Power Quality Instrument – Cyber security requirements

This global standard define the characteristics of the fixed installed indoor Power Quality Instrument (according to IEC 62586-1) and accessories for measurement of power quality parameters in a.c. distribution systems with a declared fundamental frequency of 50 Hz or 60 Hz.

Countries' I&N	Elaborated by	Collaborations by	Verified by	Approved by
Argentina	-	-	-	**Federico Luis Cetrangolo**
Brazil	-	-	-	**Amadeu F. De Macedo**
Chile	-	-	-	**Daniel González**
Colombia	-	-	-	**Juan Gómez**
Iberia	-	-	**José María Romero Gordón** **Juan Miguel González Provost**	**Maria Avery**
Italy	-	-	-	**Gianluca Sapienza**
Peru	-	-	-	**Robert Sánchez**
Romania	-	-	-	**Vasilica Obrejan**

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

Revision	Date	List of modifications
01	04.03.2021	First release

INDEX

1. ACRONYMS 4

2. SCOPE OF THE WORK 5

3. REFERENCES 6

3.1. FOR ALL COUNTRIES 6

3.2. FOR ALL COUNTRIES 6

4. REPLACED STANDARDS 6

5. PQI CYBER SECURITY REQUIREMENTS DESCRIPTION 7

6. PQI HARDWARE CYBER SECURITY REQUIREMENTS 7

6.1. HARDWARE ARCHITECTURE 7

6.1.1 Hardware Platform 7

6.1.2 Security-specific functions 8

6.1.3 Interfaces and physical ports/connectors security 8

6.2. HARDWARE SOLUTIONS 9

6.2.1 Anti-intrusion mechanisms 9

6.2.2 Concealment of the components 10

6.2.3 Power supply control 11

7. PQI FIRMWARE CYBER SECURITY REQUIREMENTS 12

7.1. FEATURES OF THE OPERATING SYSTEM 12

7.1.1 Bootloader 12

7.1.2 Operating System 12

7.2. MIDDLEWARE COMPONENTS 14

7.2.1 Remote Management functionalities of the device 14

7.2.2 Security of the Software code developed by the Supplier 15

7.2.3 Required Security Software 16

7.2.4 Remote Management Software 16

7.3. HARDENING 17

7.3.1 Hardening Guideline 17

7.3.2 Security Logging 18

7.3.3 Cellular Data Communications 19

7.4. SECURITY PATCHING 19

7.4.1 Updates during the PQI supply 19

7.4.2 Security updates during the PQI operation 20

7.4.3 Update Security 21

7.5. USERS, CREDENTIALS AND CERTIFICATES MANAGEMENT 21

7.5.1 Credentials Security 21

7.5.2 Centralized authentication 22

7.5.3 Certificates and Cryptographic Keys 22

7.5.4 Update of certificates and cryptographic keys 22

7.5.5 Techniques for the protection of the administrative access to the device 23

8. DOCUMENTARY REQUIREMENTS 24

8.1. DETAILED TECHNICAL DOCUMENTATION TO BE PROVIDED 24

8.1.1 Required technical details 24

9. CYBER SECURITY REQUIREMENTS BIDDING FORM 25

10. ANNEX 1 - SECURITY CONFIGURATIONS API 27

GENERAL INFORMATION 27

XWS authentication 27

Activation and deactivation of the service ssh 28

NETWORK SERVICES CONFIGURATION 29

FIREWALL SERVICE 31

Activation and deactivation of the firewall service 31

bulk download or bulk upload of iptables (or similar) rules configuration file *31*
CREDENTIALS/KEYS SERVICE 32
Bulk Download *32*
Web server users *33*
Upload update and get of Cryptographic Keys and Digital Certificates *34*
SYSLOG SERVICE 35
Configuration *35*
Log download *36*
SysLog configuration download *36*
SYSTEM FUNCTIONS 36
UPDATES 36
INFORMATION AND CHARACTERISTICS OF THE DEVICE 37

TABLES

Table 1 – PQI Cyber Security - Level of compliance with the requirements 25

ANNEX

Annex 1 – Security Configurations API 27

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. **DNF** Dandified YUM (software package manager)
f. **DS** Distribution Substation
g. **FW** Firmware
h. **GS** Enel Global Standard
i. **HW** Hardware
j. **HV** High Voltage
k. **JTAG** Joint Test Action Group
l. **CPU** PQI main processor
m. **MV** Medium Voltage
n. **NTP** Network Time Protocol
o. **OS** Operating System
p. **PCB** Printed Circuit Board
q. **RADIUS** Remote Authentication Dial-In User Service
r. **REST** REpresentational State Transfer
s. **SFTPD** Secure FTP Daemon
t. **Syslog-ng** System Log next generation
u. **SR_XX** Security Requirement (XX type, e.g. SW = software)
v. **SSH** Secure Shell
w. **SSL** Secure Sockets Layer
x. **SSD** Solid State Disk
y. **SW** Software
z. **TCP** Transmission Control Protocol
aa. **TLS** Transport Layer Security
bb. **TPM** Trusted Platform Module

2. SCOPE OF THE WORK

The Cyber Security requirements for Power Quality Instrument have been defined for the Enel product “PQI” (GSTQ001 and GSTQ002). However, these requirements may be adopted in other similar devices and so it could be used as reference in the device technical specifications.

3. REFERENCES

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

3.1. For all countries

IEC 61850 series	Communication networks and systems for power utility automation
Enel CSG 12	Cyber Security Guideline no. 12 – Version no.2 dated 08/10/2019 Enel Operational Technologies (OT) security guideline on industrial control systems
Enel CSG 7	Cyber Security Guideline no.7 – Version no.2 dated 30/09/2017 Enel “IT Security Guidelines - APPLICATIONS”

3.2. For all countries

Countries should kindly declare the applicable local standards.

4. REPLACED STANDARDS

5. PQI CYBER SECURITY REQUIREMENTS[1] DESCRIPTION

The security requirements belong to three categories:

- **Hardware security requirements**: this section includes the Hardware requirements that "strengthen" the PQI 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 PQI 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.
Be reminded that the Supplier shall size hardware capabilities of the PQI device taking into account the adequate performance requirements of both application services and security features.

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

6. PQI HARDWARE CYBER SECURITY REQUIREMENTS

6.1. Hardware Architecture

This section contains the Hardware architecture requirements necessary to guarantee the security requirements.

6.1.1 Hardware Platform

6.1.1.1 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.

6.1.1.2 SR_HR_02

Requirement type: **Mandatory**

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

6.1.1.3 SR_HR_03

Requirement type: **Mandatory**

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

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

6.1.1.4 SR_HR_04

Requirement type: **Mandatory**

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

6.1.2 Security-specific functions

6.1.2.1 SR_HR_05

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).

6.1.2.2 SR_HR_06

Requirement type: **Mandatory**

The CPU or any additional component in the PQI must provide the following security feature:

- the integrity validation of the PQI Bootloader or Firmware, by verifying their digital signature during the device start-up, through the use of the Secure Boot.

As an example, please, refer to the Arm Trusted Firmware[3] functionality.

6.1.2.3 SR_HR_07

Requirement type: **Optional**

The PQI should support the complete encryption of its Flash memory through algorithms that are currently classified as secure in the reference document published by the ECRYPT-CSA "*D5.4 Algorithms, Key Size and Protocols Report*" (latest available version). A secure storage system (according to the Anti-tampering mechanisms) for the archiving of the encryption keys or of the certificates can be provided.

6.1.3 Interfaces and physical ports/connectors security

6.1.3.1 SR_HR_08

Requirement type: **Mandatory**

During the operation of the PQI, the programming and/or debugging interfaces must be blocked at HW level. Therefore, the Supplier is requested to remove all the programming ports available on the electronic boards of the PQI intended for the operation in the substations (particular care must be taken of the JTAG interfaces).

This requirement can be waived only for PQIs 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[4].)

[2] https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf
[3] https://www.arm.com/products/security-on-arm/trustzone
[4] https://www.digi.com/resources/documentation/digidocs/90001546/concept/trustfence/c_secure_jtag_android.htm

6.1.3.2 SR_HR_09

Requirement type: **Mandatory**

All of the physical interfaces and ports not expressly required by the Enel functional specifications, according to this security annex, must be blocked at Hardware level (e.g. USB ports, additional serial interfaces, etc.). In addition, with exception of the cellular interface (see also § 7.3.3), wireless interfaces (e.g. Bluetooth, Wi-Fi, Infrared, etc.) are not allowed. In any case, it must be possible to software block any physical and software interface of the device.

6.2. 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.

6.2.1 Anti-intrusion mechanisms

6.2.1.1 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.

6.2.1.2 SR_HR_11

Requirement type: **Mandatory**

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

6.2.1.3 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.

6.2.1.4 SR_HR_13

Requirement type: **Optional**

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

6.1.3.3 SR_HR_14

Requirement type: **Mandatory**

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

- one or more switches must be provided to detect the PQI modules opening (for example the modem module);
- 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, at least, a security event (log and syslog).

Furthermore the device must be able to detect possible manipulation of the modem kit and GPS kit (e.g. extraction of the SIM or the modem itself).

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

6.1.3.4 SR_HR_15

Requirement type: **Optional**

The device should be equipped with Tamper Detection solutions able to work even if the PQI 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 PQI (according to the requirement SR_HR_11).

6.1.3.5 SR_HR_16

Requirement type: **Optional**

In addition to the requirement SR_HR_14, the device should be able to trigger the following Tamper Response solutions/actions:

- 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.

6.2.2 Concealment of the components

6.2.2.1 SR_HR_17

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.

6.2.2.2 SR_HR_18

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.

6.2.2.3 SR_HR_19

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.

6.2.2.4 SR_HR_20

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.

6.2.3 Power supply control

6.2.3.1 SR_HR_21

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. PQI 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 PQI configurations and the device management and maintenance over time.

In this document the term Firmware means the entire set of the PQI 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.

7.1. Features of the Operating System

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

7.1.1 Bootloader

7.1.1.1 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. No Bootloader lock password shall be present in the device Bootloader.

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.

7.1.2 Operating System

7.1.2.1 SR_SW_02

Requirement type: **Mandatory**

The Supplier shall equip the PQI with a Unix type OS such as Linux, FreeBSD or QNX. In any case the Operating System must have, at least, the following characteristics:

- updatable and extensible in terms of functionality during the service life of the PQI;
- maintained by a Supplier or a community providing updates and Security Patches;
- replaceable if discontinued and, therefore, independent of the CPU 's hardware Manufacturer;
- generated through "Yocto Project[5]" or a similar framework that guarantees the same functionality in terms of upgradeability and flexibility. The framework must be of the latest version available and supported by the CPU. Enel suggests to use the Poky distribution or a distribution derived from it;
- the latest final OS version or distribution branch must be used (release candidate or beta versions are not allowed).

[5] https://www.yoctoproject.org/
https://www.freebsd.org/community.html
https://github.com/mark-nicholson/poky

At the time each PQI 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.

Note: in case of Operating Systems generated using Yocto, the 5 (five) years stablished in requirement are not mandatory but the support (non deprecate status) should last longer as possible and guaranteed by the producer/maintainer.

7.1.2.2 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[6], SSH[7];

7.1.2.3 SR_SW_04

Requirement type: **Mandatory**

Every PQI 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 PQI with Enel Public Key Infrastructure for Certificate Management (enrolment/renewal/revocation/status validation, etc.), the device must support also the following protocols and reference standards:

- CMP (Certificated Management Protocol) -> RFC 4210[A]
- EST (Enrollment over Secure Transport) -> RFC 7030[B]
- OCSP (Online Certificate Status Protocol) -> RFC 6960[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 the ECRYPT-CSA[2] "*D5.4 Algorithms, Key Size and Protocols Report*" (latest available version).

[A] https://tools.ietf.org/html/rfc4210
[B] https://tools.ietf.org/html/rfc7030
[C] https://tools.ietf.org/html/rfc6960

[6] https://en.wikipedia.org/wiki/Transport_Layer_Security
[7] https://en.wikipedia.org/wiki/Secure_Shell

7.2. Middleware Components

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

7.2.1 Remote Management functionalities of the device

7.2.1.1 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 PQIs, such as:

- SSH service configuration:
  - activation/deactivation of the service (activated by default),
  - Public Keys addition and removal in "authorized_keys";
- Network services configuration:
  - NTP server configuration for clock synchronization (or GPS source),
  - system hostname configuration,
  - system DNS configuration,
  - IP addresses (IPv4 and IPv6) configuration (with subnet mask and default gateway too);
- Firewall service:
  - activation/deactivation,
  - bulk download or bulk upload of Iptables (or similar) 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:
  - supporting the factory reset feature, by removing all data and restoring initial configurations (original manufacturer settings). The erasing method used in the factory reset feature (data clearing) must completely remove all data residing on the flash memory by using random sequences of zeros and ones to overwrite data onto all sectors of the device, rendering the data unrecoverable (or hard to recover) and achieving the data sanitization,
  - 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 information (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

7.2.1.2 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 every time API method is mentioned. Furthermore, these APIs must share same channel of the Web application (coexistence).

7.2.2 Security of the Software code developed by the Supplier

7.2.2.1 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".*

Furthermore, Web applications or API produced by the Supplier must be free of vulnerabilities according to the OWASP Top Ten[8] (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, discrepancies with the requirements in the Enel guidelines are identified.

7.2.2.2 SR_SW_08

Requirement type: **Mandatory**

All applications developed by the Supplier running on the PQI must perform the tracking of the security logs by generating a 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 high importance administrative operations performed on the device (as described in SR_SW_16);
- all the administrative operations performed on the SIM and Cellular modem (e.g. extraction of the SIM, no synchronization, loss of the communication with the modem, etc.).

7.2.2.3 SR_SW_09

Requirement type: **Mandatory**

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

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

7.2.2.4 SR_SW_10

Requirement type: **Optional**

If the Supplier executes Security Static Code Analysis with own tools[9], aimed at identifying potential security vulnerabilities in the code he developed, when issuing the PQI, 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.

7.2.3 Required Security Software

7.2.3.1 SR_SW_11

Requirement type: **Mandatory**

The PQI 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 (or similar) with related dependencies (libraries and Kernel modules);
- OpenSSH;
- OpenSSL or LibreSSL;
- SELinux or similar (for example, MAC in FreeBSD);
- RADIUS centralized authentication modules;
- LDAP and LDAPs;
- Syslog-ng daemon;
- NTP daemon;
- Bash or sh scripting environment.

7.2.3.2 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:

- 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.

7.2.4 Remote Management Software

7.2.4.1 SR_SW_12

Requirement type: **Mandatory**

The supplier must equip the device with a web interface to manage the functionality of the application software and security configurations.

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

7.3. Hardening

This section specifies the security configurations (Hardening) the PQI 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.

7.3.1 Hardening Guideline

7.3.1.1 SR_SW_13

Requirement type: **Mandatory**

The Supplier shall configure the PQI so that the only daemons or (IP) network services are the ones authorized by Enel, according to the following list:

- Web Server relying on the https service, using TCP port 443, for exposing Web interfaces/device management APIs;
- Secure Shell relying on the SSH service, using TCP port 22, for administrative access to the device;
- Services and protocols strictly required by the communications of the device applications.
- 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.

7.3.1.2 SR_SW_14

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[10];
- Web server selected by the Supplier[11];
- Operating system.

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

7.3.1.3 SR_SW_15

Requirement type: **Mandatory**

For the following functions only:

- Clock update via NTP and other authorized synchronization protocols;
- Modbus RTU;
- Sending log messages via Syslog;
- Radius

the use of unencrypted (IP) network communications, although the PQI is required to natively support the secure versions too, could be approved by Enel just in particular circumstances; in this cases, the

[10] https://wiki.centos.org/HowTos/Network/SecuringSSH

[11] https://www.owasp.org/index.php/SCG_WS_nginx, https://www.owasp.org/index.php/SCG_WS_Apache

communications must be secured via Network Security technologies/solutions (e.g. enabling/configuring security features in the network devices).

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 PQI, 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 PQIs as described in the previous paragraph, the Supplier shall implement methods to update the PQI in order to replace the algorithms that will be considered insecure with secure ones.

Be reminded that through the Cellular interface only secure protocols (based on TLS or SSH) are allowed, not secure protocol must be approved by Enel before their implementation.

7.3.2 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 PQI in a way that it will be able to trace the operations performed on/by the device.

7.3.2.1 SR_SW_16

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

- Successful user login to the system through any implemented interface in remote/local access (e.g. SSH access, Web access, API access, PQI 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 PQI Management SW;
- Extraction/Insertion of the SIM
- 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 (Enel SIEM) system by using syslog protocol (according for example to RFC 5424) and following Enel Guideline 10 "Infrastructural Security" prescriptions.

Furthermore, the PQI must also log the following events and send them through Syslog:

- Loss of communications between the PQI 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.

7.3.2.2 SR_SW_17

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.

7.3.3 Cellular Data Communications

7.3.3.1 SR_SW_18

Requirement type: **Optional**

The PQI shall use embedded-SIM (eSIM).

7.3.3.2 SR_SW_19

Requirement type: **Mandatory**

The APN auth key provided by Enel must be properly managed as defined in the requirement SR_SW_26.

7.4. Security Patching

The Firmware of the PQI is equipped with Software components 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 PQI software be updatable with security patches that guarantee the requested level of device security over time.

7.4.1 Updates during the PQI supply

7.4.1.1 SR_SW_20

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[12]), 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.
This requirement is applicable also to the internal modem (if provided).

[12] https://www.cvedetails.com/

7.4.2 Security updates during the PQI operation

7.4.2.1 SR_SW_21

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[13] 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 PQI.

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.

7.4.2.2 SR_SW_21bis

Requirement type: **Mandatory**

The Firmware of the PQI Modem must be updatable and extensible in terms of functionality during the service life of the PQI and the updates shall be issued by the Supplier as defined in SR_SW_21.

7.4.2.3 SR_SW_22

Requirement type: **Mandatory**

The device must be equipped with the following update methods:

- manual installation on the device via Web interface
- update via API;
- It should be possible to upload the update on the device via SSH service
- update via centralized repository (through DNF[14] or similar).

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).

[13] “made public” means published on the (Web) sites of the reference software-house

[14] https://en.wikipedia.org/wiki/DNF_(software)

- 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_16.
- 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.

7.4.2.4 SR_SW_23

Requirement type: **Mandatory**

In the event that a security update is required when a supply is in progress (ref. SR_SW_21), the devices to be supplied must already include it.

7.4.3 Update Security

7.4.3.1 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 traced via the syslog service and the event must be sent to the ENEL SIEM.

7.5. Users, credentials and certificates management

7.5.1 Credentials Security

7.5.1.1 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 privileged approach.
- Anti-brute-force login protection (time and attempts lock).

This requirement is applicable also to the internal modem (if provided).

7.5.1.2 SR_SW_26

Requirement type: **Mandatory**

"Hardcoded" credentials, which 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, the methodology used must be described and communicated to ENEL before the implementation.

7.5.2 Centralized authentication

7.5.2.1 SR_SW_27

Requirement type: **Mandatory**

The PQIs 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.

7.5.3 Certificates and Cryptographic Keys

7.5.3.1 SR_SW_28

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*)

7.5.3.2 SR_SW_29

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*”).

7.5.4 Update of certificates and cryptographic keys

7.5.4.1 SR_SW_30

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.

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

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

7.5.5.1 SR_SW_31

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.

7.5.5.2 SR_SW_32

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 (“`SecurityAdministrator`”) user that can only modify the security parameters and configurations as defined in SR_SW_05.

8. DOCUMENTARY REQUIREMENTS

8.1. Detailed Technical Documentation to be provided

8.1.1 Required technical details

8.1.1.1 SR_DC_01

Requirement type: **Mandatory**

The Supplier, in addition to the supply of the PQI, shall provide detailed documentation and software regarding the adopted security configurations, highlighting all the aspects of compliance with the requirements in this GS. 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 requirements 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 detail 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.

9. CYBER SECURITY REQUIREMENTS BIDDING FORM

The Supplier/Bidder shall fill the following table, related to the Cybersecurity requirements described in Chapters 6, 7 and 8.

Table 1 – PQI Cyber Security - Level of compliance with the requirements					
N.	**Technical Specification**	**Mandatory**	**Yes**	**No**	**Remarks for any deviation or notes**
6.1 HW Cyber security requirements - Architecture					
SR_HR_01		x			
SR_HR_02		x			
SR_HR_03		x			
SR_HR_04		x			
SR_HR_05		x			
SR_HR_06		x			
SR_HR_07					
SR_HR_08		x			
SR_HR_09		x			
6.2 HW Cyber security requirements – HW solutions					
SR_HR_10		x			
SR_HR_11		x			
SR_HR_12					
SR_HR_13					
SR_HR_14		x			
SR_HR_15					
SR_HR_16					
SR_HR_17		x			
SR_HR_18					
SR_HR_19					
SR_HR_20					
SR_HR_21					
7.1 PQI FW Cyber security requirements – Features of the OS					
SR_SW_01		x			
SR_SW_02		x			
SR_SW_03		x			
SR_SW_04		x			
7.2 PQI 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		x			
7.3 PQI 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					
SR_SW_19		x			
7.4 PQI FW Cyber security requirements – Security Patching					
SR_SW_20		x			
SR_SW_21		x			

Table 1 – PQI Cyber Security - Level of compliance with the requirements					
N.	**Technical Specification**	**Mandatory**	**Yes**	**No**	**Remarks for any deviation or notes**
SR_SW_21bis		x			
SR_SW_22		x			
SR_SW_23		x			
SR_SW_24		x			
7.5 PQI 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			
8.1 Detailed Technical Documentation to be provided					
SR_DC_01		x			

ANNEX

10. 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, which 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 PQI 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 addition

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>"
  }
]
```

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>”
  ],
  "dhcp": "<ip address_dhcp server>",
  "ntpServers": [
    "<ntp server 1>",…,
    "<ntp server N>"
  ]
 }
```

Retrieve network services configuration info (IPv6)

Request

```
GET   http://<hostname>:<port>/securityConfigurations/v1/networkServicesConfigv6
```

Response

```
{
"ipAddressesv6": [
      {"ipAddressv6":"<ipv6 address 1>","prefixLength":"<prefix length 1>",
"defaultGatewayv6":"<default gatewayv6 1>", ”nic”:”<network interface card>”,
“mode”: “<DHCP/SLAAC/FIXED>” },
      {"ipAddressv6":"<ipv6 address N>"," prefixLength":"<prefix length 2>",
"defaultGatewayv6":"<default gatewayv6 N>", ”nic”:”<network interface card>”,
“mode”: “<DHCP/SLAAC/FIXED>” }
  ],
  "dnsv6": [
    "<ipv6 dns server 1>",…,
    "<ipv6 dns server N>”
  ],
  "ntpServersv6": [
    "<ntpv6 server 1>",…,
    "<ntpv6 server N>"
 ]
}
```

Update Network service configuration info (IPv4)

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>”
  ],
  "ntpServers": [
    "<ntp server 1>",…,
    "<ntp server N>"
 ]
}
```

Update Network Dynamic service configuration info

Request

```
POST  https://<hostname>:<port>/securityConfigurations/v1/networkDynamicConfig
{
  "hostname": "<hostname>",
  "dns": [
    "<ip dns server 1>",
    "<ip dns server N>”
  ],
  "dhcp": True/False,
  "ntpServers": [ "<ntp server 1>", …, "<ntp server N>" ]
}
```

NOTE: items marked in grey may not be necessary when DHCP mode is set.

Update Network service configuration info (IPv6)

Request

```
POST  https://<hostname>:<port>/securityConfigurations/v1/networkServicesConfigv6
{
"ipAddressesv6": [
      {"ipAddressv6":"<ipv6 address 1>","prefixLength":"<prefix length 1>",
"defaultGatewayv6":"<default gatewayv6 1>", "nic":"<network interface card>",
"mode": "<DHCP/SLAAC/FIXED>" },
      {"ipAddressv6":"<ipv6 address N>"," prefixLength":"<prefix length 2>",
"defaultGatewayv6":"<default gatewayv6 N>", "nic":"<network interface card>",
"mode": "<DHCP/SLAAC/FIXED>" }
  ],
  "dnsv6": [
    "<ipv6 dns server 1>",
    "<ipv6 dns server N>"
  ],
  "ntpServersv6": [
    "<ntpv6 server 1>", …,
    "<ntpv6 server N>"
 ]
}
```

NOTE: items marked in grey may not be necessary when DHCP mode is set.

Firewall service

Activation and deactivation 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 (or similar) 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/changePassw
ord
{
  "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 PQI;
- "X509" X509 Certificates pair for the https service; these Certificates must be different on each PQI;
- "Public Key" Public Key pool for the remote access via SSH; these Certificates must be different on each PQI;
- "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 PQI;
- "X509" X509 Certificates pair for the https service; these Certificates must be different on each PQI;
- "Public Key" Public Key pool for the remote access via SSH; these Certificates must be different on each PQI;
- "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

Update Syslog service configuration info (IPv4)

Request

```
POST  https://<hostname>:<port>/securityConfigurations/v1/syslogServiceIpv4
{
  "syslogServers": [
    "<ip syslog server 1>",…,
    "<ip syslog server N>"
 ]
}
```

Retrieve Syslog service configuration info (IPv4)

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>"},
}
```

Retrieve Syslog service configuration info (IPv6)
Request

```
GET   https://<hostname>:<port>/securityConfigurations/v1/syslogService/configv6
```

Response

```
{
  "destinationServerIPv6": [
      {"ipv6":"<destination server IPv6 1>","port":"<port N>", "protocol":"<protocol
1>"},
      {"ipv6":"<destination server IPv6 N>","port":"<port N>", "protocol":"<protocol
N>"}
  ]
}
```

Log download

Retrieve the system Log.
Log must be in <zip> format with BASE64 encoding 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 with BASE64 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

Factory reset, by removing all data and restoring initial configurations (original manufacturer settings).
Request

```
POST  https://<hostname>:<port>/securityConfigurations/v1/systemFunctions/resetFactory
```

Device restart
Request

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

Updates

Upload security update or firmware file in BASE64 encoding.
Request

```
POST  https://<hostname>:<port>/securityConfigurations/v1/update/upload
{
  "update": "<update file>"
}
```

Configuration of the repository for the package management system.
NOTE: “update” parameter is ALWAYS encoded to BASE64 format.
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 is 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>",
  "SIMnumber": "<SIM number>",
  "MobileOperator": "<Mobile Operator>",
```

```
  "IMEI": "<IMEI>",
  "SIM CCID": "<SIM CCID>",
}
```

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