IEC TR 61850-90-16

Edition 1.0 2021-06

TECHNICAL REPORT

colour inside

Communication networks and systems in power utility automations – Part 90-16: Requirements of system management for Smart Energy Automation

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TR 61850-90-16

Edition 1.0 2021-06

TECHNICAL REPORT

colour inside

Communication networks and systems in power utility automations – Part 90-16: Requirements of system management for Smart Energy Automation

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-9713-1

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

COMMUNICATION NETWORKS AND SYSTEMS IN POWER UTILITY AUTOMATIONS –

Part 90-16: Requirements of system management for Smart Energy Automation

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 61850-90-16 has been prepared by IEC technical committee TC57: Power systems management and associated information exchange. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
57/2315/DTR	57/2352/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

A list of all the parts in the IEC 61850 series, published under the general title *Communication networks and systems in power utility automations*, can be found on the IEC website.

This publication is split into two parts:

- This document, providing an overview of the main content, and high-level diagrams
- This document has an associated machine-readable version of the use-cases in the form of a zipped HTML code component IEC_TR_61850-90-16_HTML_2020_FullDC2.zip. It uses Active X components and is compatible with Microsoft Internet Explorer

The same copyright and licensing conditions apply to the "paper" part (this document) and the complementary HTML part provided within the IEC_TR_61850-90-16_HTML_2020_FullDC2.zip file.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The distribution grid is facing a massive roll out and refurbishment of automation equipment to implement deeper monitoring and new smart grid applications. The new equipment to be deployed in order to solve today's issues (MV voltage and reactive power regulation for example) will necessarily have to be adjustable and updatable in order to face challenges of tomorrow (for example massive electric vehicles fleets, low voltage automation, etc.) which will arrive long before the end of its 20 years' service life. Furthermore, there is a necessity for the equipment to adapt to the evolving and growing cybersecurity threats.

The equipment will therefore need to be patched, updated and reconfigured, and this has to be done remotely due to the great number of equipment. This is a cornerstone of the System Management (SM), which refers to functionalities that are not directly linked to the operational role of the equipment but allow it to perform its operational functions in the best conditions possible. System Management or Smart Grid Devices Management also includes other functions such as asset management or supervision.

These functionalities need to be managed by the grid operator and address multiple devices from different vendors through independent Information Systems and thus the requirements and exchanges need to be standardized. As these are to be applied to IEC 61850 compliant equipment, these mechanisms need to be integrated in the standard.

COMMUNICATION NETWORKS AND SYSTEMS IN POWER UTILITY AUTOMATIONS –

Part 90-16: Requirements of system management for Smart Energy Automation

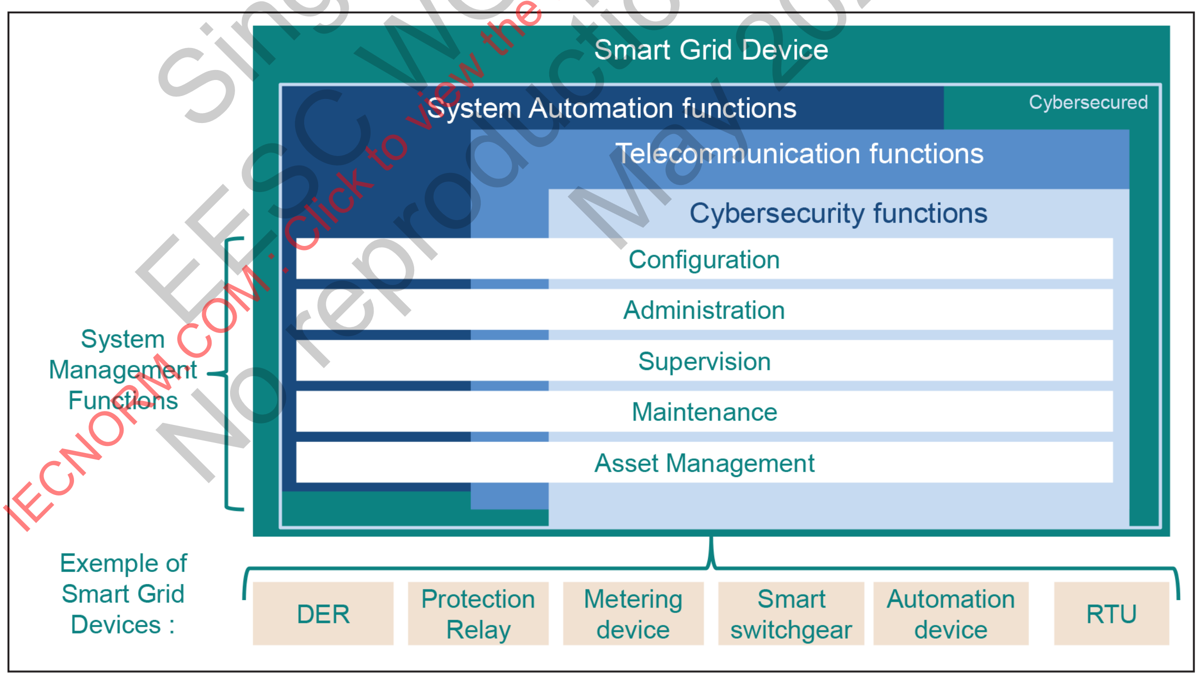
1 Scope

This part of IEC 61850, which is a technical report, specifies the mechanisms for the system management of Smart Grid Devices as IEC 61850 equipment in power utility automation as well as telecommunication and cybersecurity equipment.

System Management of Smart Grid Devices or Smart Grid Device Management refers to functionalities that are not directly linked to the operational role of the equipment (which for grid automation equipment would be to protect and allow remote supervision and control on the grid) but allow it to perform its operational functions in the best conditions possible.

The main functions of Smart Grid Device Management can be categorized as illustrated in Figure 1 and described below. These actions being available from remote information systems, they affect system automation functions, telecommunication functions and cybersecurity functions as these three categories are interacting in a Smart grid Device or system.

The Smart Grid domain has been chosen for these use cases, including distributed energy resources. This content is expected to be applicable to other domains, such as industrial automation domain and grid user domain.



IEC

Figure 1 – Scope of the functions and objects covered by the Smart Grid Device Management

IEC TR 62351-10, *Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines.* The main five functions for System Management are listed below:

1) IEC TR 62351-90-1, *Power systems management and associated information exchange - Data and communications security - Part 90-1: Guidelines for handling role-based access control in power systems*
2) Managing the software (administration): download, update and manage the firmware versions of automation equipment;
3) Supervising: active supervision of Smart Grid devices in order to ensure the required quality of service of the system, to diagnose potential problems and if possible to suggest resiliency solutions in case of deficiency;
4) Maintaining the system: collect data concerning the operational state of the equipment in order to be able to initiate predictive analysis, perform maintenance actions and reduce failure probabilities;
5) Managing one's assets: collect and transfer patrimonial data to the information systems in charge of asset management and maintenance.

This part of IEC 61850 specifies these functions through use cases associated state machines, requirements and processes necessary for their implementation.

Since the outcome of that work will affect several parts of IEC 61850, in a first step, this technical report has been prepared, which addresses the topic from an application specific viewpoint across all affected parts of IEC 61850. That approach is similar to what is done for example with IEC 61850-90-1 for the communication between substations. Once the report is approved, the affected parts of the standard can be amended with the results from the report.

The major part of the work consists in designing the use cases with the appropriate requirements.

Smart Grid Devices Management Use Cases will also be used for extracting requirements on cybersecurity:

- These steps and requirements will "surround" the Use Case functional steps for the most part, but may require some validation steps within the procedures as well.
- The IEC 62351 series should address those requirements (For example: modifying RBAC parameters in an IED, install RBAC parameters inside the IED).
- Those cybersecurity workflows and requirements will be considered as pre-requisites in Smart Grid Devices Management Use Cases.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-7-2, *Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*

IEC 62351-8, *Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management*

IEC 62351-9, *Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment*

IEC TR 62351-10, *Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines*

IEC TR 62351-90-1, *Power systems management and associated information exchange – Data and communications security – Part 90-1: Guidelines for handling role-based access control in power systems*

IEC TR 62443-2-3:2015, *Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment*

IEC 62443-3-3, *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

IEC 62443-4-2, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
actor
entity that communicates and interacts

Note 1 to entry: These actors can include people, software applications, systems, databases, and even the power system itself.

Note 2 to entry: In IEC TS 62913 this term includes the concepts of Business Role and System Role involved in Use Cases.

[SOURCE: IEC 62559-2:2015]

3.2
asset management
systematic process of developing, operating, maintaining, upgrading, and disposing of assets in the most cost-effective manner (including all costs, risks and performance attributes)

3.3
business role
role describing a finite set of responsibilities that is assumed by a party (organisations, organisational entities or physical persons)

3.4
role
type of actor which has responsibilities and represents the external intended behaviour of a party

EXAMPLE 1 A legally defined market participant (e.g. grid operator, customer), a generic role which represents a bundle of possible roles (e.g. flexibility operator) or an artificially defined body needed for generic process and Use Case descriptions.

Note 1 to entry: The IEC TS 62913 series use two kinds of roles: Business Roles and System Roles.

Note 2 to entry: Legally or generically defined external actors may be named and identified by their roles.

3.5
system role

role describing a finite set of functionalities that is assumed by an entity (devices, information system, equipment)

3.6
use case

specification of a set of actions performed by a system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system

Note 1 to entry: There are two types of Use Cases:

- Business Use Cases describe how Business Roles interact to execute a business process. These processes are derived from services, i.e. business transactions, which have previously been identified.
- System Use Cases describe how System and/or Business Roles of a given system interact to perform a Smart Grid Function required to enable / facilitate the business processes described in Business Use Cases. Their purpose is to detail the execution of those processes from an Information System perspective.

Table 1 highlights the differences between these 2 types of Use Case.

Table 1 – Differences between Business and System Use Cases

Type of Use Case	Description	Actors involved
Business Use Cases (BUC)	Depicts a business process– Expected to be system agnostic	Business Roles (organisations, organisational entities or physical persons)
System Use Cases (SUC)	Depicts a function or sub-function supporting one or several business processes	Business Roles and System Roles (Devices, Information System)

Note 2 to entry: Since a Smart Grid Function can be used to enable / facilitate more than one business process, a System Use Case can be linked to more than one Business Use Case.

3.7
IED

Intelligent Electronic Device which receives data from sensors and power equipment and can issue control commands, such as tripping circuit breakers if it senses voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level

4 Smart Grid System life cycle

4.1 Overview

A Smart Grid System is composed of several Smart Grid Devices (IEDs, Cybersecurity devices, telecommunication devices) and network equipment covering multiple functions as described in Figure 2. Smart Grid Devices can include automation functions as well as telecommunication or cybersecurity functions as described in Figure 1. Automation functions (as well as telecommunication or cybersecurity functions) can be spread on several devices as shown in Figure 2. Automation System lifecycle depends on the lifecycle of individual elements.

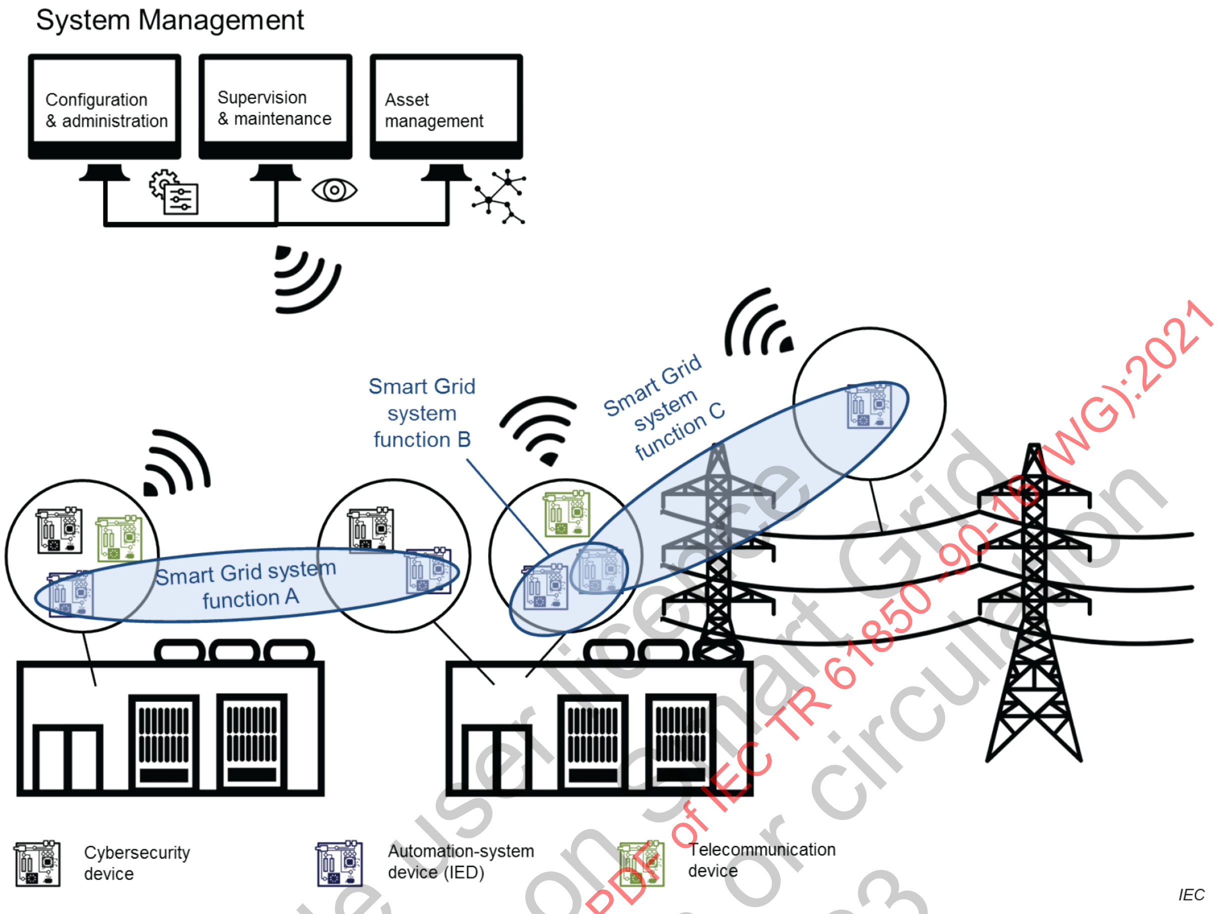

System Management
Configuration & administration
Supervision & maintenance
Asset management
Smart Grid system function A
Smart Grid system function B
Smart Grid system function C
Cybersecurity device
Automation-system device (IED)
Telecommunication device
IEC

Figure 2 – Smart Grid Systems and system management

4.2 IED life-cycle

4.2.1 Software

During the lifecycle of an IED, different versions of software will be developed. These new software versions add new functionalities and correct problems. The grid operator has to evaluate if the new version will be installed or not. The decision is based on:

- Needs to implement the new features.
- Identified error correction that may have an impact on system reliability or security.

Before deploying the new software version, the grid operator may decide to do new tests to be sure that the new version is functionally compliant and is error free.

4.2.2 Hardware

It is also possible that the manufacturer identifies and corrects a hardware problem. The modification is made on site and configuration or software updates might be required.

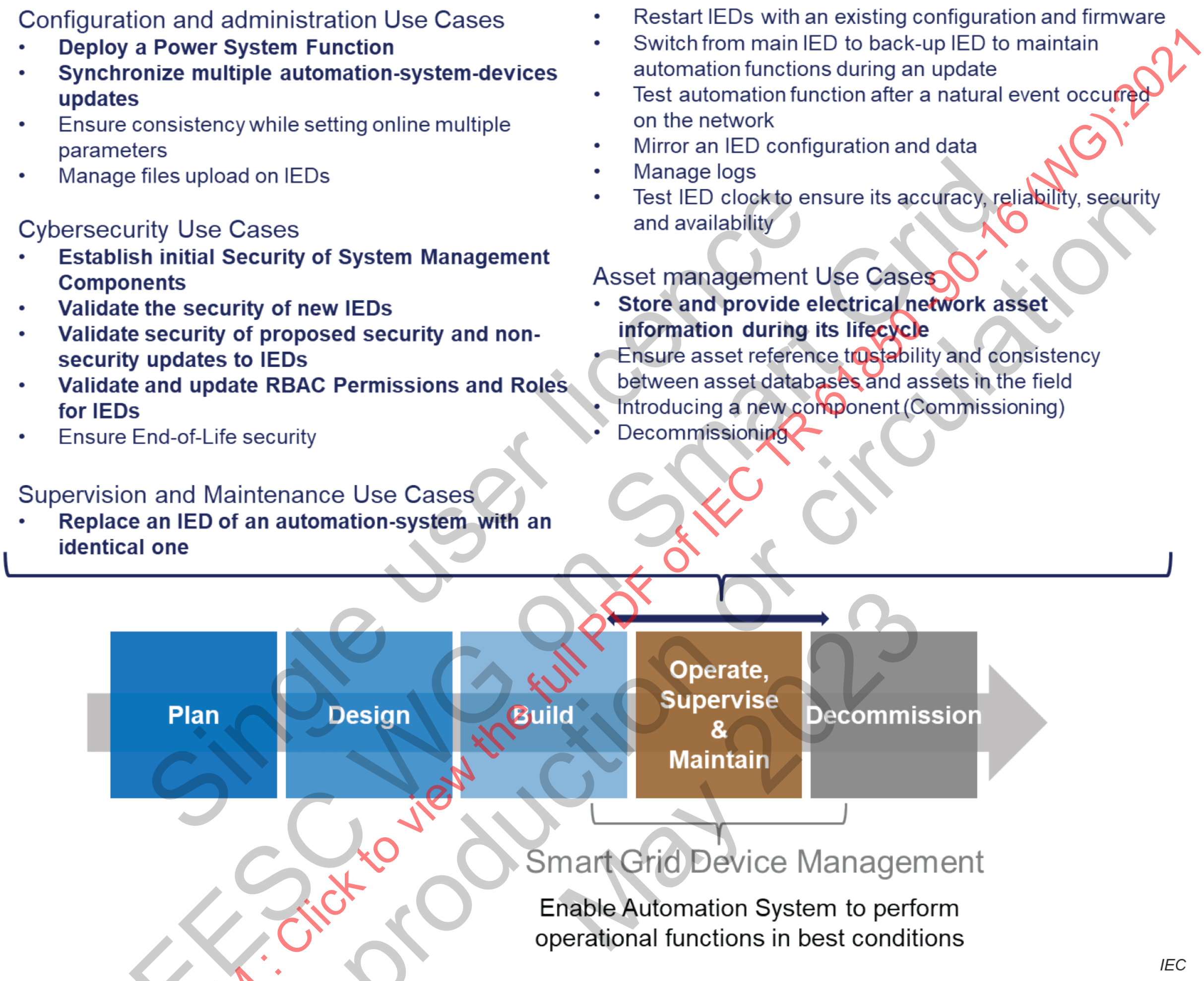
4.2.3 Main life-cycle stages

As shown in Figure 3, system management mostly focuses on the "Operate, Supervise and Maintain" phase of the lifecycle.

In addition, system management is a key enabler of the business use case "Enable Automation System to perform operational functions in best conditions" as depicted in Clause 5.

When considering the whole steps of a system, within its life cycle it appears that addressing system management leads to consider the list of system use cases as depicted in Figure 3.

The current stage of the document only covers the system use cases which are marked in bold in Figure 3 with a special focus on the system use case "Deploy a Power System Function". Each of these system use cases are further depicted in Clause 6. A short description of the others uses cases is given in Annex A.



Configuration and administration Use Cases

- **Deploy a Power System Function**
- **Synchronize multiple automation-system-devices updates**
- Ensure consistency while setting online multiple parameters
- Manage files upload on IEDs

Cybersecurity Use Cases

- **Establish initial Security of System Management Components**
- **Validate the security of new IEDs**
- **Validate security of proposed security and non-security updates to IEDs**
- **Validate and update RBAC Permissions and Roles for IEDs**
- Ensure End-of-Life security

Supervision and Maintenance Use Cases

- **Replace an IED of an automation-system with an identical one**
- Restart IEDs with an existing configuration and firmware
- Switch from main IED to back-up IED to maintain automation functions during an update
- Test automation function after a natural event occurred on the network
- Mirror an IED configuration and data
- Manage logs
- Test IED clock to ensure its accuracy, reliability, security and availability

Asset management Use Cases

- **Store and provide electrical network asset information during its lifecycle**
- Ensure asset reference trustability and consistency between asset databases and assets in the field
- Introducing a new component (Commissioning)
- Decommissioning

Smart Grid Device Management

Enable Automation System to perform operational functions in best conditions

Figure 3 – Different Use Cases through the lifecycle of a smart grid system

4.2.4 Cybersecurity lifecycle for system management

4.2.4.1 General

For system management, three cybersecurity processes need to be addressed:

1) The system management update process itself must include cybersecurity procedures and technologies to ensure that the people, applications, IEDs, and other systems are authenticated and authorized, and that the interactions between the systems are validated and properly logged.

2) IEDs must have their operational software initially secured as well as securely updated in order to continue to operate securely.

3) The same security process should take place whenever the cybersecurity software is updated.

In both cases, cybersecurity standards should be used as appropriate see [1][1] to [10].

4.2.4.2 Cybersecurity for the system management system

The system management system must be secure before any IEDs can be securely updated. These steps include:

- Implement and validate security systems, security-related databases, and security applications
- Establish secure networks for exchanging data securely between System Management components
- Implement and establish security of the system management (System Management) systems, databases, and applications
- Determine all types of information that will require consistency and conformance validation before being updated to IEDs
- Establish initial RBAC permissions for data in System Management systems, databases, and applications
- Establish System Management Roles and associate them with permissions with all of the System Management components
- Test system management components for functionality and for security of the process
- Monitor the security of the information exchanges and periodically retest the system management components for functionality and for security of the process

4.2.4.3 Managing cybersecurity during updates of operational software

The first cybersecurity process is to manage the update of operational software in the IED(s). It involves the following steps:

- The (human) system management users log into the system management system which validates their login credentials and determines what access permissions they have as determined by their roles.
- The software or firmware is validated from a cybersecurity perspective, with verification that it is the correct version, has all correct certificates or keys, and that there is no malware embedded in it.
- A secure connection is established between the system management application and the IED(s) to be updated, using administrative certificates or other means to authenticate the connection.
- The IED's relevant operational certificates are validated to determine they are not revoked or expired.
- During the software/firmware update process, each step is validated to ensure that the users, applications, IEDs, and/or other systems involved are authorized for that step.

All steps that include cybersecurity validation or authorization, including those where the software is rolled back, are logged in the appropriate security logs.

4.2.4.4 Updating the cybersecurity software in systems

The next cybersecurity process uses basically the same steps that are used for updating the software/firmware of the IEDs, involves the following steps:

- The cybersecurity software or firmware is validated as functionally correct and free of malware.

[1] Numbers in square brackets refer to the bibliography.

- A secure connection is established between the system management application and the IED(s) to be updated, using administrative certificates or other means to authenticate the connection.
- The IED's relevant operational certificates are validated to determine they are not revoked or expired.
- The updated cybersecurity software or firmware is transferred to the IED(s).
- The IED(s) validate the cybersecurity software.
- At the appropriate time, the IED(s) switch to the updated cybersecurity software.
- If there is an error condition or other failure, the IED(s) switch back to the existing cybersecurity software.
- If there is no error condition, the IED(s) start using the updated cybersecurity software.

All steps are logged in the appropriate security logs.

The use cases for these cybersecurity requirements are described in 6.4.

4.3 System management roles identified

4.3.1 Business roles

The Business roles identified for the system management Use Cases are listed in Table 2.

Table 2 – System management business roles

Role name	Role description
Systems Management Operator	A party responsible for configuring, administrating, supervising and maintaining Smart Grid Devices as parts of an Automation System: IEDs, group of IEDs and Telecommunication or Cybersecurity devices, from commissioning to decommissioning during their service life
Distribution Grid Operator	Entity responsible for the planning, operation, maintenance, and the development in given areas of the electricity distribution network (LV, MV, and potentially HV), the quality of electricity supply (power delivery, voltage etc.) and for customer access to ESR market through his system under regulated conditions. Equivalent to MV/LV System Operators. [See IEC SRD 62913-2-1]
Equipment Manufacturer	Entity that produces and sells electrical devices and electricity management devices.
Grid Operator	A party that operates one or more grids. It can be an EHV and HV System Operator and/or a HV and MV/LV System Operator. [See IEC SRD 62913-2-1]
Grid User	A party connected to the grid and consuming and/or producing electricity. Grid Users include Consumers, Producers, and Prosumers. Prosumer is a party that both consumes and produces electricity. Equivalent to Party Connected to the Grid. [See IEC SRD 62913-2-1]
Asset Field Operator or Asset Maintenance Operator	A party responsible for maintaining physical assets from commissioning to decommissioning during their service life
System Operator	Party responsible for safe and reliable operation of a part of the electric power system in a certain area and for connection to other parts of the electric power system. [SOURCE: IEC 60050-617:2009, 617-02-09]

4.3.2 System roles

The system roles identified for the system management Use Cases are listed in Table 3.

Table 3 – System management system roles

Role name	Role description
Asset-Configuration and data Information System (ACIS)	The Information System recording configuration and settings data changes in automation-systems
Asset-Health Information System (AHIS)	The Information System recording health information of an asset (counters, status, watchdogs, alarms …)
Asset-Location Information System (ALIS)	The Information System recording field location information (latitude, longitude, link to physical infrastructures …)
Asset-Operations Information System (AOIS)	The Information System recording field and remote construction, commissioning, decommissioning, maintenance and inspection operations
Asset-Patrimonial Information System (APIS)	The Information System recording patrimonial information such as (Supplier, plate number, procurement information …)
Certificate authority	An entity that issues digital certificates
Device Management Information System (DMIS)	Any Information System managing one or multiple IED, with the capability to transmit data, control, files from, or to, an IED, for example configuration, supervision or maintenance purpose.
DMIS – Element Manager (EM)	Function management system. It manages the following aspects of a function deployed on one or several devices • Fault Management • Configuration Management (configuration roll-out, settings …) • Accounting Management (Use supervision …) • Performance Management • Security Management Those management items are known as FCAPS aspects of a function
DMIS – EM -Cybersecurity-Element Manager (CEMIS)	Cybersecurity function management system, managing FCAPS aspects of a cyber function with a validation and management role over the cybersecurity elements (keys, certificates, RBAC …) for a given system with the capability to transmit data from, or to, equipment or systems.
DMIS – EM -Power System Element Manager (PSEMIS)	Power System function management system, managing FCAPS aspects of a function with a validation and management role over the key elements for a given system with the capability to transmit data from, or to, equipment or systems.
DMIS – EM -Telecommunication Element Manager (TEMIS)	Telecommunication function management system, managing FCAPS aspects of a function with a validation and management role over the key elements for a given system with the capability to transmit data from, or to, equipment or systems
E2EO – Cybersecurity Policy Administrator (CPA)	Information System holding the requirements and policies for deploying functions dedicated to or linked to the Cybersecurity domain
E2EO – Function Orchestration	Sub system of the End-to-End Orchestrator dedicated to retrieve requirements from the FDC and from policy managers to elaborate task workflows
E2EO – Power System Policy Administrator (PSPA)	Information System holding the requirements and policies for deploying functions dedicated to or linked to the Power System domain
E2EO – Telecommunication Network Policy Administrator (TPNA)	Information System holding the requirements and policies for deploying functions dedicated to or linked to the Telecommunication domain

Role name	Role description
Electrical Network Asset (ENA)	Electrical Network Asset can either be a primary equipment for an automation system asset, a telecommunication asset or a cyber security asset such as (non exhaustive): • Intrusion sensor • Routers • Switches • Reclosers • Protections An Electrical Network Asset can be an IED or rely on an IED for communication
End-to-End Orchestrator (E2EO)	Task orchestration system for tasks such as: deployments, configurations, activations on all domains
FD – Deployment Manager (DM)	Information System monitoring functions deployment on a IED's
FD – OS and FW Data Base (FWDB)	Database holding software packages ready for deployment
Function Descriptor Catalogue (FDC)	Information System holding the description of the elements required for implementing a function and the specific associated requirements and policies for deploying this function
Grid history information system (GHIS)	The Information System archiving electrotechnical measures, and monitoring information from the grid
IED – Device Cybersecurity Functions (DCF)	Dedicated functions for cybersecurity on an IED
IED – Device Power System Functions (DPSF)	Dedicated functions for automation on the power system on a IED
IED – Device Telecommunication Functions (DTF)	Dedicated functions for telecommunication on an IED
IED – Local Installer(LI)	Dedicated functions on a IED for installing software's update
Intelligent Electronic Device (IED)	Any device incorporating one or more processors, with the capability to receive or send, data/control from, or to, an external source, for example electronic multi-function meters, digital relays, controllers. Device capable of executing the behaviour of one or more specified logical nodes in a particular context and delimited by its interfaces. [SOURCE: IEC TS 61850-2:2019, 2.59] An IED is an automation system device or a Smart Grid Device
Owner of IED	Owner of the Intelligent Electronic Device
Owner of System Management system	Owner of system management system
RBAC Installation and Validation Tools	Tools used for installing and verifying role-based access permissions and rights for IEDs
RBAC installer	Installer of the role-based access permissions and rights
RBAC Permissions and Rights Repository	Database containing the links between roles and permissions, as well as the rights for specific types of data
SC – Cybersecurity Functions Configurator (CFC)	System Configurator dedicated to Cybersecurity functions
SC – Power System Functions Configurator (PSFC)	System Configurator dedicated to Power System automation functions
SC – Telecommunication Functions Configurator (TFC)	System Configurator dedicated to Telecommunication functions
SCADA System	Supervisory Control And Data Acquisition system
Security manager	Manager of security of the system management processes and equipment

Role name	Role description
Security manager of telecommunication network	Manager of the security of the telecommunication networks
System Configurator (SC)	Information System for specifying and building configuration for IEDs functions
Vendor of security product	Manufacturer of security products
Vendors of system management products	Manufacturer of system management products

4.4 System management architecture

As mentioned in the introduction, system management needs to be managed remotely and securely by the grid operator. The high level architecture used for Use Cases is illustrated in Figure 4.

For individual equipment, i.e. for example secondary substation automation or the grid operator's interface with power generation on automation systems, the IS communicates directly with the IED. Due to the large number of such equipment, the different interactions need to be done remotely as much as possible.

However, for larger automation systems containing several IEDs, such as those in HV/MV substations, a "local concentrator", similar to the telecontrol proxy/gateway defined in IEC 61850-90-2 but for system management purposes, can be used. This local system management administrator allows to perform locally the same use cases as those available from the IS. The interactions between the IS and the IEDs can be direct or indirect, as shown in Figure 5.

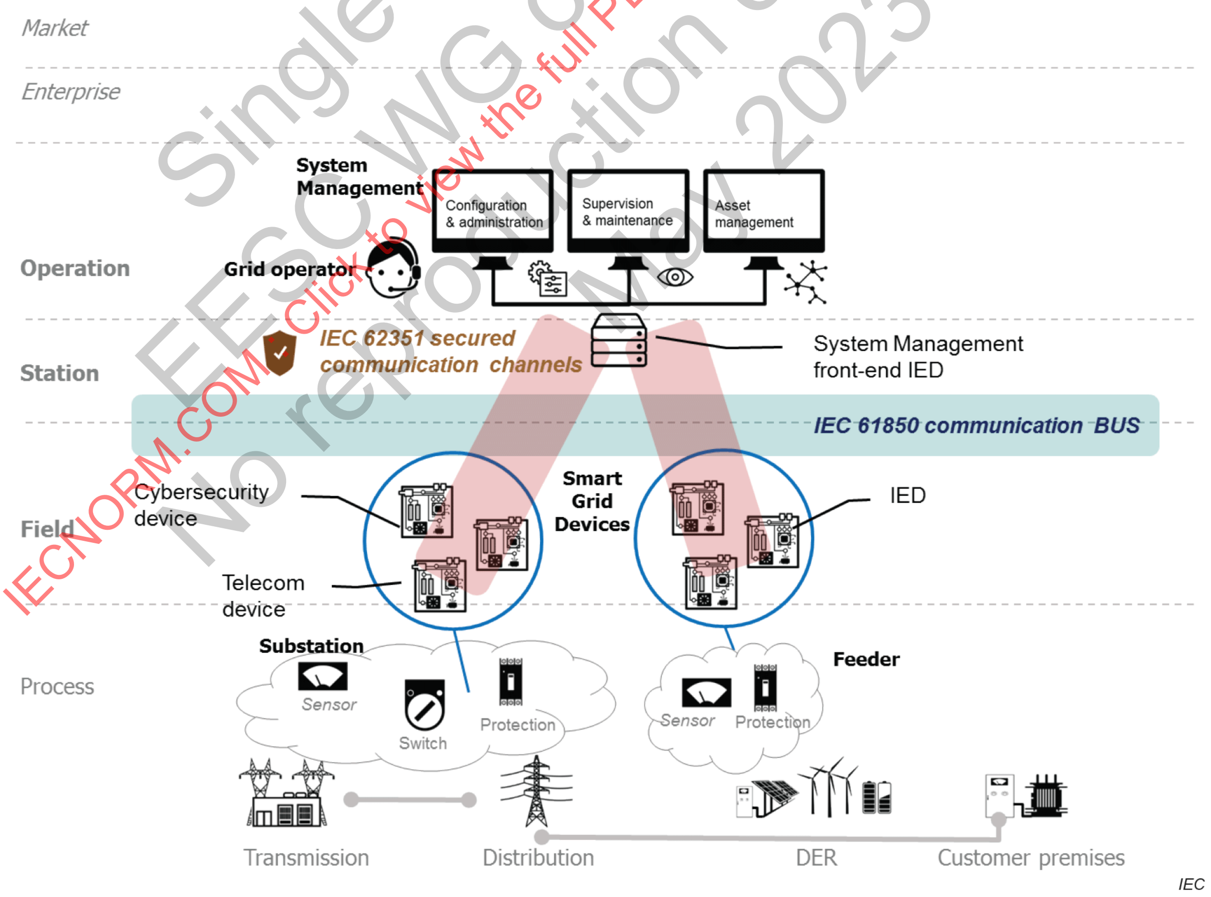


Figure 4 – Illustration of system management architecture on SGAM

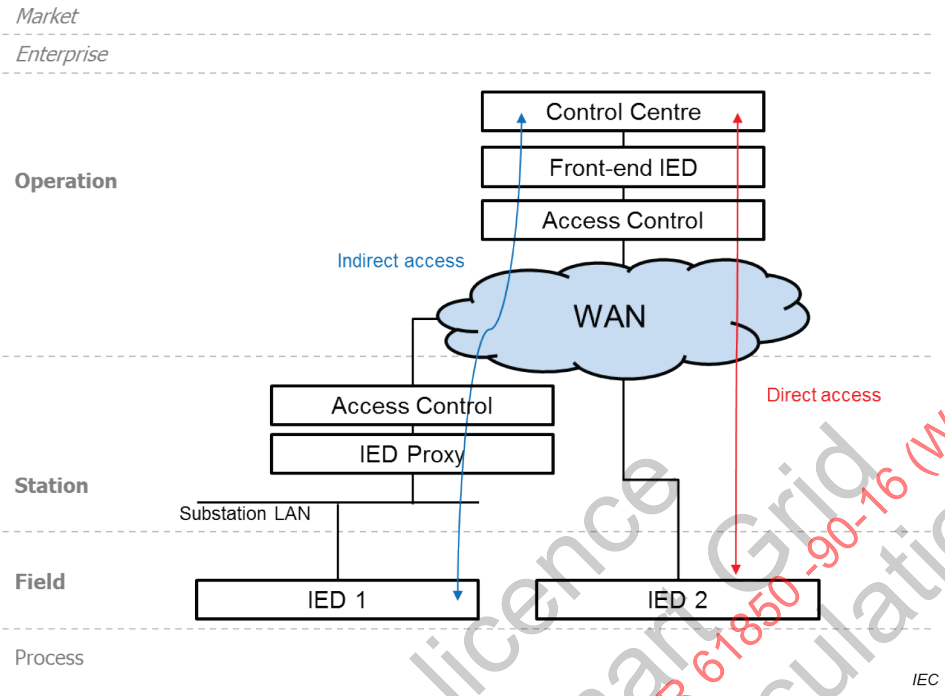


Figure 5 – Interactions between Information System and IEDs

The role-system architecture based on the system role list can be represented as in Figure 6. This architecture is taken from a group specification of ETSI on Network Function Virtualisation (NFV) – management and orchestration.

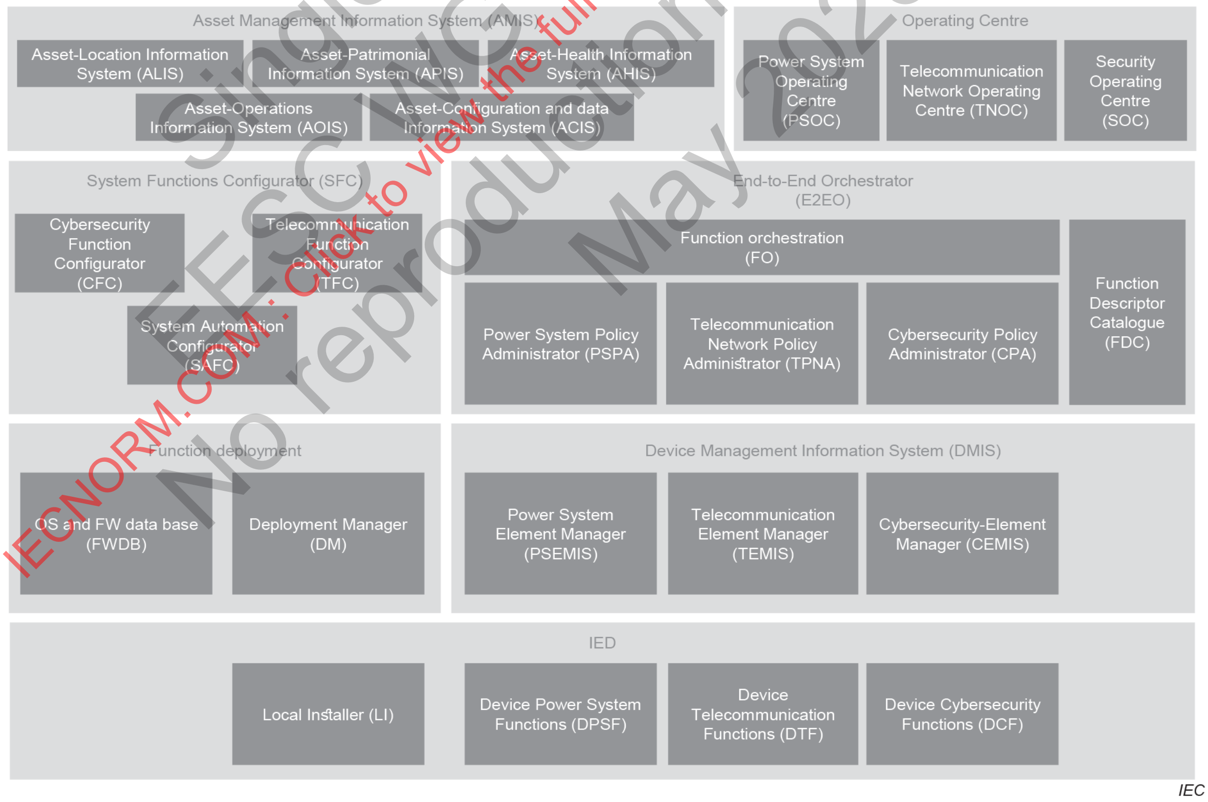

Asset Management Information System (AMIS)
Asset-Location Information System (ALIS)
Asset-Patrimonial Information System (APIS)
Asset-Health Information System (AHIS)
Asset-Operations Information System (AOIS)
Asset-Configuration and data Information System (ACIS)
Operating Centre
Power System Operating Centre (PSOC)
Telecommunication Network Operating Centre (TNOC)
Security Operating Centre (SOC)
System Functions Configurator (SFC)
Cybersecurity Function Configurator (CFC)
Telecommunication Function Configurator (TFC)
System Automation Configurator (SAFC)
End-to-End Orchestrator (E2EO)
Function orchestration (FO)
Power System Policy Administrator (PSPA)
Telecommunication Network Policy Administrator (TPNA)
Cybersecurity Policy Administrator (CPA)
Function Descriptor Catalogue (FDC)
Function deployment
OS and FW data base (FWDB)
Deployment Manager (DM)
Device Management Information System (DMIS)
Power System Element Manager (PSEMIS)
Telecommunication Element Manager (TEMIS)
Cybersecurity-Element Manager (CEMIS)
IED
Local Installer (LI)
Device Power System Functions (DPSF)
Device Telecommunication Functions (DTF)
Device Cybersecurity Functions (DCF)
IEC

Figure 6 – General architecture of key roles involved in system management

5 System management Business Use Cases

5.1 General

For the Business Use Cases and System Use Cases, the completeness of figures is available in the HTML file linked to this document.

5.2 BUC: Enable Automation System to perform operational functions in best conditions

5.2.1 Description of the use case

5.2.1.1 Name of use case

ID	Area(s)/Domain(s)/Zone(s)	Name of use case
61850-90-16-BUC1	Distribution Grid Management	Enable Automation Systems to perform operational functions in best conditions

5.2.1.2 Scope and objectives of use case

Scope	This business Use Case concerns functionalities that are not directly linked to the operational role of the system automation equipment but allow it to perform its operational functions in the best conditions possible.
Objective(s)	Ensure Grid Operator capability to operate its Automation Systems to guarantee continuity and quality of supply: • Easier, more reliable and secured system deployment and commissioning • Secured and easier system maintenance and operating • System activity monitoring and log for tracking and audit
Related business case(s)	Optimise network operations in real-time

5.2.1.3 Narrative of Use Case

Short description
It consists in managing the configuration or the firmware of an Automation System, supervising live adequate operating parameters, retrieving log files and identification data of the equipment in order for the Grid operator to ensure the capability to operate its Automation Systems.
Complete description
The devices to be deployed for deeper monitoring and new smart grid applications will necessarily have to be upgradeable to face new needs and adaptable to the evolving and growing cybersecurity threats. To avoid significant costs remote System Management capability is a necessity, as a huge number of equipment will have to be able to be patched, updated and reconfigured. This use case can be summarized as follows, these actions being available from remote information systems: 1) Configuring: configure operational data, whether it be off line or on-line (grid topology, protection and PLC parameters …); 2) Managing the software: download, upgrade and manage the firmware versions of automation equipment; 3) Supervising: supervise live the smooth running of the system, and be able to identify diagnose and if possible suggest resiliency solutions in case of deficiency in order to ensure the required quality of service; 4) Maintaining the system: collect data concerning the operational state of the equipment in order to be able to lead predictive analysis, launch maintenance actions and reduce failure probabilities; 5) Knowing one’s assets: collect and transfer patrimonial data to the information systems in charge of asset management and maintenance.

5.2.1.4 Key performance indicators (KPI)

ID	Name	Description	Reference to mentioned use case objectives
1	Automation system availability time / year	Availability time of the Automation system per year with its operational functions working with performances expected with the reliability expected, and the level of security expected.	Ensure Grid Operator capability to operate its Automation Systems to guarantee continuity and quality of supply

5.2.1.5 Use case conditions

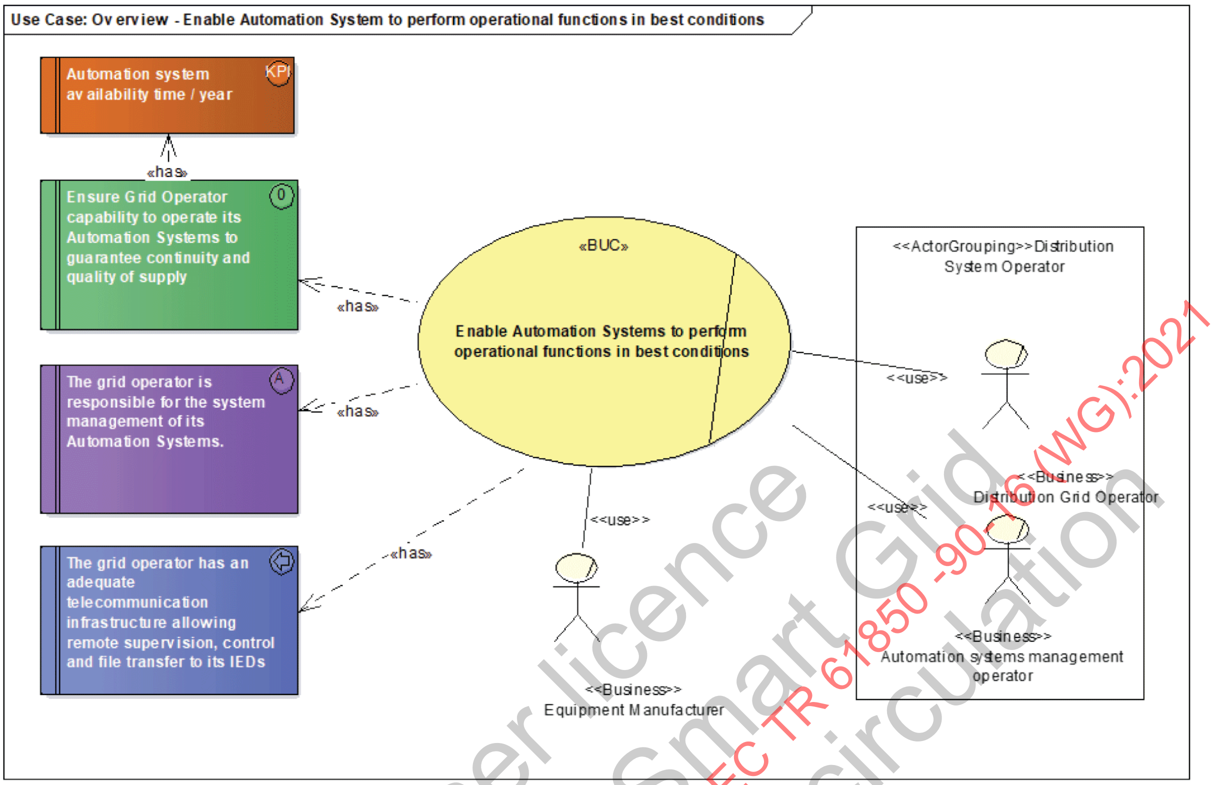
Assumptions	
1	The grid operator is responsible for the system management of its Automation Systems.
Prerequisites	
1	The grid operator has an adequate telecommunication infrastructure allowing remote supervision, control and file transfer to its IEDs

5.2.1.6 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
<<SUC>> Synchronize multiple automation-system-devices updates <<SUC>> Replace an IED of an automation-system with an identical one <<SUC>> Deploy a Power System Function
Level of depth
Short description
Generic, regional or national relation
Generic
Nature of the use case
BUC
Further keywords for classification
Configuration management, Administration, Maintenance, Update, File transfer, Supervision, Asset management, Hypervision

5.2.2 Diagrams of use case

Figure 7 gives the general conditions to perform operational functions in best conditions


Use Case: Overview - Enable Automation System to perform operational functions in best conditions
Automation system availability time / year
KPI
«has»
Ensure Grid Operator capability to operate its Automation Systems to guarantee continuity and quality of supply
O
«has»
The grid operator is responsible for the system management of its Automation Systems.
A
«has»
The grid operator has an adequate telecommunication infrastructure allowing remote supervision, control and file transfer to its IEDs
«has»
«BUC»
Enable Automation Systems to perform operational functions in best conditions
<<use>>
<<Business>>
Equipment Manufacturer
<<ActorGrouping>>Distribution System Operator
<<use>>
<<Business>>
Distribution Grid Operator
<<use>>
<<Business>>
Automation systems management operator

IEC

Figure 7 – Overview of BUC Enable Automation System to perform operational functions in best conditions

5.2.3 Technical details

5.2.3.1 Actors

Actor name	Actor type	Actor description	Further information specific to this use case
Distribution Grid Operator	Business	See Table 2	
Equipment Manufacturer	Business	See Table 2	
Grid Operator	Business	See Table 2	
Automation systems management operator	Business	See Table 2	

5.2.3.2 References

No.	Reference Type	Reference	Status	Impact on use case	Originator / organisation	Link
1		IEC 61850-7-2: Abstract communication service interface (ACSI)			IEC	

6 System management system Use Cases

6.1 General

This clause only provides an overview of the content of the selected system Use Cases. Further details can be found in the associated HTML code component hosted within the *IEC_TR_61850-90-16.HTML.2020.FullDC2.zip* file.

6.2 Configuration and administration system Use Cases

6.2.1 System Use Cases identified

Table 4 describes the system Use Cases that have been identified. The list is non-exhaustive and will be updated as other versions of the present document are issued.

Table 4 – Identified configuration and administration system Use Cases

Index of the system Use cases	Identified system Use Cases	Brief description
61850-90-16 SUC1	Deploy a Power System Function	Ensure that the targeted automation-system device has the best conditions to perform its operational functions by: – Delivering and installing an update to the automation-system device firmware, – Updating configuration of the automation-system device.
61850-90-16 SUC2	Synchronize multiple automation-system-devices updates	Coordinate the updates, FW and/or configuration, of multiple IEDs, or group of IEDs, to operate a system. The updates can occur in the same substation, between substations, along a feeder.

6.2.2 SUC: Deploy a Power System Function

6.2.2.1 Description of the use case

6.2.2.1.1 Name of use case

ID	Area(s)/Domain(s)/Zone(s)	Name of use case
61850-90-16-SUC1	System Management	Deploy of a Power System Function

6.2.2.1.2 Scope and objectives of use case

Scope	Updating an IED's configuration and/or firmware components consists in remotely configuring the IED's operational data (grid topology, protection and control/command parameters ...) through configuration files or updating its firmware or parts of its firmware by uploading a software installation package. This use case concerns offline IED update through configuration files and firmware package. It describes the steps of communication between the IED and the Device Management Information System (DMIS) to select the IED, upload, activate and manage the configuration file and firmware package. This Use Case concerns the individual update of an IED and not the synchronisation of several updates.
Objective(s)	Ensure that the targeted automation-system device has the best conditions to perform its operational functions by: Delivering and installing an update to the automation-system device firmware; Updating configuration of the automation-system device.
Related business case(s)	

6.2.2.1.3 Narrative of Use Case

Short description
This System Use Case starts with the operator asking for the deployment of Power System Function in an IED. The workflow for this Use Case depends mainly on the system-role architecture defined previously. As such, this description is adherent with architecture's choice and system-role repartition between different actors. This Use Case is composed of three major scenarios: – Ask for deployment of Power system Function – Get context and requirements for the function deployment – Generate a specific workflow for the power system function based on the retrieved requirements

Complete description
1. Ask for deployment of Power system Function
1.1. Display detailed information of the selected IED
1.2. Request function description
1.3. Request IED status
1.4. Request Preliminary Cybersecurity verification
1.5. Select a Power System Function
1.6. Send function description
1.7. Send status information from Asset Management
1.8. Description: Status information for each IED include : – Localisation, – Health, – Operation, – Configuration
1.9. Verify that the selected IED is the correct IED for being updated
1.10. Verify compatibility between selected IED and selected Function
1.11. Verify existing security elements in the selected IED, such as certificates, passwords, and security software
2. Get context and requirements for the deployment of the function
2.1. FO gets the FLISR function description from FDC
2.2. FO gets the Power System context and requirements from PSPA (details about localization, SA functions impacted by the deployment)
2.3. FO gets the Telecom Network context and requirements from TNPA (topology information …)
2.4. FO gets the Cybersecurity context and requirements from CPA
2.5. Collect context and requirements
2.6. Requests the Cybersecurity context and requirements from CPA
2.7. Requests the Power System context and requirements from PSPA (details about localization, System Automation functions impacted by the deployment …)
2.8. Requests the Power System function description from FDC
2.9. Requests the Telecom Network context and requirements from TNPA (topology information …)
2.10. Send Cybersecurity context and requirements
2.11. Send Function description
2.12. Send Power system context and requirement
2.13. Send Telecommunication Network context and requirements
3. Generate a specific workflow for the power system function based on the retrieved requirements
Description: Workflow example:
3.1. Deactivate specific power system function
3.2. Change Telecom configuration for deployment
3.3. Change Cyber configuration for deployment
3.4. Deploy Power System function
3.5. Deploy cybersecurity function
3.6. Update cybersecurity configuration
3.7. Activate cybersecurity function
3.8. Update telecom configuration
3.9. Activate cybersecurity function
3.10. Update power system configuration
3.11. Activate Power System function
If the retrieved requirements were different, a different deployment workflow would have been generated.
Workflow steps :
• **3.1 – Deactivate specific Power System Function** – checks the coherence of the order with the current Power system context – Confirm Function deactivation – Deactivates the concerned SAF (System Automation Function) – Forward the Deactivation confirmation – Forward the Deactivation confirmation to Function Orchestrator – Orders the deactivation of specific power system functions to the PSPA – Sends the order to the concerned EM – Validate the first step of the deployment workflow

- **3.2 – Change Telecom Configuration for Deployment**
  - Asks for the generation of the appropriate configuration
  - Checks the coherence of the order with the current telecommunication network context
  - informs of the good configuration update of the telecommunication function
  - Orders the telecommunication function configuration update
  - Sends a report of the telecommunication configuration update
  - Sends the updated telecommunication configuration
  - Updates the configuration of the concerned telecommunication function
  - Validates the second step of the deployment workflow
- **3.3 – Change Cyber configuration for deployment**
  - Asks for the generation of the appropriate configuration
  - Checks the coherence of the order with the current cybersecurity context
  - informs of the good configuration update of the cybersecurity function
  - Orders the cybersecurity function configuration update
  - Sends a report of the cybersecurity configuration update
  - Sends the updated cybersecurity configuration
  - Updates the configuration of the concerned cybersecurity function
  - Validates the third step of the deployment workflow
- **3.4 – Deploy Firmware**
  - Acknowledge Firmware reception
  - Informs the FO of the installation of the firmware
  - Informs the FO of the new monitored function
  - Informs the PSPA of the new monitored function
  - Monitor the new function
  - Orders the Power System function deployment
  - Request the Power System Element Manager to monitor the installed firmware
  - Requests specific details of the deployment from the FDC
  - Requests the associated FW from the FWD (FirmWare Database)
  - Send installation Report to the DM
  - Sends detailed information about the Power System Function
  - Sends the Firmware to DM
  - Validate the Firmware Installation
- **3.5 – Deploy cybersecurity function**
  - Asks for detailed information about the cybersecurity function
  - Deploys the cybersecurity Firmware
  - Informs of the new monitored function
  - Informs the Cybersecurity Element Manager
  - Monitors the new cybersecurity function
  - Orders the cybersecurity function deployment
  - Provides requested information
  - Provides the requested Firmware
  - reports of the good deployment of the cybersecurity function
  - Reports the deployment results
  - Reports to the FO of the monitored function
  - Requests the cybersecurity Firmware
  - Sends the Firmware
  - Validates this step of the deployment workflow
- **3.6 – Update cybersecurity configuration**
  - Asks for the generation of the appropriate configuration
  - Asks for the new cybersecurity context of the IED
  - Checks the coherence of the order with the current cybersecurity context
  - Confirms the update of the cybersecurity configuration
  - Forward the updated cybersecurity configuration
  - Informs of the good cybersecurity update of the concerned Cybersecurity Function
  - Orders the Cybersecurity function configuration update
  - Sends a report of the configuration update
  - Sends the cybersecurity context
  - Sends the updated cybersecurity configuration

  - Updates the configuration
  - Validates this step of deployment workflow
- **3.7 – Activate cybersecurity function**
  - Activate the cybersecurity function
  - Checks the coherence of the order with the current cybersecurity context
  - forwards the activation reports
  - Informs of the good activation of the cybersecurity function
  - Orders the activation of the new updated cybersecurity functions
  - Requests activation of the cybersecurity function
  - sends activation report
  - Sends the activation request
  - Validates this step of deployment workflow
- **3.8 – Update telecom configuration**
  - Asks for the generation of the appropriate configuration
  - Asks for the new telecommunication context of the IED
  - Checks the coherence of the order with the current telecommunication context
  - Confirms the update of the telecommunication configuration
  - Forward the updated telecommunication configuration
  - Informs of the good telecommunication update of the concerned Telecommunication Function
  - Orders the Telecommunication function configuration update
  - Sends a report of the configuration update
  - Sends the telecommunication context
  - Sends the updated telecommunication configuration
  - Updates the configuration
  - Validates this step of deployment workflow
- **3.9 – Activate Telecommunication function**
  - Activate the Telecommunication Function
  - Checks the coherence of the order with the current telecommunication context
  - Forwards the activation reports
  - Informs of the good activation of the Telecommunication Function
  - Orders the activation of the new updated Telecommunication Functions
  - Requests activation of the Telecommunication Function
  - sends activation report
  - Sends the activation request
  - Validates this step of deployment workflow
- **3.10 – Update power system configuration**
  - Asks for the generation of the appropriate configuration
  - Checks the coherence of the order with the current power system context
  - Reports Configuration Status
  - Reports Configuration update status
  - Requests the configuration upload
  - Requests the new power system context of the IED
  - Requests the Power System functions configuration update
  - Sends Context information
  - Sends the new configuration
  - Validate the Configuration
- **3.11 – Activate Power System function**
  - Checks the coherence of the order with the current context
  - Informs the FO of Configuration Promotion
  - Informs the FO of Firmware Promotion
  - Orders the activation of the new Power System Function
  - Request Configuration Activation
  - Request Firmware Activation
  - Sends the order to the Element Manager for Configuration Activation
  - Sends the order to the Element Manager for Firmware Activation
  - Validate The activation of the PS Function deployment

6.2.2.1.4 Key performance indicators (KPI)

ID	Name	Description	Reference to mentioned use case objectives
1	Percentage of update success on the first attempt		Ensure that the targeted automation-system device has the best conditions to perform its operational functions by: Delivering and installing an update to the automation-system device firmware; Updating configuration of the automation-system device.

6.2.2.1.5 Use case conditions

	Assumptions
1	On automation-system device FW update, the device must stay uniquely addressable (minimal configuration guaranteed)
2	IED has "validation" capabilities: The IED is able to validate a firmware: – recognize the content of firmware, – verify the content of firmware regarding the "header"
	Prerequisites
1	An inventory of the automation systems devices is available: This inventory includes all the updatable devices (RTUs, IEDs) and the software and updates/upgrades/patches in use with the following information: • Asset owner • Device manufacturer • Make and model ID • HW version • FW version (boot code version …) • OS version (+ patches …) • SW versions • Fail and fault tolerance • Category or group • Installed and not installed updates • Interdependencies • Architecture and connectivity (How to deploy?) • Criticality Ref. IEC TR 62443-2-3:2015, Annex B
2	Updates available and applicable for each automation systems devices are known through a descriptor: • Device manufacturer ID • HW/FW ID • Update ID • Update supplier ID • Applicability of the Update • Status of manufacturer testing • Results of manufacturer testing • Status of asset owner testing • Results of asset owner testing
3	When a new firmware package file is received through a bundle package, the automation-system device is able to detect it and validate it
4	Fully operational automation systems and telecommunication infrastructure (no downgraded scenario)
5	The updates have been released by manufacturer and tested by asset owner: • Update available • Applicable to the devices under consideration • Tested against the devices under consideration

6.2.2.1.6 Further information to the use case for classification/mapping

Classification information Relation to other use cases
<<BUC>> Enable Automation Systems to perform operational functions in best conditions <<SUC>> Synchronize multiple automation-system-devices updates
Level of depth
Complete description
Nature of the use case
SUC
Further keywords for classification
Configuration management, Update, File transfer, Firmware administration

6.2.2.2 Diagrams of use case

Figure 8 describes the workflow of the use case "Deploy a Power System function".

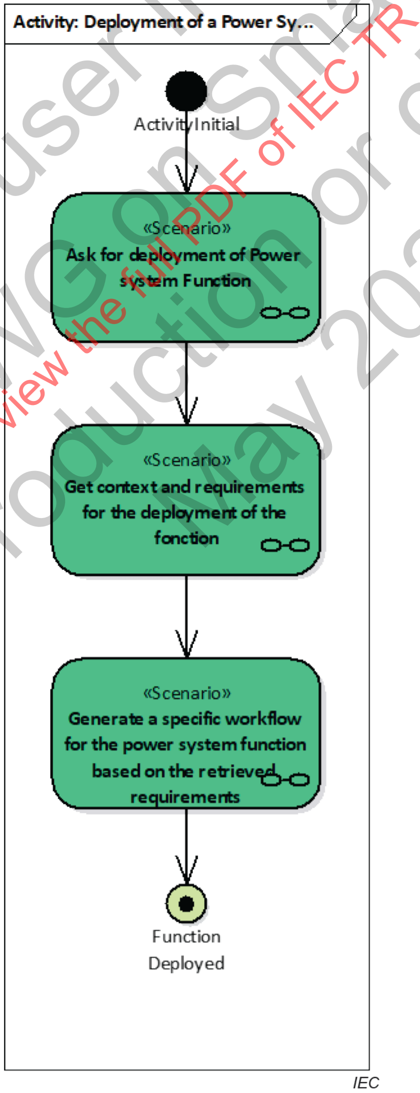

Activity: Deployment of a Power Sy...
ActivityInitial
«Scenario»
Ask for deployment of Power system Function
«Scenario»
Get context and requirements for the deployment of the fonction
«Scenario»
Generate a specific workflow for the power system function based on the retrieved requirements
Function Deployed
IEC

Figure 8 – Scenario diagram of SUC Deploy a Power System function

6.2.2.3 Technical details - References

No.	Reference Type	Reference	Status	Impact on use case	Originator / organisation	Link
2	Standard	IEC 61850-7-2: Abstract communication service interface (ACSI)			IEC	
3	Standard	IEC TR 61850-90-6: Use of IEC 61850 for Distribution Automation Systems			IEC	

6.2.2.4 Step by step analysis of use case - Overview of scenarios

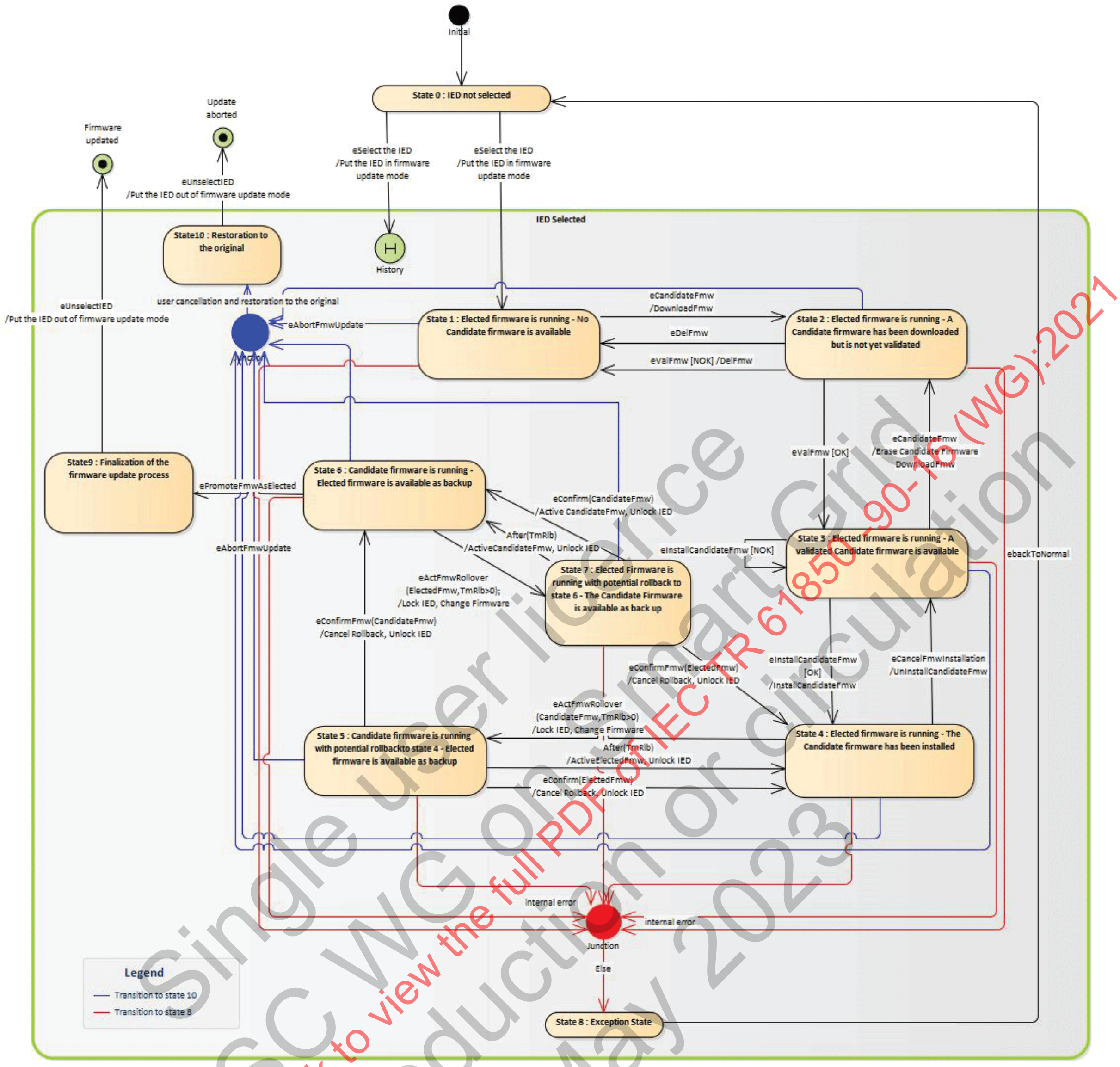
Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Ask for deployment of Power system Function	Display detailed information of the selected IED and its status from Asset Management Information System for verification prior to update Request function description from FDC to verify compatibility between targeted IED and selected Function	Grid operator	New power system function deployment need		Function selected and IED targeted available and compatible
2	Get context and requirements for the deployment of the function	• FO gets the FLISR function description from FDC • FO gets the Power System context and requirements from PSPA (details about localization, SA functions impacted by the deployment) • FO gets the Telecom Network context and requirements from TNPA (topology information …)* • FO gets the Cybersecurity context and requirements from CPA	Function Orchestration (FO)		Function selected and IED targeted available and compatible	Deployment requirements available

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
3	Generate a specific workflow for the power system function based on the retrieved requirements	Workflow example: • Deactivate specific power system function • Change Telecom configuration for deployment • Change Cyber configuration for deployment • ***Deploy Power System function*** • Deploy cybersecurity function • Update cybersecurity configuration • Activate cybersecurity function • Update telecom configuration • Activate cybersecurity function • ***Update power system configuration*** • ***Activate Power System function*** **If the retrieved requirements were different, a different deployment workflow would have been generated**	E2EO		Deployment requirements available	Deployment workflow described and ready to start
3.1	Deactivate specific Power System Function		SCADA		Deployment workflow described and ready to start	Power System Function activated
3.2	Change Telecom Configuration for Deployment		TEMIS			Telecom reconfigured
3.3	Change Cyber configuration for deployment		CEMIS			Cybersecurit y reconfigured
3.4	Deploy Firmware		Deployment Manager			Firmware deployed
3.5	Deploy cybersecurity function		Deployment Manager			New function deployed
3.6	Update cybersecurity configuration		CEMIS			IED cybersecurity configuration updated
3.7	Activate cybersecurity function		Security Operating Centre (SOC)			Cybersecurit y updated and active
3.8	Update telecom configuration		TEMIS			IED telecom configuration updated

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
3.9	Activate Telecommunication function		Telecommunication Network Operating Centre (TNOC)			Telecommunication updated and active
3.10	Update power system configuration		PSEMIS			IED configuration updated
3.11	Activate Power System function		SCADA			Function deployed on IED and active

6.2.2.5 Scenario: Deploy firmware

This scenario is based on the state machine described in Figure 9 and the transitions described in Table 5.


Initial
State 0 : IED not selected
Firmware updated
Update aborted
eUnselectIED
/Put the IED out of firmware update mode
eSelect the IED
/Put the IED in firmware update mode
eSelect the IED
/Put the IED in firmware update mode
IED Selected
State10 : Restoration to the original
History
user cancellation and restoration to the original
eUnselectIED
/Put the IED out of firmware update mode
eAbortFmwUpdate
Junction
State 1 : Elected firmware is running - No Candidate firmware is available
eCandidateFmw
/DownloadFmw
eDelFmw
eValFmw [NOK] /DelFmw
State 2 : Elected firmware is running - A Candidate firmware has been downloaded but is not yet validated
eValFmw [OK]
eCandidateFmw
/Erase Candidate Firmware
DownloadFmw
State9 : Finalization of the firmware update process
ePromoteFmwAsElected
State 6 : Candidate firmware is running - Elected firmware is available as backup
eConfirm(CandidateFmw)
/Active CandidateFmw, Unlock IED
After(TmRlb)
/ActiveCandidateFmw, Unlock IED
eAbortFmwUpdate
eInstallCandidateFmw [NOK]
State 3 : Elected firmware is running - A validated Candidate firmware is available
ebackToNormal
eActFmwRollover
(ElectedFmw,TmRlb>0);
/Lock IED, Change Firmware
State 7 : Elected Firmware is running with potential rollback to state 6 - The Candidate Firmware is available as back up
eConfirmFmw(CandidateFmw)
/Cancel Rollback, Unlock IED
eConfirmFmw(ElectedFmw)
/Cancel Rollback, Unlock IED
eInstallCandidateFmw
[OK]
/InstallCandidateFmw
eCancelFmwInstallation
/UnInstallCandidateFmw
eActFmwRollover
(CandidateFmw,TmRlb>0)
/Lock IED, Change Firmware
State 5 : Candidate firmware is running with potential rollbackto state 4 - Elected firmware is available as backup
After(TmRlb)
/ActiveElectedFmw, Unlock IED
eConfirm(ElectedFmw)
/Cancel Rollback, Unlock IED
State 4 : Elected firmware is running - The Candidate firmware has been installed
internal error
internal error
Junction
Else
State 8 : Exception State
Legend
Transition to state 10
Transition to state 8

IEC

Figure 9 – Deploy firmware state machine

Table 5 – Deploy firmware state machine transitions

Name	Description	From state ...	To state ...
eSelectIED	An IED has been selected for receiving a new firmware	0	1
eCandidateFmw	A candidate firmware is available and ready to be downloaded in the IED.	1	2
eDelFmw	A candidate firmware was deleted.	2	1
eValFmw[OK]	A candidate firmware has been validated by the IED. This request could be made externally or automatically by the IED.	2	3
eValFmw[NOK]	A candidate firmware validation by the IED failed. The candidate firmware is deleted by the IED. This request could be made externally or automatically by the IED.	2	1
eInstallCandidateFmw[OK]	The installation of the candidate firmware was requested and successful.	3	4
eInstallCandidateFmw [NOK]	The installation of the candidate firmware was requested and unsuccessful.	3	3

Name	Description	From state ...	To state ...
eCancelFmwInstallation	A request for cancelling the installation of the firmware was made.	4	3
ePromoteFmwAsElected	The whole process of firmware modification was successful, the candidate firmware must become the default firmware and the available firmware must be deleted.	6	9
Event eActFmwRollover (CandidateFmw;TmRlb>0):	A request has been made to activate the Candidate firmware. The TmRlb could be put to none for disabling the use of a timer.	4	5
Event eActFmwRollover (ElectedFmw;TmRlb>0):	A request has been made to activate the Elected firmware. The TmRlb could be put to none for disabling the use of a timer.	6	7
Event eConfirmFmw (CandidateFmw):	If the confirmation event comes in time for the Candidate firmware, the rollover is considered as successful and the timer for the rollback is stopped. (state 5 to 6) This request could be made externally or automatically by the IED.	7	6
Event eConfirmFmw (ElectedFmw):	If the confirmation event comes in time (before the end of the timer rollback) for the Elected firmware, the rollover is considered as successful and the timer for the rollback is stopped. (state 7 to 4) This request could be made externally or automatically by the IED.	7	4
Event eConfirmFmw (CandidateFmw):	The rollover is considered as unsuccessful, the timer for the rollback is stopped and a rollback is made from the Elected firmware to the Candidate firmware. (state 5 to 4) This request could be made externally or automatically by the IED.	5	4
Event eConfirmFmw (ElectedFmw):	The rollover is considered as unsuccessful, the timer for the rollback is stopped and a rollback is made from the Candidate firmware to the Elected firmware. (state 7 to 6) This request could be made externally or automatically by the IED.	7	6
Event After(TmRlb):	If no confirmation comes in time, the running firmware switch to the previous one.	5	4
eAbortFmwUpdate	A request for aborting the firmware update process has been made.	1-7	10
eUnSelectIED	An IED has been unselected and put out of the firmware update mode. This request could be made externally or automatically by the IED.	9	FINAL
eBackToNormal	Following an error, the IED get back to the state 0 where it is not selected. This request could be made externally or automatically by the IED.	8	0

6.2.2.6 Scenario: Update and activate power system configuration

This scenario is based on the state machine described in Figure 10 and the transitions described in Table 6.

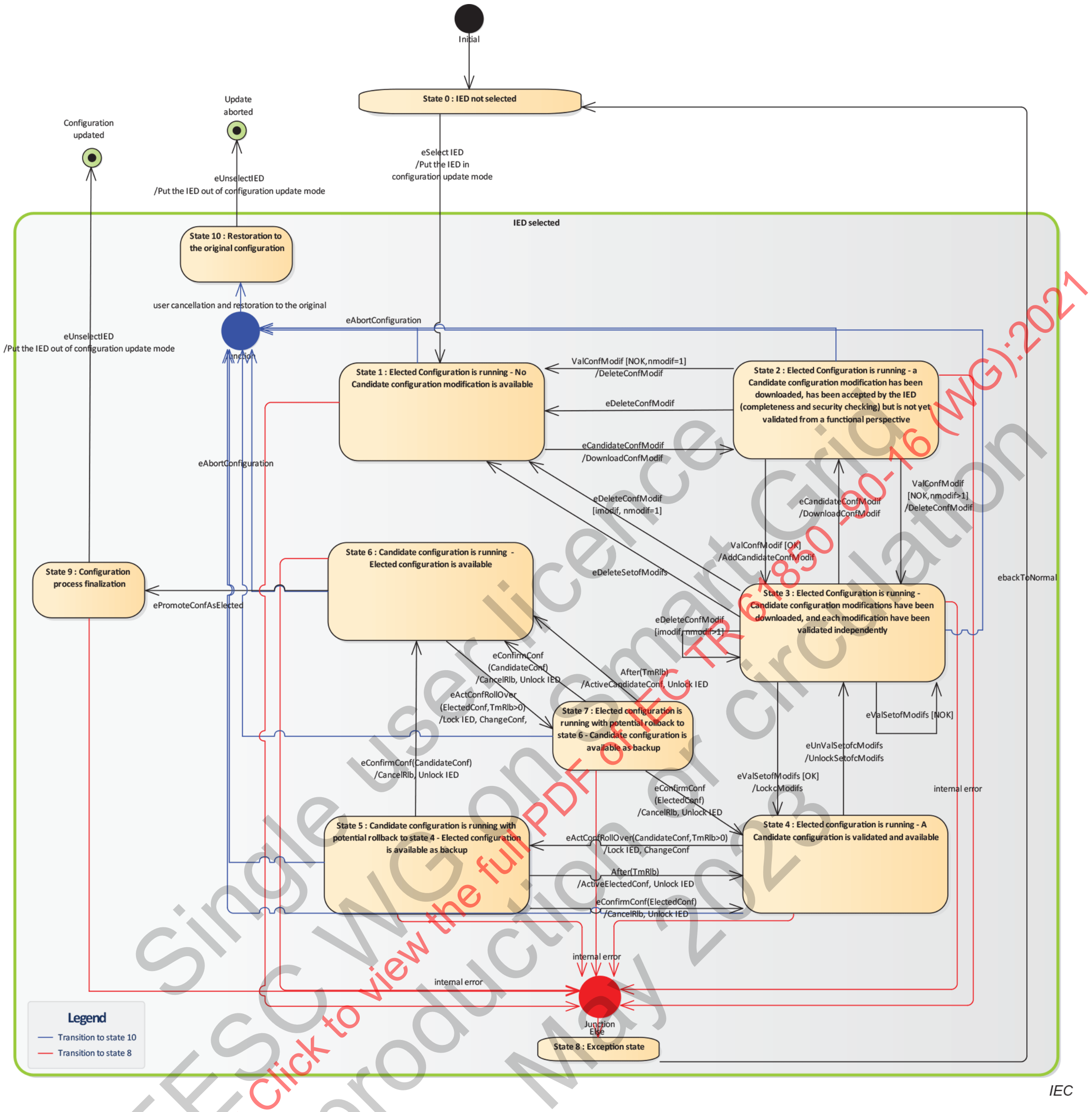

Initial
State 0 : IED not selected
Update aborted
Configuration updated
eSelect IED
/Put the IED in
configuration update mode
eUnselectIED
/Put the IED out of configuration update mode
IED selected
State 10 : Restoration to the original configuration
user cancellation and restoration to the original
eAbortConfiguration
Junction
eUnselectIED
/Put the IED out of configuration update mode
State 1 : Elected Configuration is running - No Candidate configuration modification is available
ValConfModif [NOK,nmodif=1]
/DeleteConfModif
eDeleteConfModif
eCandidateConfModif
/DownloadConfModif
State 2 : Elected Configuration is running - a Candidate configuration modification has been downloaded, has been accepted by the IED (completeness and security checking) but is not yet validated from a functional perspective
eAbortConfiguration
eDeleteConfModif
[imodif, nmodif=1]
eCandidateConfModif
/DownloadConfModif
ValConfModif
[NOK,nmodif>1]
/DeleteConfModif
ValConfModif [OK]
/AddCandidateConfModif
eDeleteSetofModifs
ebackToNormal
State 9 : Configuration process finalization
ePromoteConfAsElected
State 6 : Candidate configuration is running - Elected configuration is available
State 3 : Elected Configuration is running - Candidate configuration modifications have been downloaded, and each modification have been validated independently
eDeleteConfModif
[imodif, nmodif>1]
eConfirmConf
(CandidateConf)
/CancelRlb, Unlock IED
After(TmRlb)
/ActiveCandidateConf, Unlock IED
eActConfRollOver
(ElectedConf,TmRlb>0)
/Lock IED, ChangeConf,
State 7 : Elected configuration is running with potential rollback to state 6 - Candidate configuration is available as backup
eValSetofModifs [NOK]
eUnValSetofcModifs
/UnlockSetofcModifs
eConfirmConf(CandidateConf)
/CancelRlb, Unlock IED
eValSetofModifs [OK]
/LockcModifs
internal error
eConfirmConf
(ElectedConf)
/CancelRlb, Unlock IED
State 5 : Candidate configuration is running with potential rollback to state 4 - Elected configuration is available as backup
eActConfRollOver(CandidateConf,TmRlb>0)
/Lock IED, ChangeConf
State 4 : Elected configuration is running - A Candidate configuration is validated and available
After(TmRlb)
/ActiveElectedConf, Unlock IED
eConfirmConf(ElectedConf)
/CancelRlb, Unlock IED
internal error
internal error
Junction
Else
State 8 : Exception state
Legend
Transition to state 10
Transition to state 8
IEC

Figure 10 – Update and activate power system configuration state machine

Table 6 – Update and activate power system configuration state machine transitions

Name	Description	From state ...	To state ...
eSelectIED	An IED has been selected for receiving a new configuration.	0	1
eCandidateConfModif	A candidate modification has been made and is ready to be downloaded in the IED.	1	2
eDeleteConfModif	A candidate modification was deleted.	2	1
eDeleteSetofModifs	The whole set of modifications was deleted.	3	1
eValConfModif[OK]	A candidate configuration has been validated syntactically and semantically by the IED. This request could be made externally or automatically by the IED.	2	3
eValConfModif[NOK]	A candidate configuration validation (syntactically and semantically) by the IED failed. This candidate modification is deleted by the IED. This request could be made externally or automatically by the IED.	2	3

Name	Description	From state …	To state …
eValSetofModif[OK]	A validation of the consistency of the whole set of modification was made and confirmed by the IED.	3	4
eValSetofModif[NOK]	A validation of the consistency of the whole set of modification was made and was stated unsuccessful by the IED.	3	3
eUnvalSetofcModif	New modifications are desired, a request of unlocking the set of confirmed modification has been made.	4	3
ePromoteConfAsElected	The whole process of configuration modification was successful, the candidate configuration must become the default configuration and the available configuration must be deleted.	6	9
Event eActConfRollover(CandidateConf;TmRlb>0):	A request has been made to activate the CandidateConf. The TmRlb could be put to none for disabling the use of a timer.	4	5
Event eActConfRollover (ElectedConf;TmRlb>0)	A request has been made to activate the ElectedConf. The TmRlb could be put to none for disabling the use of a timer.	6	7
Event eConfirmConf (CandidateConf):	If the confirmation event comes in time for the CandidateConfiguration, the rollover is considered as successful and the timer for the rollback is stopped. (state 5 to 6) This request could be made externally or automatically by the IED.	5	6
Event eConfirmConf (ElectedConf):	If the confirmation event comes in time (before the end of the timer rollback) for the ElectedConfiguration, the rollover is considered as successful and the timer for the rollback is stopped. (state 7 to 4) This request could be made externally or automatically by the IED.	7	4
Event eConfirmConf (CandidateConf):	The rollover is considered as unsuccessful, the timer for the rollback is stopped and a rollback is made from the Elected Configuration to the Candidate Configuration. (state 5 to 4) This request could be made externally or automatically by the IED.	5	4
Event eConfirmConf (ElectedConf):	The rollover is considered as unsuccessful, the timer for the rollback is stopped and a rollback is made from the Candidate Configuration to the Elected Configuration. (state 7 to 6) This request could be made externally or automatically by the IED.	7	6
Event After(TmRlb):	If no confirmation comes in time, the running configuration switch to the previous one.	5	4
eAbortConfiguration	A request for aborting the configuration processus has been made.	1-7	10
eUnSelectIED	An IED has been unselected and put out of the configuration mode. This request could be made externally or automatically by the IED.	9	FINAL
eBackToNormal	Following an error, the IED get back to the state 0 where it is not selected. This request could be made externally or automatically by the IED.	8	0

6.2.3 SUC: Synchronize multiple automation-system-devices updates

6.2.3.1 Description of the use case

6.2.3.1.1 Name of use case

ID	Area(s)/Domain(s)/Zone(s)	Name of use case
61850-90-16 SUC2	Distribution Grid Management, Distribution Grid Management	Synchronize multiple automation-system-devices updates

6.2.3.1.2 Scope and objectives of use case

Scope	Only centralised synchronization is addressed in this use case
Objective(s)	Update FW and /or configuration of multiple IEDs of a system in an organized and synchronized way decided by the system operator
Related business case(s)	

6.2.3.1.3 Narrative of Use Case

Short description

Coordinate the updates, FW and/or configuration, of multiple IEDs, or group of IEDs, to operate a system. The updates can occur in the same substation, between substations, along a feeder.

Complete description

Using the DMIS, define a work program composed of different steps of configuration and/or FW update for an IED or group of IEDs, those steps are characterized by:

- An IED list
- A corresponding list of updates for those IEDs
- An update condition
  - Timeframe
  - External event as an opportunity (Scheduled or unplanned outage ...)
  - Device Management System internal event (Previous update successful ...)
- A failure mode
  - All or nothing (all IEDs should be updated successfully, if at least one fail the other switch back to their previous configuration)
  - Maximum update (The Device Management Information System try to update the maximum IEDs)
  - Stop at first failure (IEDs are updated following the sequence until one fails, then the sequence is stopped with no switch back for the IED successfully updated)

Example, the operator has defined the following work program (containing 3 steps) using the DMIS

Step 1	Update both the FW protection relay A and B in the same substation A
Work program plan and synchronize	
IED protection relay A @ substation A	FW 1.3.1.108 + current configuration
IED protection relay B @ substation A	FW 1.3.1.108 + current configuration
Update condition: Timeframe 03/11/2017 23:00:00	
Failure mode: Maximum	
Step 2	Update both protection relay (A and B) configuration in the main substation A as well as SCADA configuration
Work program plan and synchronize	
IED protection relay @ substation A	New configuration (Change in MinOpTmms)
IED protection relay @ substation A	New configuration (Change in MinOpTmms)
IED DSO regional SCADA	Update configuration (Change in MinOpTmms)
Update condition: Step 1 total success	
Failure mode: All or nothing	
Step 3	Update of the main substation automatic source transfer function
Work program plan and synchronize	
IED automatism	Update configuration (Change in AATS LN)
Update condition: Timeframe 04/11/2017 04:00:00	
Failure mode: All or nothing	

6.2.3.1.4 Use Case conditions

Assumptions	
1	Time-based synchronisation can only occur within a define timeframe and not at an exact time
2	The synchronization preparation, activation and supervision is managed centrally and not locally from a network operator perspective
3	The nature of the updates (FW and/or Configuration) to synchronize do not need to be identical: Ex: We can synchronize the update of a FW A on a group of IED with the update of a FW B and a Configuration 1 on another group.
Prerequisites	
1	An inventory of the automation systems devices is available: This inventory includes all the updatable devices (RTUs, IEDs) and the software and updates/upgrades/patches in use with the following information: • Asset owner • Device manufacturer • Make and model ID • HW version • FW version (boot code version, ...) • OS version (+ patches...) • SW versions • Fail and fault tolerance • Category or group • Installed and not installed updates • Interdependencies • Architecture and connectivity (How to deploy) • Criticality Ref. IEC TR 62443-2-3:2015, Annex B
2	Fully operational automation systems and telecommunication infrastructure (no downgraded scenario)

6.2.3.1.5 Further information to the Use Case for classification/mapping

Relation to other use cases
<<BUC>> Enable Automation Systems to perform operational functions in best conditions <<SUC>> Update automation-system devices configuration file and firmware
Nature of the use case
SUC

6.2.3.1.6 Diagrams of Use Case

Figure 11 and Figure 12 describe the use case "Synchronize multiple updates to automation devices" and its activity sequences.

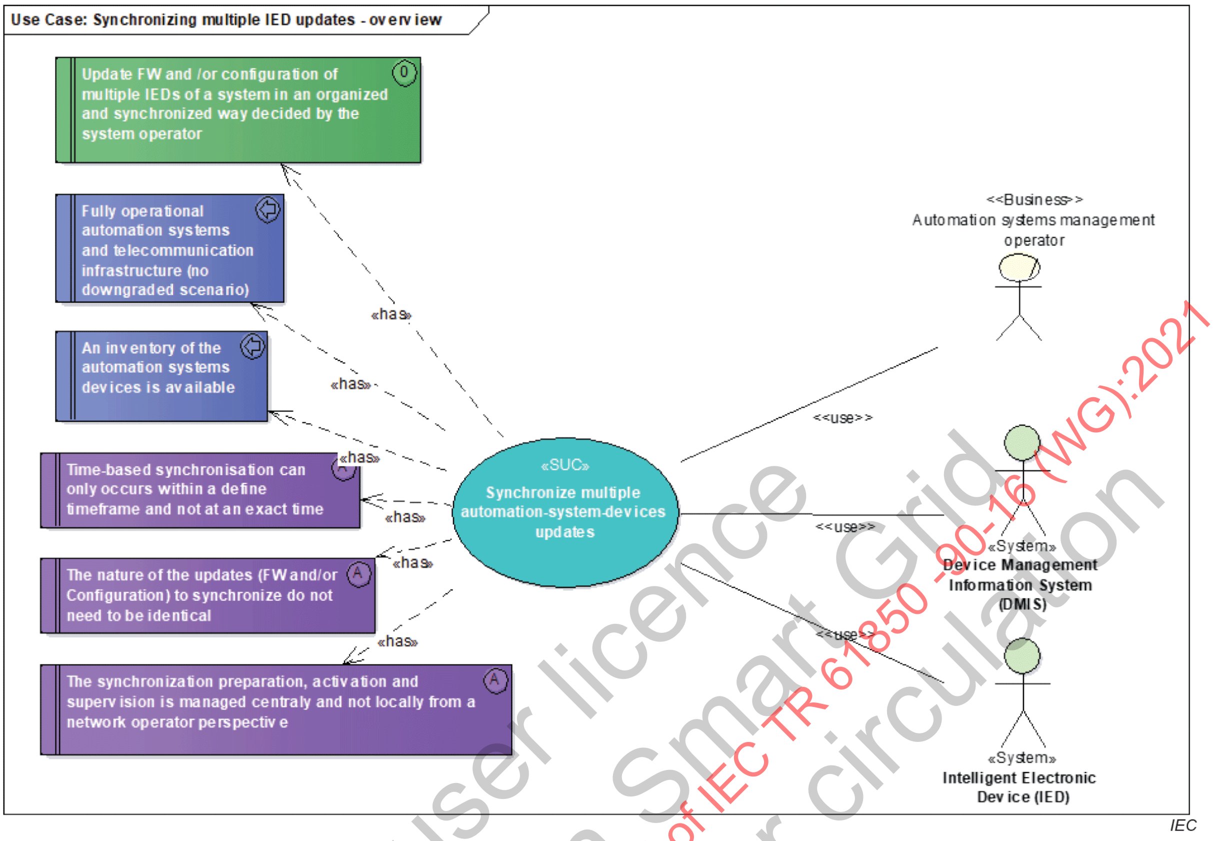

Use Case: Synchronizing multiple IED updates - overview
Update FW and /or configuration of multiple IEDs of a system in an organized and synchronized way decided by the system operator
0
Fully operational automation systems and telecommunication infrastructure (no downgraded scenario)
An inventory of the automation systems devices is available
Time-based synchronisation can only occurs within a define timeframe and not at an exact time
The nature of the updates (FW and/or Configuration) to synchronize do not need to be identical
A
The synchronization preparation, activation and supervision is managed centraly and not locally from a network operator perspective
A
«has»
«has»
«has»
«has»
«has»
«has»
«SUC»
Synchronize multiple automation-system-devices updates
<<use>>
<<use>>
<<use>>
<<Business>>
Automation systems management operator
«System»
Device Management Information System (DMIS)
«System»
Intelligent Electronic Device (IED)
IEC

Figure 11 – Overview of SUC: Synchronize multiple automation-system-devices updates

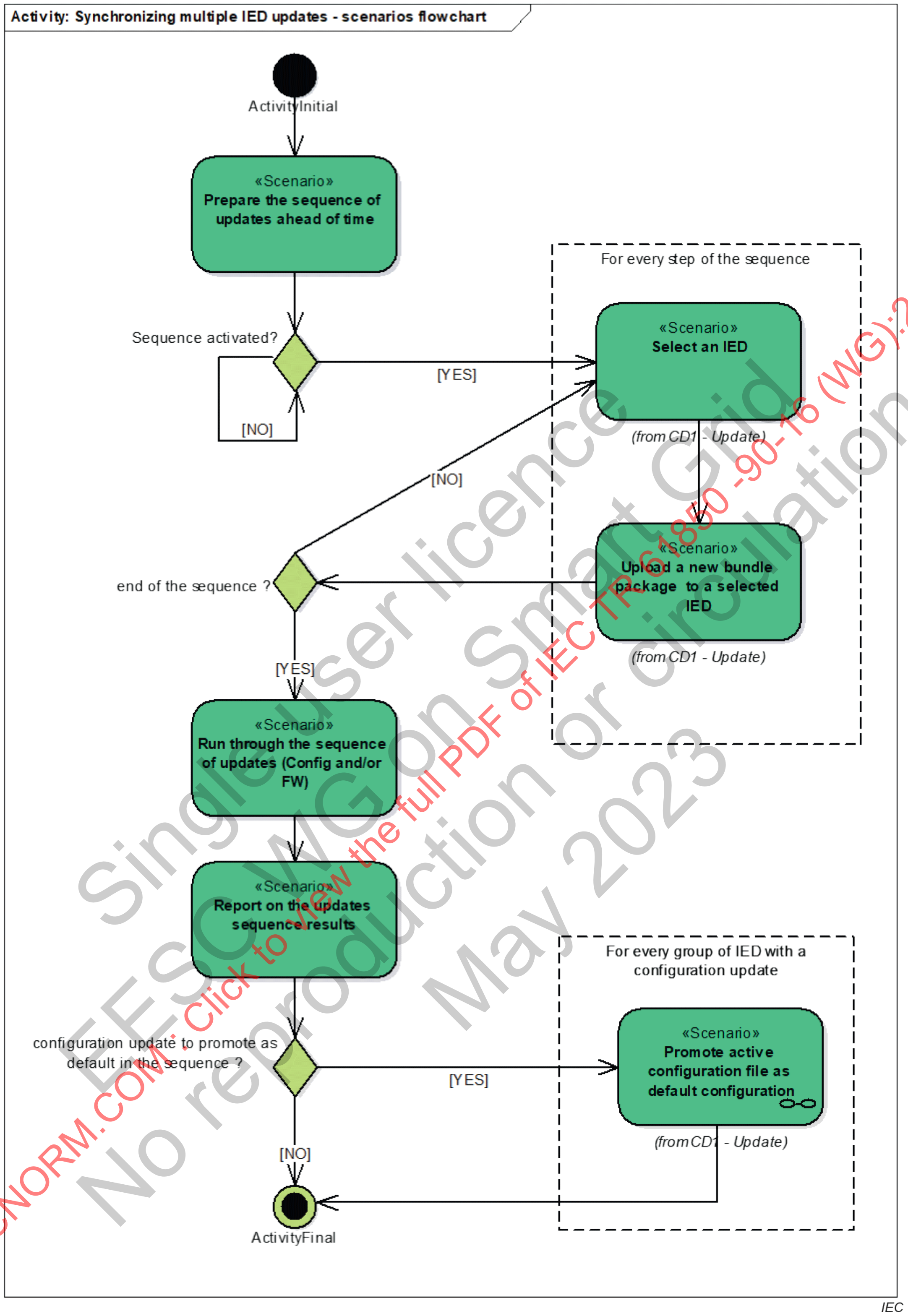

Activity: Synchronizing multiple IED updates - scenarios flowchart
ActivityInitial
«Scenario»
Prepare the sequence of updates ahead of time
Sequence activated?
[NO]
[YES]
For every step of the sequence
«Scenario»
Select an IED
(from CD1 - Update)
«Scenario»
Upload a new bundle package to a selected IED
(from CD1 - Update)
[NO]
end of the sequence ?
[YES]
«Scenario»
Run through the sequence of updates (Config and/or FW)
«Scenario»
Report on the updates sequence results
configuration update to promote as default in the sequence ?
[YES]
For every group of IED with a configuration update
«Scenario»
Promote active configuration file as default configuration
(from CD1 - Update)
[NO]
ActivityFinal
IEC

Figure 12 – Overview of SUC: scenario flow chart of "Synchronizing multiple IED updates"

6.2.3.2 Technical details

6.2.3.2.1 Actors

Actor name	Actor type	Actor description	Further information specific to this use case
Intelligent Electronic Device (IED)	System	See Table 3	
Device Management Information System (DMIS)	System	See Table 3	
Automation systems management operator	Business	See Table 2	

6.2.3.3 Step by step analysis of use case - Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Prepare the sequence of updates ahead of time	Ahead of time: • Identify the IED and groups of IED to update • Specify the update to realize (FW and/or CID) • Specify the condition (time, event) • Define the type of failure accepted (All or nothing, maximum update, stops at first failure…)	Grid operator	Multiple updates need		A sequence of updates is ready to launch
2	Run through the sequence of updates (Configuration and/or FW)	Run through the updates using 61850-90-16-SUC1 Deploy of a Power System Function	E2EO		A sequence of updates is ready to launch	End of sequence
3	Report on the updates sequence results	Produce a reporting on all the updates and steps of the sequence of updates	DMIS		End of sequence	Report produced on the updates sequence

6.3 Asset management, supervision and maintenance system Use Cases

6.3.1 System Use Cases identified

Collect data concerning the operational state of the equipment in order to be able to lead predictive analysis, launch maintenance actions and reduce failure probabilities.

The goal is to collect and transfer patrimonial data to the information systems in charge of asset management and maintenance.

Table 7 describes the system Use Cases that have been identified. The list is non-exhaustive and will be updated as new editions of THIS document are issued.

Table 7 – Identified asset management, supervision and maintenance System Use Cases

Index of the System Use cases	Identified System Use Cases	Brief description
61850-90-16-SUC3	Replace an IED of an automation-system with an identical one	Replace a complete faulty IED of an existing automation system with an identical IED HW. This replacement follows a maintenance or asset management decision. This Use Case covers the system management operation before, during and following this physical replacement Upgrading the hardware of a working IED, or predictive maintenance are out of scope
61850-90-16-SUC4	Store and provide electrical network asset information during its lifecycle	Along the lifecycle of an Electrical Network Asset (ENA), store its nameplate, location information, IDs of its software and hardware components as well as generate a Version Identifier and provide it for maintenance, asset management and supervision applications. Storing that information can be done through ENA communication capabilities or through an IED it is connected to acting as a proxy for that information.

6.3.2 SUC: Replace an IED of an automation-system with an identical one

6.3.2.1.1 Description of the Use Case

6.3.2.1.2 Name of Use Case

ID	Area(s)/Domain(s)/Zone(s)	Name of use case
61850-90-16-SUC3	Distribution Grid Management, Distribution Grid Management	Replace an IED of an automation-system with an identical one

6.3.2.1.3 Scope and objectives of Use Case

Scope	Replace a complete IED of an existing automation system with an identical IED HW. This replacement follows a maintenance or asset management decision. This Use Case covers the system management operation before, during and following this physical replacement. Upgrading the hardware of a working IED, or predictive maintenance are out of scope
Objective(s)	Ensure the replacement of an IED of an automation system by an identical IED with respect to its capabilities: Ensure the physical replacement of a complete IED of an existing automation system by an identical IED with respect to its capabilities (Expecting the exactly same behaviour): • exactly the correct configuration and/or firmware versions • persistence of all the persistent and cumulated data • settings including security management • certificates keys and RBAC permissions
Related business case(s)	

6.3.2.1.4 Narrative of Use Case

Short description
The new IED should have the same capabilities, it should be an identical IED HW and it should be set-up to ensure the same behaviour than the faulty one with respect to its capabilities. Retrieval mechanisms should ensure availability of the maximum level of information from the IED before it needs to be replaced (Use the complete log + incremental log through the DMIS or available to the DMIS to define the actual IED environment: configuration, FW, persistent data, settings ….)
Complete description
To be completed

6.3.2.1.5 Use Case conditions

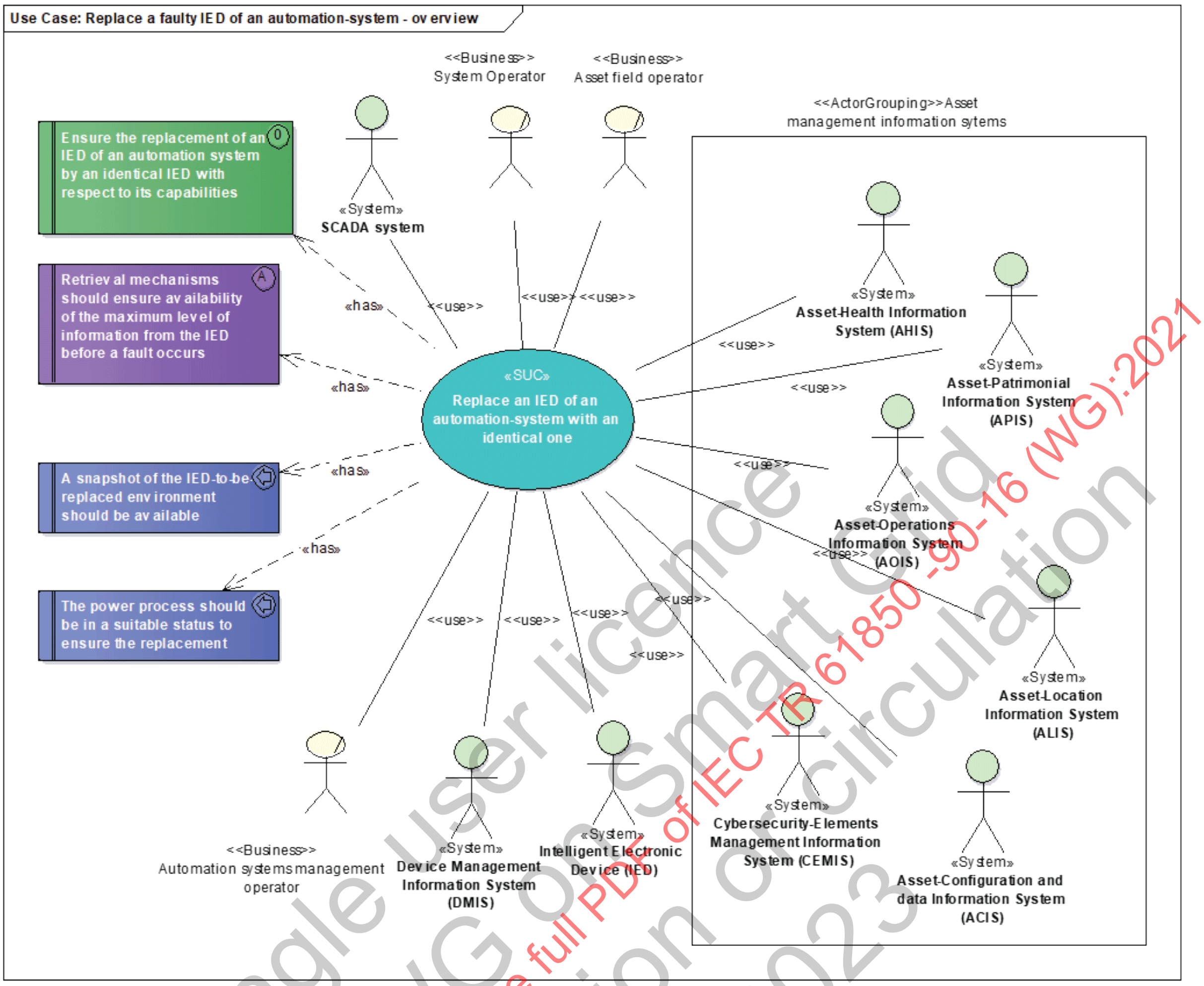
Assumptions	
1	Retrieval mechanisms should ensure availability of the maximum level of information from the IED before a fault occurs: The IED environment includes: • Configuration • FW • Settings • Persistent & cumulated data • Keys & certificates • RBAC permissions During the running life of an IED "snapshots" of this environment should be captured (see Use Case "Store and provide asset management information of an IED") on a regular basis and when key elements evolve”.
Prerequisites	
1	The power process should be in a suitable status to ensure the replacement: The process" should be in a suitable status to ensure the replacement: Safety mode. The Device Management Information System should know that the process is in a locked "safety mode"
2	A snapshot of the IED-to-be-replaced environment should be available: The snapshot of the IED-to-be-replaced environment should include a maximum of the following: • Configuration • FW • Settings • Persistent & cumulated data • Keys & certificates • RBAC permissions

6.3.2.1.6 Further information to the Use Case for classification/mapping

Classification information
Relation to other use cases
<<BUC>> Enable Automation Systems to perform operational functions in best conditions
Nature of the use case
SUC

6.3.2.2 Diagrams of Use Case

Figure 13 and Figure 14 represent the use of "Replace an IED of an automation system with an identical system" and behavior sequences.


Use Case: Replace a faulty IED of an automation-system - overview
Ensure the replacement of an IED of an automation system by an identical IED with respect to its capabilities
Retrieval mechanisms should ensure availability of the maximum level of information from the IED before a fault occurs
A snapshot of the IED-to-be-replaced environment should be available
The power process should be in a suitable status to ensure the replacement
«has»
«has»
«has»
«has»
«System»
SCADA system
<<Business>>
System Operator
<<Business>>
Asset field operator
<<use>>
<<use>>
<<use>>
«SUC»
Replace an IED of an automation-system with an identical one
<<ActorGrouping>>Asset management information sytems
«System»
Asset-Health Information System (AHIS)
«System»
Asset-Patrimonial Information System (APIS)
«System»
Asset-Operations Information System (AOIS)
«System»
Asset-Location Information System (ALIS)
«System»
Cybersecurity-Elements Management Information System (CEMIS)
«System»
Asset-Configuration and data Information System (ACIS)
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
<<Business>>
Automation systems management operator
«System»
Device Management Information System (DMIS)
«System»
Intelligent Electronic Device (IED)

IEC

Figure 13 – Overview of SUC: Replace an IED of an automation-system with an identical one

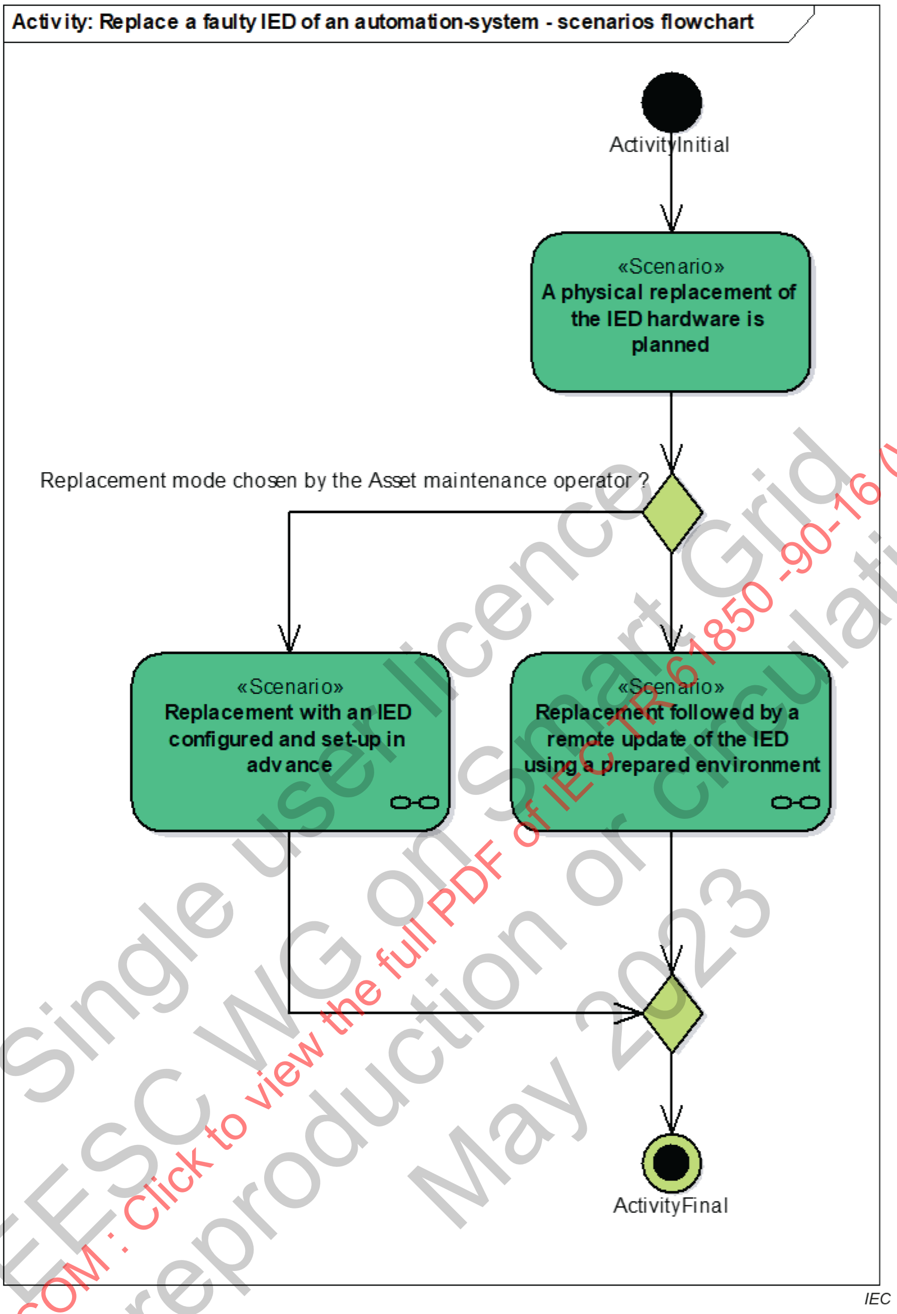

Activity: Replace a faulty IED of an automation-system - scenarios flowchart
ActivityInitial
«Scenario»
A physical replacement of the IED hardware is planned
Replacement mode chosen by the Asset maintenance operator ?
«Scenario»
Replacement with an IED configured and set-up in advance
«Scenario»
Replacement followed by a remote update of the IED using a prepared environment
ActivityFinal
IEC

Figure 14 – Scenario diagram of SUC: Replace an IED of an automation-system with an identical one

6.3.2.3 Actors

Grouping (e.g. domains, zones)		**Group description**	
Asset management information systems			
Actor name	**Actor type**	**Actor description**	**Further information specific to this use case**
Cybersecurity-Elements Management Information System (CEMIS)	System	See Table 3	
Asset-Patrimonial Information System (APIS)	System	See Table 3	
Asset-Operations Information System (AOIS)	System	See Table 3	
Asset-Health Information System (AHIS)	System	See Table 3	
Asset-Location Information System (ALIS)	System	See Table 3	
Asset-Configuration and data Information System (ACIS)	System	See Table 3	
System Operator	Business	See Table 2	
SCADA system	System	See Table 3	
Intelligent Electronic Device (IED)	System	See Table 3	
Device Management Information System (DMIS)	System	See Table 3	
Automation systems management operator	Business	See Table 2	
Asset field operator	Business	See Table 2	
Asset Maintenance Operator	Business	See Table 2	

6.3.2.4 Step by step analysis of use case - Overview of scenarios

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	A physical replacement of the IED hardware is planned	Following maintenance and supervision process an IED is identified as faulty, the Asset Maintenance operator plans to send a field operator to physically replace the IED hardware. Results of this planning are available to the System operator as well as IED system management operator. A replacement mode is chosen: • Replacement with an IED configured and set-up in advance • Replacement followed by a remote update of the IED using a prepared environment	Asset Maintenance Operator	Maintenance and supervision process identifying IED as faulty		A replacement mode is chosen

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
2	Replacement followed by a remote update of the IED using a prepared environment	Following the physical replacement of the IED a remote update is performed with an IED environment including: • FW • Configuration • Settings • Permanent and cumulated data • Cybersecurity elements (Keys, Certificates, RBAC permissions)	DMIS	Physical replacement of the IED		IED installed and configured
3	Replacement with an IED configured and set-up in advance	The IED has been prepared previous to the physical replacement by the Asset Maintenance Operator and/or Field Operator: • FW update • Configuration update • Settings • Update of the permanent and cumulated data • Cybersecurity elements update	DMIS	Physical replacement of the IED	IED has been prepared previous to the physical replacement	IED installed and configured

6.3.3 SUC: Store and provide electrical network asset information during its lifecycle

6.3.3.1 Description of the Use Case

6.3.3.1.1 Name of Use Case

ID	Area(s)/Domain(s)/Zone(s)	Name of use case
61850-90-16-SUC4	Distribution Grid Management, System Management	Store and provide electrical network asset information along its lifecycle

6.3.3.1.2 Scope and objectives of Use Case

Scope	This Use Case covers Electrical Network Assets (ENA) with communication capabilities or not The ENA can be connected to IEDs or IEDs themselves ENA are located on the electrical grid from generation to customer premises. As an example it can include sensors, protections, reclosers, inverters, automation system devices, telecommunication devices or cybersecurity devices. This Use Case address 4 main asset information or information sub-set: • The ENA, as a hardware, identifier such as a Nameplate (ENA-N) • The ENA Location information (GPS coordinate, localisation code …) (ENA-L) • The ENA hardware and software COmponents IDs (ENA-COID) • The ENA Version IDentifier (ENA-VID) generated from components identifier, configuration identifiers and location information and use for logging and tracking changes, consistency check… The ENA hardware and software components can be considered as ENA themselves in a recursive structure Hardware can include: sensors, electronic board, antennas, power supply (main and back-up), box, LEDs, switches … Software can include: firmware (as a whole or as modules), configuration, and set of parameters …
Objective(s)	Ensure a reliable, up to date and complete knowledge of one's network assets components and location along its lifecycle
Related business case(s)	

6.3.3.1.3 Narrative of Use Case

Short description
Along the lifecycle of an Electrical Network Asset (ENA), store its nameplate, location information, IDs of its software and hardware components as well as generate a Version Identifier and provide it for maintenance, asset management and supervision applications. Storing that information can be done through ENA communication capabilities or through an IED it is connected to acting as a proxy for that information.

6.3.3.1.4 Key performance indicators (KPI)

ID	Name	Description	Reference to mentioned use case objectives
1	Completeness and quality of the SW and HW IDs for every ENA		Ensure a reliable, up to date and complete knowledge of one's network assets components and location along its lifecycle
2	Completeness and Quality of the Version Identifier for every ENA		
3	Completeness and quality of the nameplate ID for every ENA		
4	Completeness and quality of the location data for every ENA		

6.3.3.1.5 Use case conditions

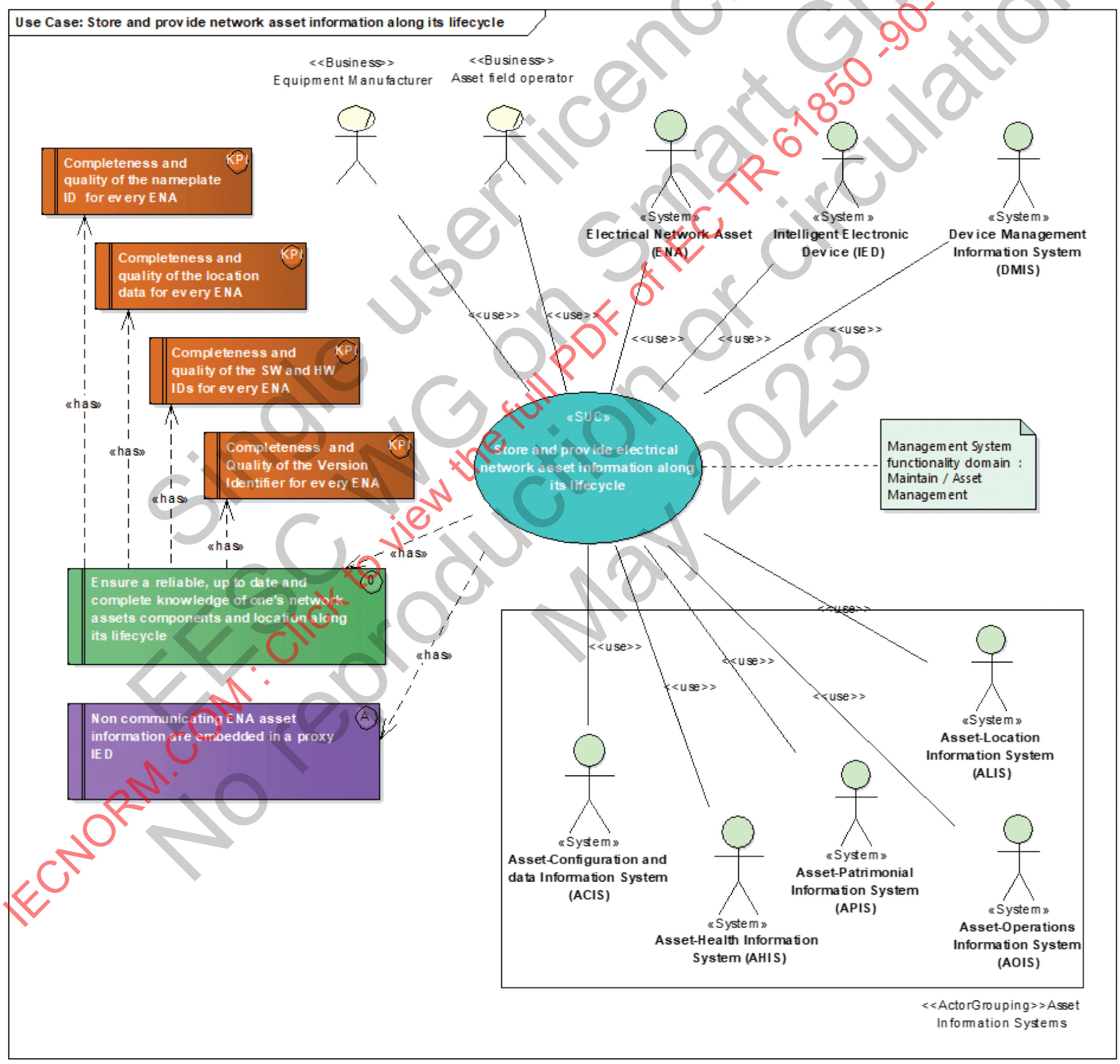
	Assumptions
1	Non communicating ENA asset information are embedded in a proxy IED: For non-communicating Electrical Network Asset, their asset information is embedded and available in an IED connected to the ENA, if this IED exist. This IED is known as Proxy-IED for asset information

6.3.3.1.6 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
<<BUC>> Enable Automation Systems to perform operational functions in best conditions <<SUC>> Ensure the asset reference trustability <<SUC>> Ensure consistency in between asset databases and assets in the field
Nature of the use case
SUC

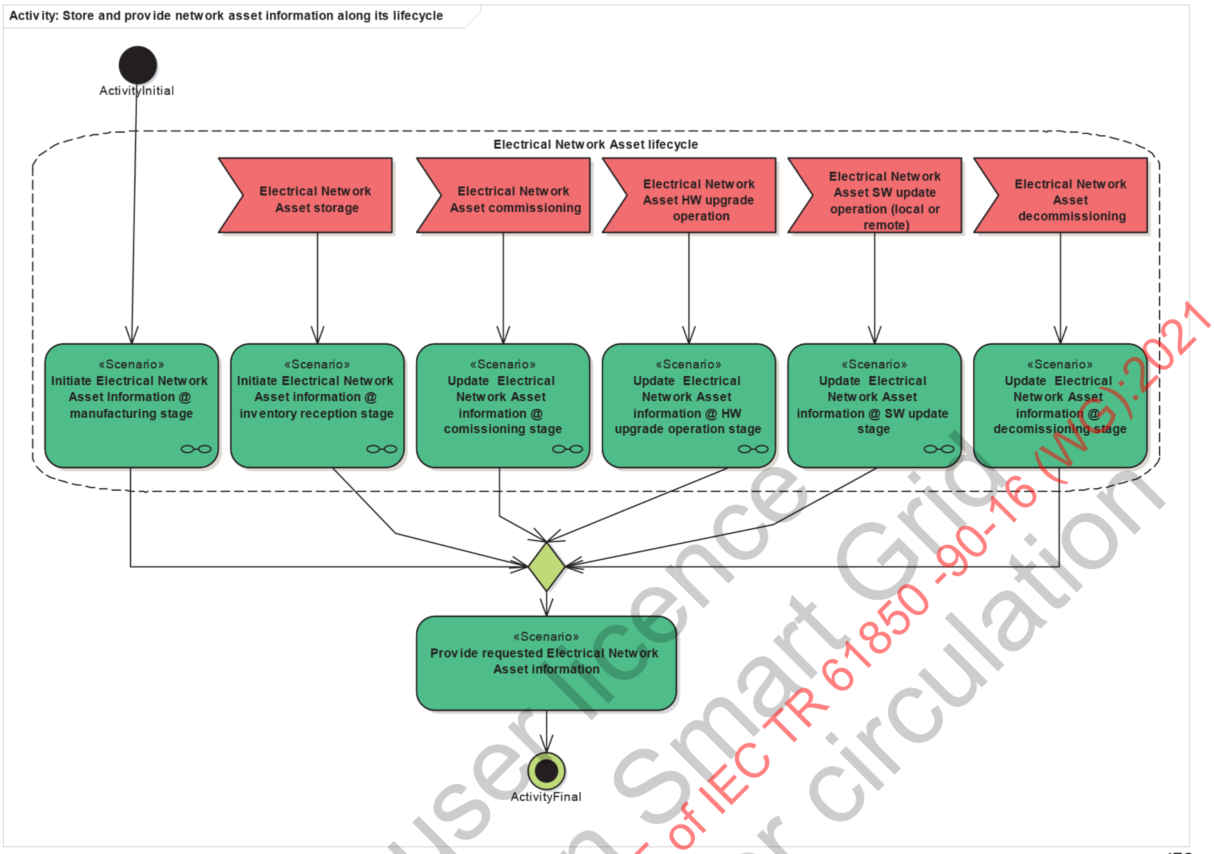
6.3.3.2 Diagrams of use case

Figure 15, Figure 16 and Figure 17 illustrate the management of information and activity of the electrical grid during its life cycle.



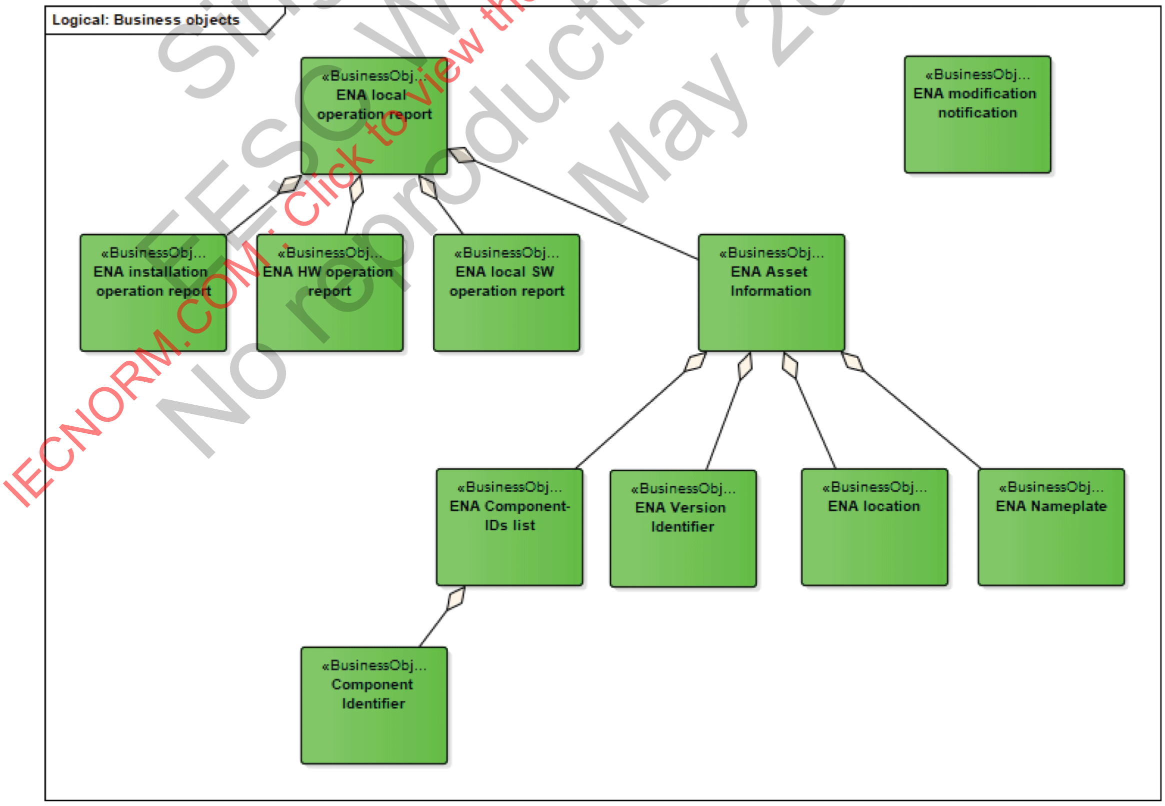
Use Case: Store and provide network asset information along its lifecycle
<<Business>> Equipment Manufacturer
<<Business>> Asset field operator
«System» Electrical Network Asset (ENA)
«System» Intelligent Electronic Device (IED)
«System» Device Management Information System (DMIS)
Completeness and quality of the nameplate ID for every ENA
KPI
Completeness and quality of the location data for every ENA
KPI
Completeness and quality of the SW and HW IDs for every ENA
KPI
Completeness and Quality of the Version Identifier for every ENA
KPI
«has»
«has»
«has»
«has»
«has»
«has»
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
«SUC» Store and provide electrical network asset information along its lifecycle
Management System functionality domain : Maintain / Asset Management
Ensure a reliable, up to date and complete knowledge of one's network assets components and location along its lifecycle
O
Non communicating ENA asset information are embedded in a proxy IED
A
<<use>>
<<use>>
<<use>>
<<use>>
<<use>>
«System» Asset-Location Information System (ALIS)
«System» Asset-Configuration and data Information System (ACIS)
«System» Asset-Health Information System (AHIS)
«System» Asset-Patrimonial Information System (APIS)
«System» Asset-Operations Information System (AOIS)
<<ActorGrouping>>Asset Information Systems
IEC

Figure 15 – Overview of SUC: Store and provide electrical network asset information during its lifecycle


Activity: Store and provide network asset information along its lifecycle
ActivityInitial
Electrical Network Asset lifecycle
Electrical Network Asset storage
Electrical Network Asset commissioning
Electrical Network Asset HW upgrade operation
Electrical Network Asset SW update operation (local or remote)
Electrical Network Asset decommissioning
«Scenario» Initiate Electrical Network Asset Information @ manufacturing stage
«Scenario» Initiate Electrical Network Asset information @ inventory reception stage
«Scenario» Update Electrical Network Asset information @ comissioning stage
«Scenario» Update Electrical Network Asset information @ HW upgrade operation stage
«Scenario» Update Electrical Network Asset information @ SW update stage
«Scenario» Update Electrical Network Asset information @ decomissioning stage
«Scenario» Provide requested Electrical Network Asset information
ActivityFinal

IEC

Figure 16 – Scenario diagram of SUC: Store and provide electrical network asset information during its lifecycle


Logical: Business objects
«BusinessObj... ENA local operation report
«BusinessObj... ENA modification notification
«BusinessObj... ENA installation operation report
«BusinessObj... ENA HW operation report
«BusinessObj... ENA local SW operation report
«BusinessObj... ENA Asset Information
«BusinessObj... ENA Component-IDs list
«BusinessObj... ENA Version Identifier
«BusinessObj... ENA location
«BusinessObj... ENA Nameplate
«BusinessObj... Component Identifier

IEC

Figure 17 – Asset information business objects

6.3.3.3 Actors

Grouping (e.g. domains, zones)		Group description	
Asset Information Systems			
Actor name	**Actor type**	**Actor description**	**Further information specific to this use case**
Asset-Configuration and data Information System (ACIS)	System	See Table 3	
Asset-Health Information System (AHIS)	System	See Table 3	
Asset-Patrimonial Information System (APIS)	System	See Table 3	
Asset-Operations Information System (AOIS)	System	See Table 3	
Asset-Location Information System (ALIS)	System	See Table 3	
Equipment Manufacturer	Business	See Table 3	
Intelligent Electronic Device (IED)	System	See Table 3	
Device Management Information System (DMIS)	System	See Table 3	
Electrical Network Asset (ENA)	System	See Table 3	
Asset field operator	Business	See Table 2.	

6.4 Cybersecurity system Use Cases for system management

6.4.1 System Use Cases identified

Table 8 provides a list of security Use Cases that are applicable to system management. The table organizes these system Use Cases as:

Index of the system Use cases	Identified system Use Cases
61850-90-16-SUC5	Initial Establishment of Security of System Management (System Management) Components
61850-90-16-SUC6	Validate the security of new IEDs (Sub-Use Cases)
61850-90-16-SUC7	Validate security of proposed security and non-security updates to IEDs (Sub-Use Cases)
61850-90-16-SUC8	Validate and Update RBAC Permissions and Roles for IEDs (Sub-Use Cases)
61850-90-16-SUC9	End-of-Life security

The sub-use cases are expected to be embedded into the functional Use Cases as they are developed.

NOTE this embedding of security use cases into functional Use Cases has not been attempted yet.

For each use case, the table includes:

- Brief description of the Use Case
- Actors
- Information exchanges
- Security discussion and basic steps

Each use case will be elaborated in Enterprise Architect and some examples are included, but not all have been so described yet.

Table 8 – List of cyber security Use Cases

Use Case brief description	Roles	Information exchanges	Security discussion and basic steps
61850-90-16-SUC5 Initial Establishment of Security of System Management (System Management) Components			
Implement and validate security systems, security-related databases, and security applications	• Vendor of Security products • Certificate Authority • Security Systems • Security Databases • Security Applications • RBAC Permissions Repository • OCSP Revocation System • User-to-Role Database • Active-X, LDAP, etc. • XACML Application	• Certificates • Security tokens • Certificate revocation lists • Security logs • Security application data • Defined Roles • RBAC initial permissions for each type of data • RBAC initial assignment of Roles to Permissions for each type of data	This initial security process is out of scope for these System Management use cases since it covers far more than just System Management, but is recognized as necessary. Some specific security systems and databases are identified
6.4.1.1 Establish secure networks for exchanging data securely between System Management components	• Network components • System Management Systems • System Management Databases • System Management Applications • Communication protocols	• Test networks for assuring the desired security level of data access • Test authorization for creating an association	This process is also out of scope since network security is more extensive than System Management. Secure networks, protocols with authentication and authorization, network monitoring, etc. need to be established for exchanging data between System Management systems, databases, and applications.
6.4.1.2 Implement and establish security of the system management (System Management) systems, databases, and applications	• Vendors of System Management products • Certificate Authority • Owners of System Management Systems • Owners of System Management Databases • Owners of System Management Applications • All stakeholders who participate in System Management (see IEC TR 61850-90-16 Actors)	• Certificates • Security tokens • Data to/from databases • Application data • Trust establishment • Establish ID to Certificate methodology	All systems, databases, and applications involved in system management must have certificates (or other security tokens), originally from the vendors and chained to the owners once installed. All stakeholders must be validated, authorized for their roles, and their trust established

Use Case brief description	Roles	Information exchanges	Security discussion and basic steps
6.4.1.3 Determine all types of information that will require consistency and conformance validation before being updated to IEDs	• List of IEDs with associated types of firmware and software • Types of Information (firmware, software, settings, security tokens, etc.) requiring conformance validation • Types of information requiring consistency validation • Databases with sources of information used for consistency and conformance validation	• For each type of information, provide location of source, what aspects must be validated, and other validation issues.	For all information that may be uploaded to an IED (firmware, software, SCL/SCD files, functions/logic, settings, security certificates or tokens, etc.), some source of validation needs to be provided. These sources may be located in any one of many systems or even remotely (e.g. vendor or CA). The type of validation should also be provided, such as matching code, values within specified ranges, cryptographic data integrity verification, authorization for upload, positive test results, etc. This Use Case will need to be expanded into multiple sub use cases to reflect the different types of validation and different sources for such validation.
6.4.1.4 Establish initial RBAC permissions for data in System Management systems, databases, and applications	• Vendors of System Management products • Owners of System Management Systems • Owners of System Management Databases • Owners of System Management Applications • RBAC Permissions Repository • Areas of Responsibility (AOR) • Operational States • Repository of types of IEDs (based on its functionality and permissions to interact with other IEDs)	• Permissions for each type of database • Permissions for services on databases • Permissions for different types of data within databases • Permissions for applications • Permissions for each type of data in different IEDs • AOR criteria • Operational State criteria	Permissions have been already established for each role. (The establishment of these role permissions is external to this process). Also have established the IED rights for each type of IED and each type of IED data. Permissions are also associated with System Management databases and applications as well as data in IEDs. They are first established in the RBAC Repository before being uploaded to IEDs. Permissions are also associated with Areas of Responsibility and Operational States. See IEC 62351-8 and IEC 62351-90-1. Permissions include: • VIEW permission • READ permission • DATASET permission • REPORTING permission • FILEREAD permission • FILEWRITE permission • CONTROL permission • CONFIG permission • SETTINGGROUP permission • FILEMNGT permission • SECURITY permission

Use Case brief description	Roles	Information exchanges	Security discussion and basic steps
6.4.1.5 Establish System Management Roles and associate them with permissions with all of the System Management components	• All System Management stakeholder roles • Owners of System Management Systems • Owners of System Management Databases • Owners of System Management Applications • Security role	• XACML files for role-to-permissions • Other techniques for establishing role-to-permissions via Allow/Deny rights	System management roles must also be established. It is "assumed" that the requirements for role-to-permissions have already been determined by the Owner's organization for access to System Management components. Typical permissions for the 90-16 actors will be identified. The association of individuals to System Management roles is out-of-scope.
6.4.1.6 Test system management components for functionality and for security of the process	• All System Management stakeholder roles • Owners of System Management Systems • Owners of System Management Databases • Owners of System Management Applications • Security role	• Test information exchanges according to the test procedures	Testing of the system management process must be undertaken, including the cyber security aspects.
6.4.1.7 Monitor the security of the information exchanges and periodically retest the system management components for functionality and for security of the process	• All System Management stakeholder roles • Owners of System Management Systems • Owners of System Management Databases • Owners of System Management Applications • Security role	• Monitor the security of the information exchanges, using Intrusion Detection, SNMP and other security measures • Monitor the sources of validation to ensure they have not had any unauthorized modifications • Test information exchanges according to the test procedures	Testing of the system management process must be undertaken, including the cyber security aspects.
IEC 61850-90-16-SUC6 Validate the security of new IEDs			
6.4.1.8 Manufacturer manufactures a new IED (see 6.4.2.2)	• Manufacturer • Newly created IED • Components to be inserted in the IED • Code: firmware, software in each component (card, memory module, etc.) • MRID for the IED and for each component • Manufacturer certificates with private key • Tools for creating MRIDs and for digitally signing code	• Registering of all assigned MRIDs • Digital signing of all software and firmware code • Manufacturer certificate public key	• A new IED is manufactured and its hardware components are installed • A permanent, global, and unique MRID of the new IED is created and stored in its TPM chip upon first booting up as per IEC 62443-3-3 and IEC 62443-4-2 • Each component within the IED is given an MRID which is stored securely • MRIDs are registered with manufacturer • Software and firmware codes are loaded and updated using the manufacturer certificate for authentication • All codes are digitally signed by the manufacturer as per IEC 62443-3-3 and IEC 62443-4-2 and IEC 62351-10

Use Case brief description	Roles	Information exchanges	Security discussion and basic steps
6.4.1.9 New owner purchases new IED and places it in a warehouse (see clause 6.4.2.3)	• Owner's IED Manager • New IED with MRID • Manufacturer certificate (may or may not be used for utilities who may just apply their own self-signed certificates) • Code: firmware, software in each component (card, memory module, etc.) • Physical Asset QR or RFID • Registry of MRIDs	• Digitally signed code (manufacturer verifies that the code has not been tampered with) • QR or RFID	• Manufacturer verifies all codes are digitally signed and are valid • Owner's IED Manager uses QR or RFID to validate and register the IED hardware as stored in warehouse • Owner's IED Manager registers all MRIDs of the IED and for each component
6.4.1.10 Owner updates and tests the new IED before placing in the field	• User in the testing role (tester) • New (or warehoused) IED • Manufacturer certificate (may or may not be used for utilities who may just apply their own self-signed certificates) • Digitally signed code for all software and firmware for each component (card, memory, etc.) • Certificate Authority (Public or Private) • OCSP • Physical Asset QR or RFID • Registration tool for new IED (e.g. Bootstrapping Remote Secure Key Infrastructure (BRSKI))	• Validation that the digitally signed code has not been tampered with. • Apply well-defined, trusted ID to new IED (field ID) and securely (signed) association with the existing certificates • Possibly certificate with attribute used as secure ID • Manufacturer certificate (if used) • PKI using EST and/or SCEP for certificate(s): private owner certificate, test public certificate (valid for say 60 days), public CA certificate for test public certificate • Registration record	• Tester verifies new IED with QR or RFID • Tester verifies with manufacturer (tool) that digitally signed code has not been tampered with • Tester uses IEC 62351-9 EST and/or SCEP to install certificates (private owner certificate, test public certificate, public CA certificate for test public certificate) • Tester checks all certificates against a CRL or an OCSP • Tester registers new IED in asset database as under test • (Tester updates any code, adds digital signatures for code if locally updated, and performs all functional tests) • Tester performs all security tests, e.g. RBAC settings
6.4.1.11 Enter security information about new IED in System Management system	• New IED with MRID • New IEC components with MRIDs • Registry of MRIDs • Asset management database(s) containing the list of operational IEDs which can keep these independent types of identity linked over time. • Security management database(s) • Security manager	• IED information • Security information for IED	• Security manager updates the database containing list of operational IEDs to include the MRIDs of the new IED and its components • Security manager updates other security databases to include the security information of the new IED • Multiple owners may have different non-persistent IDs and/or different security information

Use Case brief description	Roles	Information exchanges	Security discussion and basic steps
6.4.1.12 Owner places new IED in the field	• New IED • Security manager • Registry of MRIDs • Installer	• MRIDs and other security information for the new IED	• Security manager/installer verifies the MRIDs of the new IED and its components • Security manager/installer ensures that the new IED has not been tampered with between the lab testing and installation in the field
6.4.1.13 Verify the security of the telecommunication network	• New IED • Telecommunications network • Security manager of telecommunications network	• Security information for telecommunications network	• Security manager tests the telecommunications networks to assure that it meets the desired security level for access to the new IED
6.4.1.14 Owner commissions the new IED for operation in the field	• User in commissioning role (commissioner) • Commissioning tools • Tested IED with defined and trusted ID • Digitally signed code for all software and firmware for each component, updated during testing if necessary • Certificate Authority (Public or Private) • OCSP • Physical Asset QR or RFID	• QR or RFID information • ID of tested IED • Operational certificate with attribute used as secure ID	• Commissioner verifies new IED with QR or RFID • Commissioner verifies with manufacturer (tool) and/or tester that digitally signed code has not been tampered with • Commissioner removes the testing public certificate and its public CA certificate, and replaces it with operational public certificate (valid for say 3 to 10 years) and the public CA that certifies the validity of the public certificate • Commissioner uses IEC 62351-9 EST or SCEP to install certificates (private owner certificate, test public certificate, public CA certificate for test public certificate) • Commissioner checks all certificates against an OCSP • Commissioner registers new IED in asset database as in operation
IEC 61850-90-16-SUC7 Validate security of proposed security and non-security updates to IEDs			
6.4.1.15 Verify that selected IED is the correct IED for being updated	• Selected IED • List of IEDs Database • Security manager	• ID of selected IED • List of IDs of IEDs to update • Security information, such as certificates	Ensure that the selected IEDs is the correct IED to be updated
6.4.1.16 Validate existing security elements in the selected IED, such as certificates, passwords, and security software	• Selected IED • Security manager • Security tools	• Test scenario exchanges to validate existing security in the selected IED	Ensure that the selected IED has all security aspects up to date, such as certificates