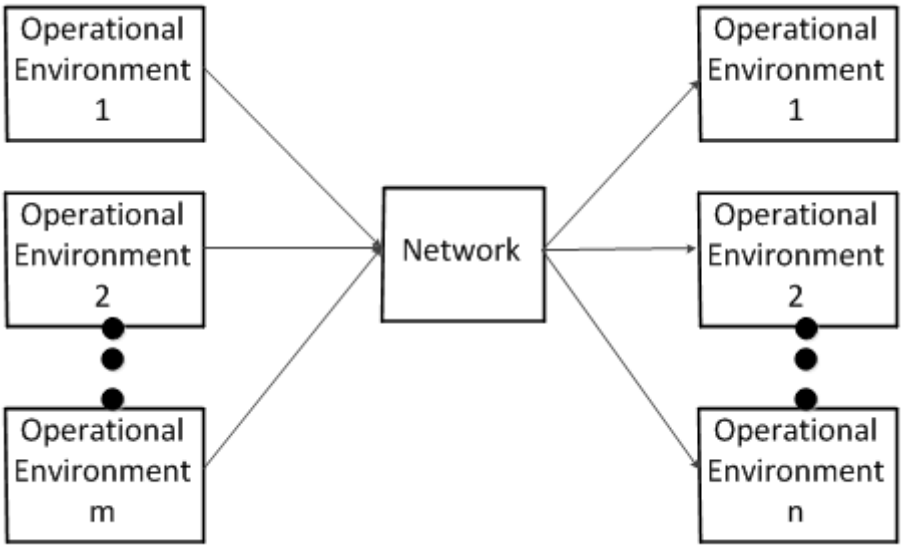

Figure 11. E2E Security building blocks

To meet the security criteria in the E2E security specification, public key signature techniques and symmetric encryption algorithms are used. Without TLS security at the transport profile, the E2E security specifications are completely implemented, resulting in a reasonably secure system. When E2E security is combined with TLS security, the system becomes secure as presented in Table 1.

The OSI and eXtensible Messaging and Presence Protocol (XMPP) operating contexts are considered in IEC TS 62351-4, with more environments included in future editions. The basic concept of the E2E building block security is to maintain it independent of the operating environment and the protected protocol. As illustrated in Figure 12, this method allows the basic E2E security definition to be improved as needed without compromising the protected protocol specification.

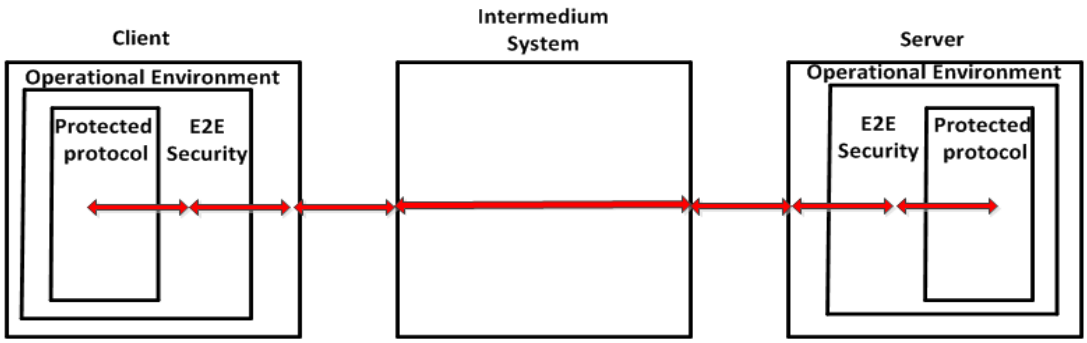

Figure 12. Relationship between environment, E2E-security, and protected protocol

The mutual links between the operating environments, E2E security, and the protected application protocol are also shown in Figure 12. Furthermore, the protected application is seen as being embedded in E2E security, which is embedded in the operating environment as well. According to the model shown in Figure 12 and reflected to the E2E security concept an application protocol data unit (APDU) is called a protected PDU (PrPDU), and within the E2E security is called (SecPDU) in which both they hold a protection protocol and security protocol control information, respectively. The APDU transporting a SecPDU is called the Environment PDU (EnvPDU). In addition to the holding SecPDU, it holds protocol control information necessary for the overall operation, as illustrated in Figure 13.

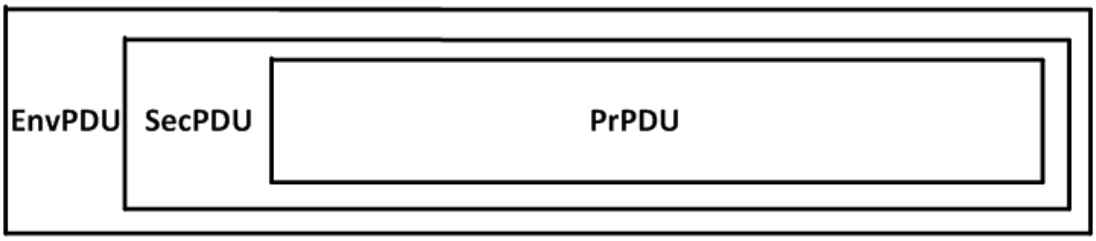

Figure 13. Relationships between ApDUs

The IEC TS 62351-4 specifies the E2E general model and separates between what is included within the standard and what is included in the application standard for the protected protocol in Figure 14.

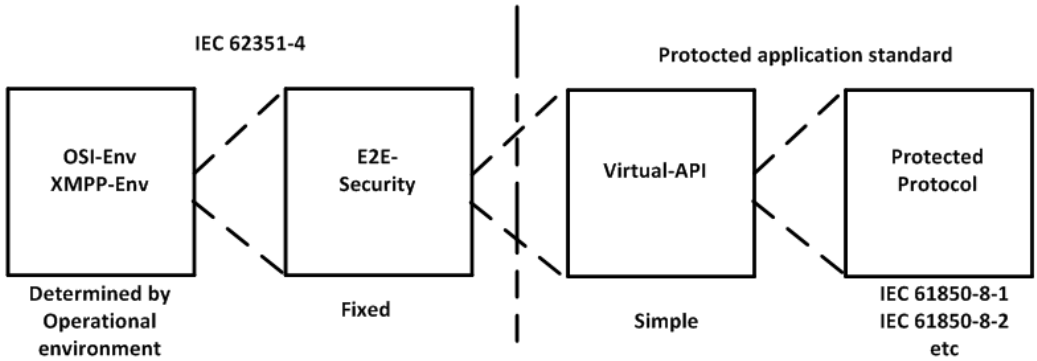

Figure 14. The scope of E2E-security specification

Because the mapping of secPDUs to EnvPDUs is independent of the protected protocol. It is possible to map several protected protocols to the same operating environment and no changes is required to the E2E security specification along with each particular

implemented protected protocol. To map the protected protocol's entry PrPDU to SecPDU, a basic interface specification known as virtual-APl is used. This mapping must be included in the protected protocol's application standard. The protocol that is being protected is unaffected. The virtual-APl can be applied as an ASN.1 module that supports either BER or EXTENDED-XER (XML) encoding, or as a W3C XSD that supports XML encoding.

3.2.4 E2E application security Association Managements

For the MMS message exchange security connection takes place between two entities. Data message exchange accrues in two phases, i.e., handshake phase and data transfer phase were through some intermediate application entities as illustrated in Figure 15.

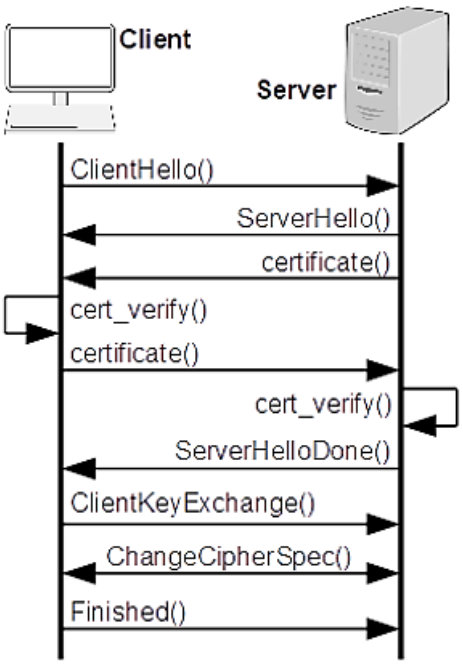

Figure 15. Message exchanges for TLS establishment for client and server.

The handshake phase is when the TLS connection is issued and negotiated; to begin a new association, the client must send an instance of the *HandshakeReq* SecPDU and has the following components

- The *pp* component defines the application's identity, which will be secured via E2E security. It might be the name of the protected protocol's standard, such as IEC 61850-8-2. The precise value to be utilized must be specified in the protected protocol definition.

- The *tbs* component that includes the *tokenl* and *applData* the first shall hold the *ClearTokenl* data type and the second shall hold an instance of the appropriate PrPDU
- The *sign* components shall hold â *signature* data value

Screenshot for the handshakeReq instance is illustrated in Figure 16.

```
HandshakeReq::= SEQUENCE {
  pp        NMTOKEN,
  tbs       SEQUENCE {
    token1    ClearToken1,
    applData  ApplData OPTIONAL,
    ... },
  sign      Signature }

NMTOKEN::= UTF8String (FROM(
  {0, 0, 0, 32} .. {0, 0, 215, 255} |
  {0, 0, 224, 0} .. {0, 0, 255, 253} |
  {0, 1, 0, 0} .. {0, 16, 255, 253}))
```

Figure 16. HandshakeReq instance

In case the server will accept the association request it needs to issue an acceptance instance of the *HandshakeAcc* SecPDU and it has the following components

- The *tokenl* component shall hold an instance of the *ctearTokenl* data type
- The *applData* component, shall hold the appropriate PrPDU instance for the protected protocol
- The component *Initiate-ResponsePDU* shall hold the instance of the data type
- The *sign* component shall hold a *Signature* data value, in which the signature over the content of the *tbs* component

Screenshot for the HandshakeAcc instance is illustrated in Figure 17.

```
HandshakeAcc::= SEQUENCE {
  tbs SEQUENCE {
    token1    ClearToken1,
    applData  ApplData OPTIONAL,
    ... },
  sign      Signature }
```

Figure 17. HandshakeAcc instance

When an association is effectively formed, the data transfer step begins. The data transmission phase is then followed by the actual data transmission as determined by the protected protocol. The data might be sent unencrypted or encrypted.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

3.3 IEC TS 62351-6 Security for IEC 61850

IEC TS 62351-6, named "Securing for IEC 61850," is a standard that focuses on securing all the protocols contained in the IEC 61850 standards by describing messages, processes, and algorithms. The following are the protocols covered by the IEC TS 62351-6 standard.

- IEC 61850-8-1: Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (lSO/lEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
- IEC 61850-9-2: Communication networks and systems in substations - Part 9-2: Specific Communication Service Mapping (SCSM) - Sampled values over ISO/lEC 8802-3
- IEC 61850-6: Communication networks and systems in substations - Part 6: Configuration description language for communication in electrical substations related to lEDs

The provisions specified in section 3.2 shall be utilized without any further changes for protocols in IEC 61850 that employ TCP/IP and MMS.

3.3.1 IEC TS 62351-6 objective

IEC TS 62351-6 proposes to IEC 61850 protocols security extensions (our concern GOOSE and SV). Because encryption is not recommended for GOOSE and SV applications that need less than 4 ms response time, the particular security risks addressed in this standard include "unauthorized modification of information through message level authentication of the messages." The IEC TS 62351-6 standard, provides security enhancements using

- IEC 61850 GOOSE and SV protocol data unit PDUs have been extended. This adds a security-relevant information field to the PDU. The extension contains a signed hash of the PDU, which is used to authenticate it.
- Adding extensions that allows to include certificate definitions within the configuration of the Substation Configuration Language (SCL) files.

3.3.2 IEC TS 62351-6 Performance issues

Before implementing any security mechanisms, to any communication infrastructure they should carefully examine the performance implications. This is especially true when it comes to real-time traffic, or systems with restricted requirements. All three limitations apply when securing energy systems using IEC 61850 communication protocol.

- IEDs based on ES protection and control use are usually have limited computing capacity, and only a (small) part of it may be dedicated to functions other than what designed for. Furthermore, replacing or upgrading for long lifetime hardware is a complicated process. As a result, security solutions for embedded devices should not necessitate substantial hardware modifications.
- Both GOOSE and SV have strict real-time restrictions that should be considered when implementing any security procedures— GOOSE has a 3ms reaction time while Sampled Values has sampling rates up to 12 kHz.
- To ensure confidentiality for information exchanges, the communication path selection procedure (e.g., the fact that GOOSE and SMV are meant to be confined to a logical substation LAN) would be employed.

The standard, on the other hand, advises that encryption be used whenever possible. It hides the contents of data from passive attackers listening in on traffic, preventing data theft and making other attacks more difficult.

3.3.3 GOOSE and SV Extended PDU

IEC TS 62351-6 adds new fields to GOOSE and SV PDUs; *AuthenticationValue* to carry Rivest-Shamir-Adleman encryption (RSA) digital signature: the input is a SHA-256 hash of PDU's contents; and *timestamp* to represent the creation time of the PDU (only used for SV). Figure 18 shows the basic structure of an enhanced PDU implementation that claims compliance to this standard for GOOSE and SV.

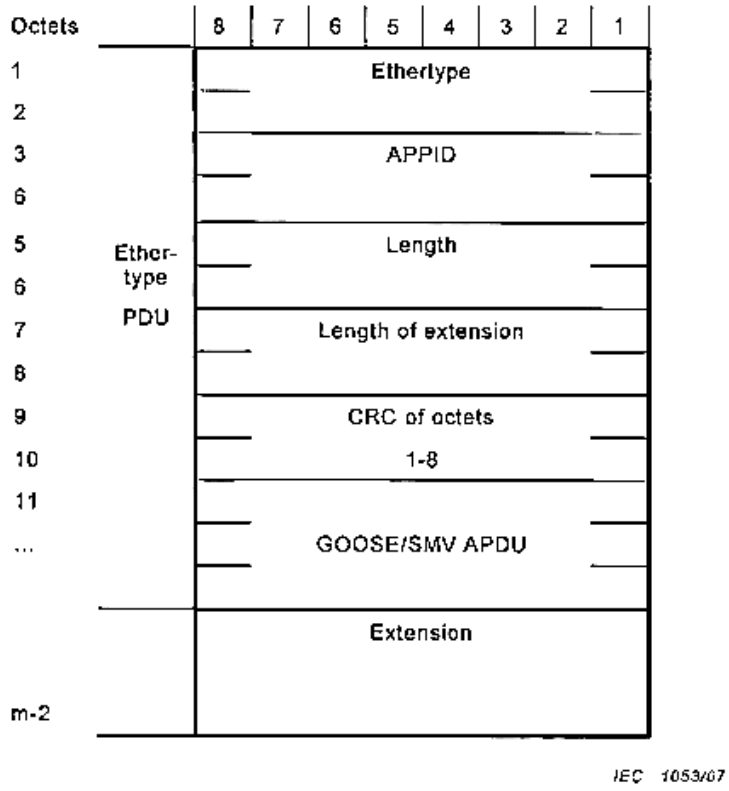

Figure 18. GOOSE and SV extended PDU general format

The requirements of this specification are as follows:

- Reserved1 field: The first octet of the extension part (Reserved1) should specify the value of octets being used by the extension octets. The range of valid values is zero (O) to 255. A value of zero(O) indicates that there are no extension octets. Whereas the Reserved1 field's second octet will be set aside for future usage.
- Reserved2 field: According to ISO/IEC 13239, the Reserved2 field must include a 16-bit cyclic redundancy check (CRC) (ISO HDLC). The CRC must be computed across Octets l-8 of the Extended PDU's VLAN information. If the Extension Length is a non-zero value, the CRC must be present.

3.3.4 Requirements on Server

The algorithm must be carried out as stated by the servers and must add a valid AuthenticationValue to every PDU. AuthenticationValue must not be present in the Extension octets' if the server does not provide it. Implementations that use the Authentica-

tionValue must also supply a public X,509 certificate for installation on the receiving clients.

3.3.5 Requirements on Clients

The subscribing client must be able to reference the source MAC Address to the AES 128-bit public Key given by the server' on a local level. Client can then validate the signature to confirm the validity of the PDU, as only the actual publisher has access to the private key necessary to create it. As a result of this modification, attackers will no longer be able to spoof or alter packets, as both require the generation of a valid signature.

3.3.6 Replay Protection for GOOSE

The security extensions will be used to supplement and guard against GOOSE replay. In addition, the following should be utilized.

- At the beginning, the process of confirming the AuthenticationValue must take place before any further processing.
- The skew period, which does not exist in standard GOOSE, is used to limit the amount of time that a GOOSE PDU is deemed valid. The client should determine what time zone is and keep track of it. It should not process a GOOSE with a skew of longer than 2 minutes. The skew period must be configurable, maximum-minimum range with a 10 second. Skew filtering significantly reduces replay attacks by preventing the usage of PDUs older than the skew period.
- Only for StNum changes should the client use skew filtering.
- Normally a GOOSE message with a higher stNum implies that it was sent more recently. The client should maintain note of the received stNum for the publishing server; if the message is received with a lower value for stNum and no rollover or timeallowedtolive timeout, it should be discarded. This behavior deals with PDUs that come out-of-order, preventing the subscriber from reacting to previous events and causing problems. It also guards against replay attacks: because stNum values should only ever rise between successive PDUs, previous

recorded PDUs have a lower stNum than the most recent one. As a result, when recorded PDUs are replayed, the subscriber rejects them.

- The stNum is set back to 0, in two cases, case one if a message timeout occurs or case two, stNum rolls-over (the 32-bit value overflows, meaning it exceeds its maximum of (2^32 − 1))
- The starting stNum shall be zero (0) at initialization/power-up.

3.3.7 Replay Protection for SV

The MAC security extensions shall be used to supplement and guard against SV tampering/replay. In addition, IEC TS 62351-6 introduces a *timestamp* field to be contained in every SV packet to represent the creation time of the PDU. Since SV PDUs do not include a timestamp field, despite IEC 61850-7-2 mentioning that timestamps should be present. Along with the security extensions implementations, the following processing should be utilized.

- At the beginning, the process of confirming the AuthenticationValue must take place before any further processing.
- Skew filtering operates in a similar fashion to GOOSE, but with a few significant changes. The skew period used by SV is set to 2 minutes, rather than being configurable like that used by GOOSE. Furthermore, all SV PDUs are filtered. To determine if an SV PDU is within the skew period, the client checks the PDU's timestamp with the local time. An SV with a timestamp that is more than 2 minutes uncoordinated, the client should not proceed the incoming PDUs.
- Discarding of lower smpCnt. For the publishing server SV PDU, the client should record and track the received smpCnt. PDUs with a greater smpCnt are usually newer. If the client receives a lower value for sqNum and there has been no rollover, the client should discard incoming PDUs.
- The stNum is set back to 0, in case, if a message timeout occurs
- The sqNum is set back to 0, if sqNum rolls-over (the 32-bit value overflows, meaning it exceeds its maximum of (2^32 − 1)).
- The starting sqNum shall be zero (0) at initialization/power-up.

3.3.8 Substation configuration language (SCL)

3.3.8.1 SCL certificate extension structure

IEC TS 62351-6 standard specifies the extension to substation configuration language (SCL) structure to allow definition of certificates that are to be used by including the following. Figure 19 illustrates the SCL extensions certificates instances,

```
<xs:complexType name="tCertificate">
        <xs:complexContent>
            <xs:extension base="tNaming">
            <xs:sequence>
                    <xs:element name="XferNumber" type="xs:unsignedInt" minOccurs="0"
maxOccurs="1" />
                    <xs:element name="SerialNumber" type="xs:normalizedString" minOccurs="1"
maxOccurs="1" />
                    <xs:element name="Subject" type="tcert" minOccurs="1" maxOccurs="1"/>
                    <xs:element name="IssuerName" type="tcert" minOccurs="1" maxOccurs="1"/>
            </xs:sequence>
        </xs:complexContent>
</xs:complexType>

<xs:complexType name="tcert">
        <xs:complexContent>
            <xs:extension base="tNaming">
            <xs:sequence>
                    <xs:element name="CommonName" type="xs:normalizedString" minOccurs="1"
maxOccurs="1" >
                    <xs:element name="IDHeirarchy" type="xs:normalizedString" minOccurs="1" />
            </xs:sequence>
        </xs:complexContent>                                                    IEC 1054/07
</xs:complexType>
```

Figure 19. SCL certificate extensions instances

Where the definitions of extension attributes are as follows: *"XferNumber"* This attribute is used to indicate the certificate's number to the transmitting IED. If the certificate is to be used for GOOSE or SV, it must have an attribute value. 'Values from 0 to 7' are acceptable. "*SerialNumber*" the serial number value of the certificate is holding in this attribute. "Subject" this attribute shall include the certificate's identifying hierarchy as it appears in the certificate for the certificate's Subject, and it is complex attribute type. "*IssuerName"* shall hold the identifying hierarchy of the certificate as present within the certificate for the *IssuerName* in the certificate and it is complex attribute type. "*CommonName*" This attribute shall contain the value of the *commonName* as found within the certificate.

3.3.8.2 Specification of Access Point security usage

For implementations claiming compliance to this standard and support for the necessary security, the AccessPoint SCL definition will be expanded to include GOOSESecurity and SVSecurity. Figure 20 illustrates the extension AccessPoint SCL definition.

```
<xs:complexType name="tAccessPoint">
  <xs:complexContent>
    <xs:extension base="tNaming">
      <xs:choice minOccurs="0">
        <xs:element name="Server" type="tServer">
          <xs:unique name="uniqueAssociationInServer">
            <xs:selector xpath="./scl:Association"/>
            <xs:field xpath="@associationID"/>
          </xs:unique>
        </xs:element>
        <xs:element ref="LN" maxOccurs="unbounded"/>
      </xs:choice>
      <xs:attribute name="router" type="xs:boolean" use="optional" default="false">
      </xs:attribute>
      <xs:attribute name="clock" type="xs:boolean" use="optional" default="false">
      </xs:attribute>
      <xs:element name="GOOSESecurity" type="tCertificate" use="optional" maxOccurs="7" >
      <xs:element name="SMVSecurity" type="tCertificate" use="optional" maxOccurs="7" >
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

IEC 1055/07

Figure 20. Extension to AccessPoint SCL definition

A minimum of one GOOSESecurity instance and one SVSecurity instance must be included in any implementation claiming to support Secure GOOSE and secure SV. The GOOSEEncryptioninUse or SVEncryptioninUse attributes, whose value(s) must be the same as the XferNumber for the certificate intended to be used for both authentication and encryption, must be present in implementations that claim to enable encryption.

3.3.9 Conformance

3.3.9.1 General conformance

To claim implementation compliance to the IEC TS 62351 standard specifications, an Enhanced Protocol Implementation Conformance Statement (PICS) should be provided. Extra Protocol implementation eXtra information (PIXIT) data may be required for some profiles.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

The following definitions apply to the clauses and tables below:

- m: mandatory support - the item shall be implemented.
- c: conditional support - the item shall be implemented if the stated condition exists.
- o: optional support - the implementation may decide to implement the item.
- x: excluded - the implementation shall not implement this item.
- i: out-of-scope - the implementation of the item is not within the scope of this specification.

Table 2: provide Information that declaring the implementation calming support for the IEC TS 62351 standard specifications.

Table 2. IEC TS 62351 Conformance table

		Client		Server		Value/Comment
		f/s		f/s		
G1	Support for IEC 61850-8-1/ISO 9506	0	C1	0	C1	
G2	Support for IEC 61850-8-1 GOOSE	0	C1	0	C1	
G3	Support for IEC 61850-9-2 SMV	0	C1	0	C1	
G4	Support for SNTP security	0		0		
C1 - At least one shall have support declared						

3.3.9.2 Conformance for implementations claiming ISO 9506 profile security

For implementations claiming support for the security profile for ISO 9506 / IEC 61850 profile, the information in Table 3 shall be provided.

Table 3. PICS for ISO 9506 profile

		Client		Server		Value/Comment
		f/s		f/s		
S1	ACSE Authentica-tion	m		m		
S2	IEC 62351-4 Sup-port	m		m		
S3A	Mandatory Cipher	m		m		

	Suite					
S3B	TLS-D H-RSA-W ITH-AES-1 28-S HA	0		m		

3.3.9.3 Conformance for implementations claiming VLAN profile security

For implementations claiming support for the security profile for VLAN IEC 61850 profile, the information in Table 4 shall be provided.

Table 4. PICS for VLAN profiles

		Client		Server		Value/Comment
		f/s		f/s		
S4	SCL extensions	m		m		
S4a	IEC 61850-8-1 GOOSE security	C1		C1		
S4b	IEC 61850-9-2 SMV security	C2		C2		
c1 - shall be”m" for implementations claiming GOOSE security conformance. c2 - shall be “m” for implementation claiming SV security conformance.						

3.3.9.4 Conformance for implementations claiming SNTP profile security

Implementations claiming support for the SNTP IEC 61850 security profile shall provide this information illustrated in Table 5.

Table 5. PICS for SNTP profiles

		Client		Server		Value/Comment
		f/s		f/s		
S7	RFC 2030	m		m		

References

[1] IEC 61850 (all parts), Communication networks and systems in substations

[2] IEC 62351 (all parts) Power systems management and associated information exchange - Data and communications security to security issues

[23] IEC Just Published Just Published | IEC Webstore

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

4 Annex A

Table 1. Commented recommended cipher suites from IEC TS 62351-4:.2007

Key exchange		Encryption	Hash	Source	Support
Algorithm	Signature				
TLS_RSA_		WITH_RC4_128_	SHA	RFC 2246 (TLS 1.0)	Disallowed (RC 4 considered weak)
TLS_RSA_		WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	o
TLS_DH_	DSS_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	o
TLS_DH_	RSA_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	o
TLS_DHE_	DSS_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	o
TLS_DHE_	RSA_	WITH_3DES_ede_CBC_	SHA	RFC 2246 (TLS 1.0)	o
TLS_DH_	DSS_	WITH_AES_128_	SHA	RFC 4346 (TLS 1.1)	o
TLS_DH_	DSS_	WITH_AES_256_	SHA	RFC 4346 (TLS 1.1)	m
TLS_DH_		WITH_AES_128_	SHA	RFC 4346 (TLS 1.1)	Disallowed (anonymous)
TLS_DH_		WITH_AES_256_	SHA	RFC 4346 (TLS 1.1)	Disallowed (anonymous)

Table 2. Commented recommended Cipher suites

Key exchange		Encryption	Hash	Source	Support
Algorithm	Signature				
TLS_RSA		WITH_AES_128_CBC_	SHA256	RFC 5246	m
TLS_DH_	RSA_	WITH_AES_128_CBC_	SHA256	RFC 5246	o
TLS_DH_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288 [5]	m
TLS_DHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5288 [5]	m
TLS_DH_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5288 [5]	o
TLS_ECDHE_	RSA_	WITH_AES_128_GCM_	SHA256	RFC 5289 [6]	o
TLS_ECDHE_	RSA_	WITH_AES_256_GCM_	SHA384	RFC 5289 [6]	o
TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256	RFC 5289 [7]	m
TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384	RFC 5289 [7]	o

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund