Protection and control devices – Cyber security requirements

This global standard defines the cyber security requirements for protection and control devices used in the distribution substations with declared fundamental frequency of 50 Hz or 60 Hz.

Countries I&N	Elaborated by	Collaborations by	Verified by	Approved by
Argentina	-	-	-	**Emilio Jimenez**
Brazil	-	-	-	**Amadeu F. De Macedo**
Chile	-	-	-	**Daniel González**
Colombia	-	-	-	**Juan Gómez**
Iberia	-	-	-	**Maria Avery**
Italy	-	-	**L. Delli Carpini**	**Gianluca Sapienza**
Peru	-	-	-	**Robert Sánchez**
Romania	-	-	-	**Vasilica Obreja**

	Elaborated by	Collaborations by	Verified by	Approved by
Global I&N – NT&I	**D. García Miralles G. Fiorenza**	**M. Gaban**	**G. Fiorenza G. Scrosati**	**F. Giammanco**

Revision	Date	List of modifications
01	06.12.2018	First approved edition
02	28.07.2020	Second edition

LIST OF MODIFICATIONS OF CURRENT EDITION

Concerning the previous version of the global standard the following modifications has been applied:

- Included in the scope of the work the device **Protection and control device for HV/MV substation – Multifunctional Transformer protection (MTP).**

- New “documentary requirements” chapter has been added with the scope to get cyber security technical documentation from Vendors (according to SR_DC_01), during Tenders.

- Annex 1 about **Security Configurations API** has been added, providing API REST details for device managemen (SR_SW_05 and SR_SW_06).

- The following cyber security **Hardware** requirements have been added:

  Mandatory

  - Increased minimum product longevity to 10 years (SR_HR_02)
  - Industrial grade components (SR_HR_03)
  - Full CPU support of encryption security protocols (SR_HR_06)
  - Secure boot (SR_HR_07)
  - Hardware block for normally not used interfaces or not requested (SR_HR_08)
  - Syslog Security events when tamper detection occurs (SR_HR_11)
  - PCB silk-screen omission (SR_HR_16)

  Optional

  - Minimum computational resources requested: memory support (SR_HR_04)
  - Paint seal or label on screws (SR_HR_13)
  - Tamper detection and response solutions (SR_HR_14)
  - Epoxy encapsulation or resin coating of the components (SR_HR_19)
  - Monitoring circuits for power supply modules (SR_HR_20)

- The following cyber security **Software** requirements have been included:

  Mandatory

  - Interactive Boot features disabling (SR_SW_01)
  - Cryptographic Keys and related x509v3 Digital Certificates (SR_SW_04, 31 and 32)
  - Remote management functionalities and requirements (SR_SW_05, 06 and 30)
  - Security guidelines for software development (SR_SW_07)
  - Centralized authentication protocols Radius and LDAP/LDAPs (SR_SW_11 and 27)
  - New security loggings and requirements (SR_SW_08 and 17)
  - Hardcode credentials not allowed (SR_SW_26)
  - Trusted Execution Environment (SR_SW_31)

Optional

- Minimum computational resources for security events: memory (SR_SW_18bis)
- Referement development communities for OS (SR_SW_02bis)

INDEX

1 ACRONYMS 6

2 SCOPE OF THE WORK 7

3 REFERENCES 8

3.1 FOR ALL COUNTRIES 8

3.2 FOR EU COUNTRIES 8

4 REPLACED STANDARDS 8

5 DOCUMENT PURPOSE AND BACKGROUND 9

6 IED CYBER SECURITY REQUIREMENTS DESCRIPTION 10

7 IED HARDWARE CYBER SECURITY REQUIREMENTS 10

7.1 HARDWARE ARCHITECTURE 10

7.1.1 Hardware Platform 10

7.1.2 Security-specific functions 11

7.1.3 Interfaces and physical ports/connectors security 11

7.2 HARDWARE SOLUTIONS 12

7.2.1 Anti-intrusion mechanisms 12

7.2.2 Concealment of the components 13

7.2.3 Power supply control 14

7.2.4 Hardware Performances 14

8 IED FIRMWARE CYBER SECURITY REQUIREMENTS 15

8.1 FEATURES OF THE OPERATING SYSTEM 15

8.1.1 Bootloader 15

8.1.2 Operating System 15

8.2 MIDDLEWARE COMPONENTS 17

8.2.1 Remote Management functionalities of the device 17

8.2.2 Security of the Software code developed by the Supplier 18

8.2.3 Required Security Software 19

8.2.4 Remote Management Software 20

8.3 HARDENING 20

8.3.1 Hardening Guideline 20

8.3.2 Security Logging 21

8.4 SECURITY PATCHING 23

8.4.1 Updates during the IED supply 23

8.4.2 Security updates during the IED operation 23

8.4.3 Update Security 25

8.5 USERS, CREDENTIALS AND CERTIFICATES MANAGEMENT 25

8.5.1 Credentials Security 25

8.5.2 Centralized authentication 26

8.5.3 Update of certificates and cryptographic keys 26

8.5.4 Techniques for the protection of the administrative access to the device 26

8.5.5 Certificates and Cryptographic Key 27

9 DOCUMENTARY REQUIREMENTS 28

9.1 DETAILED TECHNICAL DOCUMENTATION TO BE PROVIDED 28

9.1.1 Required technical details 28

10 CYBER SECURITY REQUIREMENTS BIDDING FORM 29

11 ANNEX 1 - SECURITY CONFIGURATIONS API 31

GENERAL INFORMATION 31

XWS authentication 31

Activation and deactivation of the service ssh *32*
Public Keys addiction and removal in "authorized keys" *33*
Identification of the users enabled for the service *33*
NETWORK SERVICES CONFIGURATION 34
FIREWALL SERVICE 35
Activitation and deactivitation of the firewall service *35*
bulk download or bulk upload of iptables rules configuration file *35*
CREDENTIALS/KEYS SERVICE 35
Bulk Download *35*
Web server users *37*
Upload update and get of Cryptographic Keys and Digital Certificates *37*
SYSLOG SERVICE 39
Configuration *39*
Log download *39*
SysLog configuration download *40*
SYSTEM FUNCTIONS 40
POST HTTPS://<HOSTNAME>:<PORT>/SECURITYCONFIGURATIONS/V1/SYSTEMFUNCTIONS/RESET 40
UPDATES 40
INFORMATION AND CHARACTERISTICS OF THE DEVICE 41

TABLES

Table 1 – GSTP10X product family and description 7

Table 2 – IED Cyber Security - Level of compliance with the requirements 29

ANNEX

Annex 1 – Security Configurations API 28

1 ACRONYMS

a. **API** Application Programming Interface
b. **B, kB, MB, GB** Memory size expressed with a capitol letter (e.g. kB, MB), etc. means xBYTE
c. **BASH** Bourne Again SHell
d. **CPU** Central Processing Unit
e. **CVE** Common Vulnerabilities and Exposures
f. **FW** Firmware
g. **GS** Enel Global Standard
h. **HW** Hardware
i. **HV** High Voltage
j. **ICS** Industrial Control System
k. **IED** Intelligent Electronic Device
l. **JTAG** Joint Test Action Group
m. **MV** Medium Voltage
n. **NTP** Network Time Protocol
o. **NRND** Not Recommended for New Design
p. **OS** Operating System
q. **PCB** Printed Circuit Board
r. **PSBC** Power Supply Battery Charger of the IED
s. **RADIUS** Remote Authentication Dial-In User Service
t. **REST** REpresentational State Transfer
u. **ROM** Read Only Memory
v. **RTU** Remote Terminal Unit
w. **SCADA** Supervisory Control And Data Acquisition
x. **SFTPD** Secure FTP Daemon
y. **SR_XX** Security Requirement (XX type, e.g. SW = software)
z. **SSH** Secure SHell
aa. **SSL** Secure Sockets Layer
bb. **SSSD** System Security Services Daemon
cc. **SW** Software
dd. **Syslog-ng** System Log next generation
ee. **TCP** Transmission Control Protocol
ff. **TLS** Transport Layer Security

2 SCOPE OF THE WORK

Cyber security requirements for multifunctional protection devices described in this GS can be applied to the following group of GSTPs (Table 1), moreover it is also applicable to similar devices described in other specification

Table 1 – GSTP10X product family and description

GSTP10X type all	Product family code	Description
	GSTP10X	Protection and control device for HV/MV substation – Multifunctional Feeder Protection (MFP)
	GSTP01X	Protection and control device for MV substation – RGDM control unit
	GSTP111 and annexes	Protection and control device for HV/MV substation – Multifunctional Transformer protection (MTP)

3 REFERENCES

All the references in this GSTP are intended in the last revision or amendment.

3.1 For all countries

IEC 61850 series	Communication networks and systems for power utility automation
IEEE 1588	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems
Enel CSG 12	Cyber Security Guideline no. 12 – Version no.1 dated 11/09/2017 Enel Operational Technologies (OT) security guideline on industrial control systems

3.2 For EU countries

Countries should kindly declare the applicable local standards.

4 REPLACED STANDARDS

GSTP901 rev.1	Cyber security requirements for protection and control devices

5 DOCUMENT PURPOSE AND BACKGROUND

This document standardizes the cyber security requirements for the devices used for protection and control purposes in ENEL distribution substations. Devices afore-mentioned, as described in chapters 2 and 3, are accomplished to the definition of IED, according to IEC 61850 standard and described in deep in GSTPxyz series or similar specifications.

Devices subject of this GS are provided with Ethernet-type network connections, whereby these devices are interconnected to the ICS data transmission network. They also need not only to communicate with external servers but also with RTU or IEDs installed in different substations. For this reason, IED-type protections (below abbreviated as protections) may be subject of multiple cyber-attack techniques.

It is an ENEL major goal to procure protections with strong information technology security features, according to functional requirements issued.

In response to the tender subject of this document, it is highly required that potential Suppliers describe the solutions and information technology security features expected for the protections offered, in the various areas mentioned.

In following sections are described:

a. Information technology security requirements (below, abbreviated as “security”) that Enel considers mandatory, will constitute a necessary condition for the awarding of any supplies;

b. Information technology security prerequisites that are a necessary condition for the awarding of any supplies.

6 IED CYBER SECURITY REQUIREMENTS[1] DESCRIPTION

The security requirements belong to three categories:

- **Hardware security requirements**: this section includes the Hardware requirements that "strengthen" the IED Device against physical attacks aimed at accessing to the internal/logical components. Physical security requirements against acts of vandalism or enabling an overall physical protection of the device are out of scope;
- **Firmware security requirements**: this section prescribes the typical security requirements of the on-board Software. All the SW components in the IED will be affected. This set of SW is called "firmware";
- **Documentary Requirements**: this section deals with requirements for the documentation attached to the supply.

The requirements specified in the following sections can be:

- **Mandatory**, that means necessary for the award of the contract;
- **Optional**, that could additionally increase the score of the proposal during the technical evaluation.

The Supplier is required to give details concerning the technical procedures used to fulfill both types of requirements.

Note: requirements referred to communication services or functions are applicable if the IED works in IP networks.

7 IED HARDWARE CYBER SECURITY REQUIREMENTS

7.1 Hardware Architecture

This section contains the Hardware characteristics required

- to meet the security requirements;
- to update and standardize the IED hardware performance and the device management capability during its life-time.

7.1.1 Hardware Platform

7.1.1.1 SR_HR_01

Requirement type: **Mandatory**

Hardware components, in particular the microcontroller, must not be classified as "Discontinued" or "End of Life" at the time of supply.In addition, at the time of the supply, the microcontroller must not be classified as NRND (Not Recommended for New Design) or similar.

7.1.1.2 SR_HR_02

Requirement type: **Mandatory**

The "Product Longevity", that is the minimum supply and support period of the microcontroller by the Manufacturer, must be **equal or more than 10 years.**

[1] Hereafter the terms "**will**" and "**shall**" mean "**have the duty to**".

7.1.1.3 SR_HR_03

Requirement type: **Mandatory**

The IED must use only Industrial Grade components (CPU, Memory, board, etc).

7.1.1.4 SR_HR_04

Requirement type: **Optional**

The memory/storage of the IED must have, at least, the following characteristics:

- minimum 1GB RAM memory;
- minimum 2GB Flash memory;

they must be welded directly on the PCB (without socket) and hardly removable.

These are the minimum performance requirements necessary to guarantee (now and in the future) **only the security features of the IED**. Therefore, the Supplier shall size the memory/storage devices of the IED taking into account the performance requirements adequate both to deliver the application services and to support the security services.

7.1.1.5 SR_HR_05

Requirement type: **Mandatory**

Hardware memory supports (for example, flash ROM) must be soldered directly on the board (or attached to it with equivalent systems) and they must not be easy to remove (such as, for example SD-cards or memory sockets).

7.1.2 Security-specific functions

7.1.2.1 SR_HR_06

Requirement type: **Mandatory**

The CPU must fully support and, where possible, accelerate via ad-hoc instructions or HW components the security protocols that are currently classified as secure in the reference document published by the ECRYPT-CSA[2] "*D5.4 Algorithms, Key Size and Protocols Report*" (latest available version).

7.1.2.2 SR_HR_07

Requirement type: **Mandatory**

The CPU or any additional component in the IED may provide the following security feature:

- the integrity validation of the IED Bootloader or Firmware, by verifying their digital signature during the device start-up, through the use of the secure boot.

7.1.3 Interfaces and physical ports/connectors security

7.1.3.1 SR_HR_08

Requirement type: **Mandatory**

During the operation of the IED, the programming and/or debugging interfaces must be blocked at HW level. So the Supplier is requested to remove all the programming ports available on the electronic boards

[2] https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

of the IED intended for the operation in the substations (particular care must be taken of the JTAG interfaces).

This requirement can be waived only for IEDs used for testing or debugging purposes, however it's allowed only the footprints, without descriptive labels and declaring their presence to Enel.

Alternatively to HW disabling, permanent blocking via SW is allowed (e.g. refer to Secure JTAG[3].)

7.1.3.2 SR_HR_09

Requirement type: **Mandatory**

All of the physical interfaces and ports not expressly required by the Enel functional specifications must be blocked at Hardware level (e.g. USB ports, additional serial interfaces, etc.). In addition, wireless interfaces (e.g. Bluetooth, Wi-Fi, Infrared, etc.) are not allowed.

7.2 Hardware Solutions

This section of the document contains the requirements for hardware solutions used to strengthen the security of the HW system. Some of these requirements are classic anti-tampering mechanisms, others are measures introduced to hinder the Reverse Engineering.

7.2.1 Anti-intrusion mechanisms

7.2.1.1 SR_HR_10

Requirement type: **Mandatory**

The device must be equipped with hardened enclosures or, in general, any kind of solution that avoid an easy device disassembly and track any unauthorized hardware handling or tampering.

7.2.1.2 SR_HR_11

Requirement type: **Mandatory**

The device must generate an event/log in case of tampering and send it by using Syslog protocol.

7.2.1.3 SR_HR_12

Requirement type: **Optional**

The device must be equipped with Tamper Resistant solutions, in particular:

- Suppliers should use non-standard external screws, such as Security Torx or Tri-Wing types.

7.2.1.4 SR_HR_13

Requirement type: **Optional**

The device must be provided with paint seal or label on screws that reveal break-in attempts.

[3] https://www.digi.com/resources/documentation/digidocs/90001546/concept/trustfence/c_secure_jtag_android.htm

7.2.1.5 SR_HR_14

Requirement type: **Optional**

The device should be equipped with Tamper Detection solutions, in particular:

- one or more switches must be provided to detect the IED modules opening;
- moreover, the switch status change must trigger an arbitrary commands, for example device power-off or a script execution.

The device must be able to detect unauthorized tamper switch logic modifications and generate an action. The type of action must be customizable by Enel after the production phase of the IED.

The device should be able to trigger the following Tamper Response solutions:

- syslog event in case of switch position change;
- device bootloader disabling;
- Flash memory erasing;
- cryptographic keys erasing;
- Flash memory physical burn (destruction).

It must be possible to deactivate this feature for maintenance purposes

It's up to the Supplier to propose further solutions if considered more effective the must be motivated and explained by the Supplier.

The adopted solution must comply with the mechanical and electromagnetic requirements described in the Technical Specification.

7.2.1.6 SR_HR_15

Requirement type: **Optional**

The device should be equipped with Tamper Detection solutions able to work even if the IED is powered-off (e.g. using a memory register and a buffer battery): the event will be memorized and used at the next power-on of the IED (according to the requirement SR_HR_11).

7.2.2 Concealment of the components

7.2.2.1 SR_HR_16

Requirement type: **Mandatory**

Silk-screen omission: the PCBs must not have silkscreen (e.g any kind of marking used to identify the components, test points like JTAG or other) except for the PCB code and the Manufacturer logo/data.

7.2.2.2 SR_HR_17

Requirement type: **Optional**

The silk-screens on top of the integrated circuits should be removed or hidden to limit the attacker's ability to understand the used components.

7.2.2.3 SR_HR_18

Requirement type: **Optional**

The multilayer PCB should not expose copper tracks on the outer layers that could easily be identified as linked to the pins of the Flash memories or of the CPU, e.g. the copper tracks of Serial ports, modems, JTAG or other interfaces.

7.2.2.4 SR_HR_19

Requirement type: **Optional**

The Supplier should propose the use of epoxy encapsulation or resin coating of the components as a supplementary (e.g. encryption of solid state memories) or alternative solution in case some of the mandatory security requirements can't be met, including: removal of the marking, removal of programming interfaces, etc.

7.2.3 Power supply control

7.2.3.1 SR_HR_20

Requirement type: **Optional**

The Supplier should propose the implementation of circuits monitoring the power supply of the electronic boards, with particular attention to the supplies on the external interfaces (e.g. USB ports). The detection of anomalies must be traced via a Syslog message and must trigger an operation on the system (e.g. the kill-switch activation).

7.2.4 Hardware Performances

7.2.4.1 SR_HR_21

Requirement type: **Mandatory**

The Supplier shall size hardware capabilities of the IED device taking into account the adequate performance requirements of both application services and security features.

8 IED FIRMWARE CYBER SECURITY REQUIREMENTS

This section contains the requirements related to the Firmware features and configurations in order to meet the security requirements, to allow the adaptation and standardization of the IED configurations and the device management and maintenance over time.

In this document the term Firmware means the entire set of the IED software components, including:

- Root File System;
- Kernel;
- Bootloader;
- Middleware (basic and functional applications, including Application Software).

The Firmware is stored in non-volatile and unremovable memory.

8.1 Features of the Operating System

This section defines the requirements concerning the type of OS to which the IED must comply.

8.1.1 Bootloader

8.1.1.1 SR_SW_01

Requirement type: **Mandatory**

The Supplier shall disable the interactive Boot features offered by the Bootloader and completely preclude the possibility to modify the Bootloader configurations. If the Supplier decides to use a Bootloader lock password, he must ensure that this protection cannot be easily bypassed, for example by removing the buffer battery (if present).

In addition, Bootloader password (if present) must comply with *Cyber Security Guideline no.7*

Furthermore, the Bootloader must be configured to allow the OS to boot only from the on-board non-volatile and unremovable memory (it is forbidden, for example, to boot from a USB Flash drive or any other external peripheral device).

Finally, the Bootloader must be stored in a secure partition that cannot be overwritten through a firmware update or accessed/modified from firmware partition.

8.1.2 Operating System

8.1.2.1 SR_SW_02

Requirement type: **Mandatory**

The Supplier must equip the IED with an Operating System with, at least, the following characteristics:

- updatable and extensible in terms of functionality during the service life of the IED;
- maintained by a Supplier or a community providing updates and Security Patches;
- replaceable if discontinued and, therefore, independent of the CPU 's hardware Manufacturer;
- the latest final OS version or distribution branch must be used (release candidate or beta versions are not allowed).

Unless explicitly required by Enel, at the time each protection is released and for the following 5 (five) years, the operating system, including libraries and modules on the devices, must not be classified as deprecated (for example, End-of-Support, End-of-Life, Legacy or NRND) by the producer/maintainer of the software.

8.1.2.2 SR_SW_02bis

Requirement type: **Optional**

The Operating System shall be generated through "Yocto Project[4]" or a similar framework that guarantees the same functionality in terms of upgradeability and flexibility. The framework must be the latest version available and supported by the CPU. Enel suggests to use the Poky distribution or a distribution derived from it, or, in the case of RTOS, the FreeRTOS distribution.

In case of Operating Systems generated using Yocto, the 5 (five) years stablished in requirement SR_SW_02 must not be applied.

8.1.2.3 SR_SW_03

Requirement type: **Mandatory**

The Operating System must be equipped with proper resources (Kernel modules, binary and libraries) in order to manage and fully support:

- secure communications established through TLS[5], SSH[6];
- application protocols and standards mentioned in the functional technical specification of the device as, for example, IEC 61850.

8.1.2.4 SR_SW_04

Requirement type: **Mandatory**

Every IED must support Cryptographic Keys and related Digital Certificates (Security Tokens) to establish secure communications:

- ITU-T X.509v3 and RFC 5280 for TLS secure communications
- Public keys and digital certificates for SSH remote accesses.

Furthermore, in order to ensure the interoperability of the IED with Enel Public Key Infrastructure for Certificate Management (enrollment/renewal/revocation/status validation, etc.) the device must support also the following protocols and reference standards:

- SCEP (Simple Certificate Enrolment Protocol) -> IETF Draft : draft-gutmann-scep-15[A]
- CMP (Certificated Management Protocol) -> RFC 4210[B]
- EST (Enrollment over Secure Transport) -> RFC 7030[C]

Enel, in general, will provide during TCA process all necessary Digital Certificates and Challenge Passwords; if not, the Supplier shall generate Self-Signed Certificates according to ECRYPT-CSA[2] “D5.4 Algorithms, Key Size and Protocols Report” (latest available version).

[A] https://tools.ietf.org/html/draft-gutmann-scep-15
[B] https://tools.ietf.org/html/rfc4210
[C] https://tools.ietf.org/html/rfc7030

[4] https://www.yoctoproject.org/
[5] https://en.wikipedia.org/wiki/Transport_Layer_Security
[6] https://en.wikipedia.org/wiki/Secure_Shell

8.2 Middleware Components

This section contains the Middleware requirements the IED has to comply with. Middleware refers to all the SW required for the execution of the functions the IED has been designed to, including the application software when not provided by Enel, the management system and the basic security software.

8.2.1 Remote Management functionalities of the device

8.2.1.1 SR_SW_05

Requirement type: **Mandatory**

In addition to the management functionalities specified in the Technical Specification, the FW must be provided with an easy (to implement) access to the essential security features (ref. SR_SW_06) for a correct centralized management of the IEDs, such as:

- SSH service configuration:
  - activation/deactivation of the service (activated by default),
  - Public Keys addition and removal in "authorized_keys";
- SCP/SFTP Service Configuration:
  - identification of the users enabled for the service,
  - definition of the users' access rights (reading or reading/writing);
- Network services configuration:
  - NTP server configuration for clock synchronization,
  - system hostname configuration,
  - system DNS configuration,
  - IP addresses configuration (with subnet mask and default gateway too);
- Firewall service:
  - activation/deactivation,
  - bulk download or bulk upload of iptables rules configuration file;
- Credentials/Keys Service:
  - creation/deletion of system users and http service users,
  - change of user's password and role assignment,
  - upload/update of Cryptographic Keys and Digital Certificates (as defined in SR_SW_04);
- Syslog service:
  - configuration of destination server IPs, ports and protocols for logs transmission,
  - log download;
- System functions:
  - reset of the factory configurations by removing all data and restoring initial configurations,
  - device restart;
- Updates:
  - upload of security update/new firmware,
  - configuration of the repository for the download of the update in accordance with the methods defined in the following sections,
  - execution of the update command, also with related scheduling;
- Information and characteristics of the device:
  - Hardware informations (at least, Manufacturer, Product Name, Version and univocal, for any device, Serial Number, memory, CPU size, HDD size, CPU, memory and HDD consumption, MAC address, including production timestamp of the components), Firmware version, Operating System version, Patching Level, Kernel version, https server version, Application Software version and protocols version.

8.2.1.2 SR_SW_06

Requirement type: **Mandatory**

The security configurations, as defined in the SR_SW_05 requirement, must be accessible both via API and via Web interface.

The Supplier must use the REST API type as defined in the Annex 1. Hereafter, Annex 1 has to be referred everytime API method is mentioned. Furthermore, these APIs must share same channel of the Web application (coexistence).

8.2.2 Security of the Software code developed by the Supplier

8.2.2.1 SR_SW_07

Requirement type: **Mandatory**

The Supplier undertakes to develop the SW code according to the security guidelines defined by Enel in the document *Guideline n.7 – Enel "IT Security Guidelines - APPLICATIONS".*

Futhermore, Web applications or API produced by the Supplier must be free of vulnerabilities according to the OWASP Top Ten[7] (During the control, the Supplier must consider the last version available of the OWASP Top Ten list at the time of the supply).

Enel reserves the right to perform Security Static/Dynamic Code Analysis of the software components developed by the Supplier. The Supplier will undertake all necessary corrective actions at its own expense if, during the testing phase of the product, deviations with the requirements in the Enel guidelines are identified.

8.2.2.2 SR_SW_08

Requirement type: **Mandatory**

All applications developed by the Supplier running on the IED must perform the tracking of the security logs by generating Syslog messages (according for example to RFC 5424) in the device.

ENEL considers the security events concerning

- the (both successful and failed) authentication to the system;
- all the administrative operations performed on the device of high importance (as described in SR_SW_17).

8.2.2.3 SR_SW_09

Requirement type: **Mandatory**

Applications shall operate at the lowest privilege level possible and must be able to access only the information and resources that are necessary for its legitimate purpose.

[7] https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

8.2.2.4 SR_SW_10

Requirement type: **Optional**

If the Supplier executes Security Static Code Analysis with own tools[8], aimed at identifying potential security vulnerabilities in the code he developed, when issuing the IED, he should provide Enel with the findings identified by such instruments. In case of unresolved reports, the Supplier shall explain the reason why they have not been solved.

8.2.3 Required Security Software

8.2.3.1 SR_SW_11

Requirement type: **Mandatory**

The IED must be equipped with specific security software, in particular the Supplier is required to equip the Firmware with the following software updated to the latest version:

- Iptables with related dependencies (libraries and Kernel modules);
- OpenSSH configured to support the SFTP protocol;
- OpenSSL;
- SELinux (in case of Linux OS);
- RADIUS centralized authentication modules;
- LDAP and LDAPs (in case of Linux OS);
- Syslog-ng daemon;
- NTP daemon;
- Bash or sh scripting environment.

8.2.3.2 SR_SW_11bis

Requirement type: **Mandatory**

In order to guarantee the compliance, the device must be provided with the following software applications, including all the related dependencies:

- Enel will provide NTP client for clock synchronism and the configuration of the NTP servers (the same for PTP synchronization).
- Network configuration with domain name resolution and the configuration of the DNS servers will be provided by Enel.
- Personal Firewall (iptables or similar) feature. Initially, the policies will be set in the “permit-all” mode.
- Syslog-ng daemon for the local collation of the logs and able by configuration to send also the logs to a remote server.

[8] https://www.owasp.org/index.php/Source_Code_Analysis_Tools

8.2.4 Remote Management Software

8.2.4.1 SR_SW_12

Requirement type: **Mandatory**

The device must be equipped with a web interface that enables application functionalities and security configurations management (ref. next requirement).

If explicitly required by Enel, the software for managing and configuring the parameters of the IED (i.e. "IED Management SW") must rely on a communication protocol based on TLS or SSH.

8.3 Hardening

This section specifies the security configurations (Hardening) the IED must be equipped with. These configurations allow to reduce the perimeter of attack exploitable by an attacker that attempts to take the control of the device.

8.3.1 Hardening Guideline

8.3.1.1 SR_SW_13

Requirement type: **Mandatory**

The Supplier must install on the IED only demons or (IP) network services authorized by Enel.

According to functional and cyber security requirements they are:

- Web Server relying on the https service, using TCP port 443, for exposing Web interfaces/device and APIs exposure;
- Secure Shell relying on the SSH service, using TCP port 22, for administrative access to the device;
- Services and protocols strictly related to the applicative communication of the device (example, protocol IEC 61850).
- Syslog client by using UDP port 514: as transmission logging protocol.
- Clock synchronization protocols, as Network Time Protocol (NTP), by using UDP port 123, and/or Precise Time Protocol (PTP based on IEEE1588), by using UDP port 319 and 320 and/or native Layer 2 Ethernet implementation (using well known Ethernet type 0x88F7).

Enel must previously authorize the use of any network service different from those above mentioned. The Supplier shall provide written documentation that explain the need to install additional network services comparing to the previous list.

8.3.1.2 SR_SW_14

Requirement type: **Mandatory**

It must be possible to disable via software any physical interface of the device.

8.3.1.3 SR_SW_15

Requirement type: **Mandatory**

The Firmware configuration must follow secure configuration guidelines (defined according to the selected software version and type) at least for the following components:

- SSH service[9];
- Web server selected by the Supplier[10];
- Linux OS[11] or RTOS[12]

However the Supplier, unless specifically indicated by Enel when technical proposal has been provided (during the tender and/or TCA), must choose these guidelines among those publicly available and make them known to Enel. As an example, some guidelines are reported in the footnotes.

Virtualization of any software or O.S. is not allowed.

8.3.1.4 SR_SW_16

Requirement type: **Mandatory**

According to the functional requirements, for the following functions only:

- Clock update via NTP and/or PTP (if present)
- Sending log messages via Syslog;
- Application communication like automation functions (for example, IEC-61850 standard, DNP3, ecc).

use of unencrypted (IP) network communications could be approved by Enel, although the IED device is required to natively support the secure versions too.

Unless explicit Enel approval, all the other communications must rely on underlying security protocols, that will only support encryption algorithms considered, to date and for the entire life cycle of the IED, secure, as defined in the document published by the ECRYPT-CSA[2] "*D5.4 Algorithms, Key Size and Protocols Report*" (latest available version).

If, for technical reasons, the Supplier intends to use security protocols with encryption algorithms that currently are considered safe, but may not be considered as such for the entire life cycle of the device as described in the previous paragraph, the Supplier shall implement methods to update the IED in order to replace the algorithms that will be considered insecure with secure ones.

8.3.2 Security Logging

The traceability of the actions performed on the device during the operation is a key element for its security. The Supplier shall configure the IED in a way that the it will be able to trace the operations performed on/by the device.

8.3.2.1 SR_SW_17

Requirement type: **Mandatory**

The logs generated by the operating system (SSH service, local database, web server and the various network daemons in general) and by the application software must be compatible with the syslog format. In addition, the storage of the logs must take place, initially, on the device's non-volatile memory and in the appropriate log files available by the operating system of the device (/var/log).

The IED must be configured to trace the main administrative operations performed on it, including at least:

[9] https://wiki.centos.org/HowTos/Network/SecuringSSH
[10] https://www.owasp.org/index.php/SCG_WS_nginx, https://www.owasp.org/index.php/SCG_WS_Apache
[11] https://www.sans.org/score/checklists/linux
[12] http://support7.qnx.com/download/download/22003/qnx_secure_kernel_whitepaper_RIM_MC411.67.pdf/download/download/22003/qnx_secure_kernel_whitepaper_RIM_MC411.67.pdf

- Successful and failed user login to the system through any implemented interface in remote/local access (e.g. SSH access, Web access, API access, IED Management SW);
- Failed login attempts to the system through any implemented interface;
- Execution of administrative operations using SSH access;
- Execution of security commands using the Web interface, API or the IED Management SW;
- System time modification;
- Device booting;
- Device shut down;
- User escalation and command execution through “su/sudo” commands;
- User creation/modification (both system and application)
- Services/daemon crash

These operations must be tracked inside the system via the Syslog service likewise the other security logs defined in the requirements of this document.

The device shall allow log files to be read remotely. The device shall be able to send logs to a Security Information Event Management (SIEM) system by using syslog protocol (according for example to RFC 5424) and following Enel Guideline 10 “Infrastructural Security” prescriptions.

Furthermore, the IED must also log the following events and send them throught Syslog:

- Loss of communications between the IED and other hosts;
- Rejection of any compromised or invalid data;
- Detection of internal errors and failures.

By default, the three type of events above must not be sent to the external SIEM and must be only logged, however it must be given the possibility to Enel, if needed and successively, to activate the service.

8.3.2.2 SR_SW_18

Requirement type: **Mandatory**

Non-volatile memory of the device must be able to ensure the storage of the log file for at least 30 days, considering the average use of the connected device in the field.

Therefore the "Log Rotation" function must be provided to guarantee the storage of the most recent logs and the elimination of the old ones and the logs must be sent and archived in compressed mode.

The log files must be only writable by root user.

8.3.2.3 SR_SW_18bis

Requirement type: **Optional**

The Supplier shall provide a storage space dedicated to the logs with a minimum capacity of 200 Megabytes ensuring at least the 30 days specified in SR_SW_18. These logs must be non-volatile and, therefore, saved in the non-volatile and unremovable memory.

8.4 Security Patching

Software components of the IED firmware that, regardless of the quality of the validation process adopted during the selection, development, integration and configuration phases, may be affected by not-yet-known vulnerabilities. Enel requires that the IED software be updatable with security patches guaranteeing the device security requested level over time.

8.4.1 Updates during the IED supply

8.4.1.1 SR_SW_19

Requirement type: **Mandatory**

Unless explicitly authorized by Enel, at the time of the supply the device Firmware must be equipped with communication ports, protocols, services and software updated to the latest version, properly configured and free of known vulnerabilities. Vulnerabilities are considered known if they are in a public vulnerability database (like CVE[13]), or if an advisory on them has been published. Vulnerabilities classified as CVE >= 4 are not allowed/admitted during the entire lifecycle of the product.

8.4.2 Security updates during the IED operation

8.4.2.1 SR_SW_20

Requirement type: **Mandatory**

During the entire life cycle of the supply, the Supplier shall support Enel to update the Firmware security level, in order to fix new vulnerabilities that could affect the supply and the devices in the field. Basically, as long as the contract is in place, **the Supplier is required to proactively release Software updates (Security Patches)**, at least every 6 months, aimed to resolve the security vulnerabilities made public[14] during the same time period.

Furthermore, Enel can explicitly require the release of Security Patches, for example in the following circumstances:

- as a result of a Security Assessment carried out by Enel or a third-party company;
- faced with the publication of a new vulnerability affecting the systems and that Enel considers necessary to mitigate with high priority. If the reference software-house has not yet released the relevant Security Patch, it shall implement, at least, "workaround" configurations;
- react to a targeted Cyber Attack.

The Supplier is also required to release the Security Patch within 1 month from the security update request by Enel. The Supplier shall previously test the new Security Patches on all the supplied versions of IED.

Furthermore, Enel could ask for Supplier dedicated software bundles setup. Software bundles can include more security patches or a mix of security patches and functional updates, in order to deliver easily the new packages to the field devices.

The Supplier is not required to distribute the Security Patches on individual equipment already deployed in the field: Enel is in charge of this activity.

[13] https://www.cvedetails.com/
[14] “made public means published on the (Web) sites of the reference software-house

8.4.2.2 SR_SW_21

Requirement type: **Mandatory**

The device must be equipped with the following uptdate methods:

- manual installation on the device via Web interface or IED Management SW;
- update via API;
- It should be possible to upload the update on the device via SSH service

Once the update be upload, the device, by means of a “job”, shall carry out the update according to the logic agreed during the design phase (for example, time scheduling or based on the device status).

The Supplier is required to provide the following functions regarding the protections update:

- Hash verification of the transferred update package to the device before installation.
- Compatibility verification of the update package with the firmware update status (including the resolution of dependencies)
- Update packages must be digitally signed. Device must be able to check the digital signature before proceeding with the update (function on demand through device configuration).In this case, the Supplier is in charge of the installation of the digital certificate (provided by Enel) on the target device system.
- Robustness of the update process. If the update is not correctly installed, the device system must automatically perform the roll-back procedure.
- Protection from brick/lock states during the update procedure.
- Tracking of the update activity, including data, state and result (by using syslog as described in requirements SR_SW_08 and SR_SW_17.
- It must be possible to get the specific version of the firmware installed, including the real-time security patches status of the device, both by web request and SSH access.

Due to potential limitations in the network connectivity, the updates must be preferably be applicable in a “differential” way (for example, separated patches or similar).
It shall be responsibility of the Supplier to define the most suitable method in order to ensure the integrity of the update and the stability of the device during the uploading/downloading and the installation.

8.4.2.3 SR_SW_22

Requirement type: **Optional**

The Supplier can propose a “repository” updating method by which the devices, once authorized, autonomously can carry out the download of the update required, check its compatibility with the software and hardware and carry out the updating.

In this regard, Enel will agree with the Supplier any constraints or wishes in case of an existing patch delivery solution, not in addition to what is required here, simply for the purpose of correctly guide the repository development.

8.4.2.4 SR_SW_23

Requirement type: **Mandatory**

If a security update is required when a supply is in progress (ref. SR_SW_20), the devices to be supplied must already include it.

8.4.3 Update Security

8.4.3.1 SR_SW_24

Requirement type: **Mandatory**

At least the following technical requirements regarding the security of updates must be fulfilled:

- the Supplier shall digitally sign the released updates;
- the device must be able to perform the hash check (with a known and, currently, safe algorithm) of the update package (transferred to it) before its installation.

The (both successful and failed) update of the system (or packages) must be trace via the syslog service and the event must be sent to a SIEM.

8.5 Users, credentials and certificates management

8.5.1 Credentials Security

8.5.1.1 SR_SW_25

Requirement type: **Mandatory**

The default credentials must be removed and each credential configured on the system must comply with the minimum complexity requirements (length and character pattern) according to the Enel policy (ref. Cyber Security Guideline no.7). The connection to the system with “root” user is forbidden, both remotely (e.g. via SSH) and locally (e.g., via the serial interface).

Furthermore, the device must be compatible with the following requirements:

- The provision of time-based lock-out credentials management techniques.
- The definition of at least two user profiles, Administrator and Operator, with least privilaged approach.
- Anti-brute-force login protection (time and attempts lock).

8.5.1.2 SR_SW_26

Requirement type: **Mandatory**

"Hardcoded" credentials, that means included directly in the application code, are forbidden. If the credentials are saved in configuration files, the passwords must be properly protected through the use of non-proprietary and non-deprecated Hashing [15] algorithms.

In case the application logic requires access to the password (i.e. to be used as “secret” in HMAC algorithm, or to connect to remote services via M2M interfaces) **only** the specific secrets required can be saved in encrypted files or DB sections (thus in “reversible” form). The access keys to these locations **must** be properly protected e.g. by means of services provided by the OS (keystore, or similar, depending on their availability on the OS itself), or (less preferable approach) via proper software protection/obfuscation techniques when included into the programming logic. In case the Supplier decides not to use the keystore or similar services provided by the OS, he must describe the methodology used.

[15] https://en.wikibooks.org/wiki/A-level_Computing/AQA/Paper_1/Fundamentals_of_data_structures/Hash_tables_and_hashing

8.5.2 Centralized authentication

8.5.2.1 SR_SW_27

Requirement type: **Mandatory**

The IEDs must support centralized authentication modes that can be optionally activated by Enel during the start-up phase for administrative access to the device (via SSH or Web); in particular:

- Radius centralized authentication;
- LDAP/LDAPs centralized authentication.

8.5.3 Update of certificates and cryptographic keys

8.5.3.1 SR_SW_28

Requirement type: **Mandatory**

It must be possible to update all the credentials and cryptographic keys of the device during its operation and without affecting/downgrading its functionalities.

8.5.4 Techniques for the protection of the administrative access to the device

8.5.4.1 SR_SW_29

Requirement type: **Mandatory**

It must be possible to access the device with administrative privileges (writing and reading) in the following **three modes**:

1. remote access via a web interface;
2. remote access via SSH service;
3. remote access via API.

The allowed authentication procedures are the following:

- login via username/password: modes 1 and 2;
- access through Digital Certificate or mutual authentication: modes 2 and 3.

The following features are required in order to protect the login with username/password:

- the password complexity must comply with the guidelines provided by Enel (Cyber Security Guideline no.7);
- implement password complexity validation mechanisms limited to the mode 1;
- provide timed lock-out techniques for the credentials.

8.5.4.2 SR_SW_30

Requirement type: **Mandatory**

Besides the user profiles of the device operators defined in the main specification, a profile for the administrative access via the Web interface for the Security Management of the device must be provided:

- "Security Administrator" user that can only modify the security parameters and configurations as defined in SR_SW_05.

8.5.5 Certificates and Cryptographic Key

8.5.5.1 SR_SW_31

Requirement type: **Mandatory**

Private cryptographic components (such as SSH private keys, TLS private keys, or passwords) shall be placed in a secure partition that guarantee a high level of security (Trusted Execution Environment).
In the event the TEE cannot be applied, other software solutions or modules that guarantee also a high level of protection of the cryptographic components can be proposed by Supplier (as for example *GnuPG*)

8.5.5.2 SR_SW_32

Requirement type: **Mandatory**

Management of the cryptographic keys that support data protection capabilities (authentication, encryption, digital signatures) shall be performed according to common IT security guidelines and best practices (as for example *FIPS 140-2 "Security Requirements for Cryptographic Modules*").

9 DOCUMENTARY REQUIREMENTS

9.1 Detailed Technical Documentation to be provided

9.1.1 Required technical details

9.1.1.1 SR_DC_01

Requirement type: **Mandatory**

The Supplier, in addition to the supply of the IED, shall provide detailed documentation regarding the adopted security configurations, highlighting all the aspects of compliance with the requirements in this Global Standard. Furthermore, in case of changes impacting the Cyber security of the device, the abovementioned documentation shall be updated accordingly.

In particular, the required documentation must include the following information and SW:

1. interfaces of the device including protocols and services used on each interface;
2. detailed information about HW components;
3. detailed information about interfaces and/or services that have been disabled and not removed, if any;
4. detailed specification of the security configurations adopted at HW level;
5. detailed description of the selected OS, versions of the SW packages, libraries and Kernel;
6. list of the incremental patches with respect to the adopted version of the OS;
7. detailed specification of the Hardening configurations performed on the system compared to the basic configurations of the OS;
8. detailed list of applications, utilities, scripts, databases included in the system that aren't part of the basic OS;
9. evidence of the tests or security checks carried out;
10. changes to the system compared to the basic configurations of the OS;
11. development Environment used to implement the FW;
12. all of the Credentials/Certificates configured and set in the device;
13. design evidence at a level of detail that makes it easy to verify that the security rquirements are implemented, and to test that they are implemented on the device as described;
14. password recovery mechanism test report against any weaknesses;
15. designated "security focal point" of the company who shall be responsible for receiving notifications of anomalous events relating to the security of the system, providing appropriate responses and actions in a timely manner.

All the information requested in this requirement (SR_DC_01) must be provided during the tender technical phase. Also detailed information, about how the device is comply to each cyber security requirement in this document, must be provided during the tender technical phase without exception.

10 CYBER SECURITY REQUIREMENTS BIDDING FORM

The Supplier/Bidder shall fill the following table, related to the Cybersecurity requirements described in Chapters 7, 8 and 9.

Table 2 – IED Cyber Security - Level of compliance with the requirements					
N.	**Technical Specification**	**Mandatory**	**Yes**	**No**	**Remarks for any deviation or details**
7.1 HW Cyber security requirements – HW Architecture					
SR_HR_01		x			
SR_HR_02		x			
SR_HR_03		x			
SR_HR_04					
SR_HR_05		x			
SR_HR_06		x			
SR_HR_07		x			
SR_HR_08		x			
SR_HR_09		x			
7.2 HW Cyber security requirements – HW solutions					
SR_HR_10		x			
SR_HR_11		x			
SR_HR_12					
SR_HR_13					
SR_HR_14					
SR_HR_15					
SR_HR_16		x			
SR_HR_17					
SR_HR_18					
SR_HR_19					
SR_HR_20					
SR_HR_21		x			
8.1 IED FW Cyber security requirements – Features of the OS					
SR_SW_01		x			
SR_SW_02		x			
SR_SW_02bis					
SR_SW_03		x			
SR_SW_04		x			
8.2 IED FW Cyber security requirements – MW components					
SR_SW_05		x			
SR_SW_06		x			
SR_SW_07		x			
SR_SW_08		x			
SR_SW_09		x			
SR_SW_10					
SR_SW_11		x			
SR_SW_11bis		x			
SR_SW_12					
8.3 IED FW Cyber security requirements – Hardening					
SR_SW_13		x			
SR_SW_14		x			
SR_SW_15		x			
SR_SW_16		x			
SR_SW_17		x			
SR_SW_18		x			
SR_SW_18bis					
8.4 IED FW Cyber security requirements – Security Patching					
SR_SW_19		x			
SR_SW_20		x			

Table 2 – IED Cyber Security - Level of compliance with the requirements					
N.	**Technical Specification**	**Mandatory**	**Yes**	**No**	**Remarks for any deviation or details**
SR_SW_21		x			
SR_SW_22					
SR_SW_23		x			
SR_SW_24		x			
8.5 IED FW Cyber security requirements – Users, Credentials and Certificates Management					
SR_SW_25		x			
SR_SW_26		x			
SR_SW_27		x			
SR_SW_28		x			
SR_SW_29		x			
SR_SW_30		x			
SR_SW_31		x			
SR_SW_32		x			
9.1 Detailed Technical Documentation to be provided					
SR_DC_01		x			

ANNEX

11 Annex 1 - SECURITY CONFIGURATIONS API

General information

API must adhere to the REST architectural constraints (RESTful APIs).
API must be available at the following URI:

https://<hostname>:<port>/securityConfigurations/v1

Security

Only HTTP/1.1 or higher protocol can be used.

Authentication

The API must support a custom HMAC authentication named XWS and defined here:

XWS authentication
Clients will provide HTTP Authentication and Date headers in the following format:
(XWS stands for ICS Web Services)

Authentication: XWS <username>:<digest>
Date: <timestamp>

<digest> = base64(hmac-sha256("<password>", "<verb> <pathname> <timestamp>"))

- <verb> is the http verb in uppercase (for example "GET")
- <pathname> is the pathname of the http request without the hostname, with a leading slash and with the eventual parameters (for example "/securityConfigurations/v1/ssh/service")
- <timestamp> is the number of seconds since Jan 01 1970. (UTC) of the request (for example "1557131233")
- <username> and <password> are system users credentials.

base64() means base64 encoding

hmac-sha256(<secret key>, <text to be hashed>) means hashing with the Hash-based message authentication code (HMAC) with digest algorithm SHA-256 and with secretKey <secret key> and text <text to be hashed>.

Strings must be UTF-8 encoded and the newline separator is LF (unix style)
HMAC and SHA-256 are defined in RFC4634 (https://tools.ietf.org/html/rfc4634)

Example
Assuming a request with the credential myUser1/myPassword1:

GET /securityConfigurations/v1/ssh/service
Authentication: XWS
myUser1:MTA1NGM2YmRiZDdjY2U0ZDg2ZWUxMmM2MjBmYzAwZjI4ZWYzMGIwZDQ4ZTMyNDgwZWY4ODcxMWI5YWY2YTRlMQ==
Date: 1557131233

The digest is calculated according to this string:
hmac-sha256(“myPassword1","GET /securityConfigurations/v1/ssh/service 1557131233”)=
“1054c6bdbd7cce4d86ee12c620fc00f28ef30b0d48e32480ef88711b9af6a4e1”
base64(“1054c6bdbd7cce4d86ee12c620fc00f28ef30b0d48e32480ef88711b9af6a4e1”) =
“MTA1NGM2YmRiZDdjY2U0ZDg2ZWUxMmM2MjBmYzAwZjI4ZWYzMGIwZDQ4ZTMyNDgwZWY4ODcxMWI5YWY2YTRlMQ==”

Authorization

The server must calculate the <digest> value of the request and, only if the calculated digest is equal to the provided digest, the API is authorized: otherwise a “401 Unauthorized” must be returned.

Even in presence of a correct digest, <timestamp> must be within a configurable timeframe, with a default value of 24 hours, compared to the actual time of the ICS.
No specific API is available for such a configuration, which must be handled via a firmware update, e.g. providing a specific file in a determined location, that must be declared at design time for the product, or including a specific field in an already existing configuration file.

The API server onboard on the IED must check the associated privilege before initiating the API execution. All the APIs described here must be allowed ONLY to users of the “administrator” type.

Response
If the responses contains data must be declared the content type “application/json”.

In the definition of the API, response is defined only if contain a JSON content.

Successful response must be 200 OK.

Unsuccessful response must use common http rules.

4XX Response must provide an error code and description in the JSON content.

Example:

Response OK
HTTP/1.1 200 OK

Response KO
HTTP/1.1 4XX
Content-Type: application/json;

```
{
  "errorCode": "<errorCode>",
  "errorDescripton": "<errorDescription>"
}
```

SSH service configuration

Activation and deactivation of the service ssh

Activation of the service ssh
Request
POST https://<hostname>:<port>/securityConfigurations/v1/ssh/service/start

Deactivation of the service ssh
Request
POST https://<hostname>:<port>/securityConfigurations/v1/ssh/service/stop

Get of the state of the service ssh
Request
GET https://<hostname>:<port>/securityConfigurations/v1/ssh/service
```
{
  "state": "<active|inactive>"
}
```

Public Keys addiction and removal in "authorized keys"

Public key addiction
Request
POST https://<hostname>:<port>/securityConfigurations/v1/ssh/publicKeys
```
{
  "name": "<name>",
  "publicKey": "<publicKey>"
}
```

Public key deletion
Request
POST https://<hostname>:<port>/securityConfigurations/v1/ssh/publicKeys/delete/<name>

Retrieve Public keys list
Request
GET https://<hostname>:<port>/securityConfigurations/v1/ssh/publicKeys

Response
```
[
  {
    "name": "<name 1>",
    "publicKey": "<public Key 1>"
  },
  {
    "name": "<name N>",
    "publicKey": "<public Key N>"
  }
]
```

SCP/SFTP Service Configuration

Identification of the users enabled for the service

Request
GET https://<hostname>:<port>/securityConfigurations/v1/scpSftp/users

Response

```
[
  {
    "name": "<name 1>",
    "access": "<readOnly|readWrite>"
  },
  {
    "name": "<name N>",
    "access": "<readOnly|readWrite>"
  }
]
```

Network services configuration

Retrieve network services configuration info

Request

GET http://<hostname>:<port>/securityConfigurations/v1/networkServicesConfig

Response

```
{
  "hostname": "<hostname>",
  "ipAddresses": [
      {"ipAddress":"<ip address 1>","netMask":"<net mask 1>", "defaultGateway":"<default gateway 1>",
”nic”:”<network interface card>” },
      {"ipAddress":"<ip address N>","netMask":"<net mask N>", "defaultGateway":"<default gateway N>",
”nic”:”<network interface card>” }
  ],
  "dns": [
    "<ip dns server 1>",
    "<ip dns server N>”
  ],
  "ntpServer": "<ntp server>"
}
```

Update Network service configuration info

Request

POST https://<hostname>:<port>/securityConfigurations/v1/networkServicesConfig

```
{
  "hostname": "<hostname>",
  "ipAddresses": [
      {"ipAddress":"<ip address 1>","netMask":"<net mask 1>", "defaultGateway":"<default gateway 1>",
”nic”:”<network interface card>” },
      {"ipAddress":"<ip address N>","netMask":"<net mask N>", "defaultGateway":"<default gateway N>",
”nic”:”<network interface card>” }
  ],
  "dns": [
    "<ip dns server 1>",
    "<ip dns server N>”
  ],
  "ntpServer": "<ntp server>"
}
```

Firewall service

Activitation and deactivitation of the firewall service

Activation of the firewall service
Request
POST https://<hostname>:<port>/securityConfigurations/v1/firewall/service/start

Deactivation of the firewall service
Request
POST https://<hostname>:<port>/securityConfigurations/v1/firewall/service/stop

Retrieve the state of the firewall service
Request
GET https://<hostname>:<port>/securityConfigurations/v1/firewall/service
Response
```
{
  "state": "<active|inactive>"
}
```

bulk download or bulk upload of iptables rules configuration file

Retrieve the current used iptable rules
Request
GET https://<hostname>:<port>/securityConfigurations/v1/firewall/iptable

Response
```
{
  "iptable": "<iptable file content>"
}
```

Update the iptable rules
Request
POST https://<hostname>:<port>/securityConfigurations/v1/firewall/iptable
```
{
  "iptable": "<iptable file content>"
}
```

NOTE: iptable rules must be actualized in real time
NOTE2: in the iptable rules file, newline is the ASCII LINE-FEED character (“\n”) (unix/linux default)

Credentials/Keys Service

Bulk Download
Download bulk user settings

Request
GET https://<hostname>:<port>/securityConfigurations/v1/users/bulkSettings

Response

```
[
  {
    "etcPasswd": "</etc/passwd content file>",
    "etcShadow": "</etc/shadow content file>",
    "etcGroup": "</etc/group content file>"
  }
]
```

System users

Retrieve the list of the system users

Note: “group” is optional

Request

GET https://<hostname>:<port>/securityConfigurations/v1/users/system

Response

```
[
  {
    "name": "<name 1>",
    "role": "<users|administrator>",
    “group”: “<group>”
  },
  {
    "name": "<name N>",
    "role": "<users|administrator>",
    “group”: “<group>”
  }
]
```

Create a system user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/system

```
{
  "name": "<name1>",
  "role": "<users|administrator>",
  “group”: “<group>”
}
```

Change password of a system user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/system/changePassword

```
{
  "name": "<name>",
  “password”: “<new password>”
}
```

Delete a system user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/system/delete/<name>

Web server users

Retrieve the list of the web server users

Request

GET https://<hostname>:<port>/securityConfigurations/v1/users/web

Response

```
[
  {
    "name": "<name 1>",
    "role": "<read|write|security>",
    “group”: “<group>”
  },
  {
    "name": "<name N>",
    "role": "<read|write|security>",
    “group”: “<group>”
  }
]
```

Create a web server user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/web

```
{
  "name": "<name>",
  "role": "<read|write|security>"
}
```

Change password of a web server user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/web/changePassword

```
{
  "name": "<name>",
  “password”: “<new password>”
}
```

Delete a web server user

Request

POST https://<hostname>:<port>/securityConfigurations/v1/users/web/delete/<name>

Upload update and get of Cryptographic Keys and Digital Certificates

Cryptographic Keys

Retrieve the list of the cryptographic keys.

NOTE: tokenType can assume the following value:

- “private public x509” private/public x509 Certificates pair for the TLS communication service to the SCADA infrastructure; these Certificates must be different on each IED;
- “X509” X509 Certificates pair for the https service; these Certificates must be different on each IED;
- “Public Key” Public Key pool for the remote access via SSH; these Certificates must be different on each IED;
- “Root CA public x509” Root-CA public x509 Certificate, common to all devices.

Request
GET https://<hostname>:<port>/securityConfigurations/v1/cryptographicKeys

Response

```
[
  {
    "name": "<name 1>",
    "key": "<cryptographic key 1>",
    "tokenType": "<token type 1>"
  },
  {
    "name": "<name N>",
    "key": "<cryptographic key N>",
    "tokenType": "<token type N>"
  }
]
```


Create a cryptographic key
Request
POST https://<hostname>:<port>/securityConfigurations/v1/cryptographicKeys

```
{
  "name": "<name>",
  "key": "<cryptographic key>",
  "tokenType": "<token type>"
}
```


Delete a cryptographic key
Request
POST https://<hostname>:<port>/securityConfigurations/v1/cryptographicKeys/delete/<name>

Digital Certificates

Retrieve the list of the digital certificates. All certificates must be <cer> type
NOTE: tokenType can assume the following value:

- “private public x509” private/public x509 Certificates pair for the TLS communication service to the SCADA infrastructure; these Certificates must be different on each IED;
- “X509” X509 Certificates pair for the https service; these Certificates must be different on each IED;
- “Public Key” Public Key pool for the remote access via SSH; these Certificates must be different on each IED;
- “Root CA public x509” Root-CA public x509 Certificate, common to all devices.

Request
GET https://<hostname>:<port>/securityConfigurations/v1/digitalCertificates

Response

```
[
  {
    "name": "<name 1>",
    "certificate": "<digital certificate 1>",
    "tokenType": "<token type 1>"
  },
```

```
 {
   "name": "<name N>",
   "certificate": "<digital certificate N>",
   "tokenType": "<token type N>"
 }
]
```

Upload a digital certificate
Request
POST https://<hostname>:<port>/securityConfigurations/v1/digitalCertificates

```
{
  "name": "<name>",
  "certificate": "<certificate file>"
    "tokenType": "<token type>"
}
```

Delete a digital certificate
Request
POST https://<hostname>:<port>/securityConfigurations/v1/digitalCertificates/delete/<name>

Syslog service

Configuration
Retrieve Syslog service configuration info

Request
GET https://<hostname>:<port>/securityConfigurations/v1/syslogService/config

Response

```
{
  "destinationServerIP": [
     {"ip":"<destination server IP 1>","port":"<port 1>", "protocol":"<protocol 1>"},
     {"ip":"<destination server IP N>","port":"<port N>", "protocol":"<protocol N>"}
  ]
}
```

Log download
Retrieve the system Log.
Log must be in <zip> format and must contain all the log files present in the device.

Request
GET https://<hostname>:<port>/securityConfigurations/v1/syslogService/log

Response

```
{
  "log": "<log file>"
}
```

SysLog configuration download

Retrieve the Syslog configuration files.

“syslog” content must be in <zip> format and must contain all the syslog configuration files present in the device.

Request

GET https://<hostname>:<port>/securityConfigurations/v1/syslogService/syslog

Response

```
{
  "syslog": "<syslog files>"
}
```

System functions

Device restart

Request

POST https://<hostname>:<port>/securityConfigurations/v1/systemFunctions/restart

Reset of the factory configurations by removing all data and restoring initial configurations

Request

POST https://<hostname>:<port>/securityConfigurations/v1/systemFunctions/reset

Updates

Upload security update or firmware file

Request

POST https://<hostname>:<port>/securityConfigurations/v1/update/upload

```
{
  "update": "<update file>"
}
```

Configuration of the repository for the package management system

Request

POST https://<hostname>:<port>/securityConfigurations/v1/update/repository

```
{
  "repositoryURL": "<repository URL>"
}
```

Configuration of the URL of the update filename

Request
POST https://<hostname>:<port>/securityConfigurations/v1/update/download
{
"filenameURL": "<filename URL>"
}

Start the update
NOTE: filename it's without pathname

Request
POST https://<hostname>:<port>/securityConfigurations/v1/update
{
"filename": "<file name>",
"type": "<upload|download|repository>",
"scheduling": "DDMMYYYY-HH:MM"
}

In case of update in realtime, scheduling can be empty.
If type is "upload" the update will use the file previously uploaded
If type is "downwload" the update will be downloaded at the previously defined filename URL
If type is "repository" the update will be downloaded with the package management system at the previously defined repository URL

Information and characteristics of the device

Retrieve the information of the device

Request
GET https://<hostname>:<port>/securityConfigurations/v1/deviceInformation

Response
```
{
  "Manufacturer": "<Manufacturer>",
  "ProductName": "<Product Name>",
  "Version": "<Version>",
  "SerialNumber": "<SerialNumber>",
  "FirmwareVersion": "<Firmware version>",
  "OperatingSystemVersion": "<Operating System version>",
  "Patching Level": "<PatchingLevel>",
  "Kernel version": "<KernelVersion>",
  "httpsServerVersion": "<https server version>",
  "ApplicationSoftwareVersion": "<Application Software version>"
  "MAC address": "<MAC address>",
  "Memory size": "<Memory>",
  "Memory usage": "<Memory usage>",
  "CPU size": "<CPU size>",
  "CPU usage": "<CPU usage>",
  "HDD size": "<HDD size>",
  "HDD usage": "<HDD usage>",
  "Production timestamp components": "<Production timestamp components>",
  "NTP version": "<NTP version>",
  "SSH version": "<SSH version>",
  "OperatingSystemBIT": "<Operating System BIT>",
}
```

NOTE: Serial number must be univocal for any device
CPU usage must be given in percentage