# Cyber security requirements for protection and control devices

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 | - | - | - | **Carlos Espinoza** |
| Brazil | - | - | - | **Romulo Thardelly** |
| Chile | - | - | - | **Daniel Gonzalez** |
| Colombia | - | - | - | **Juan Gomez** |
| Iberia | - | - | - | **Maria Avery** |
| Italy | - | - | - | **Gianluca Sapienza** |
| Peru | - | - | - | **Robert Sanchez** |
| Romania | - | - | - | **Vasilica Obrejan** |

| | Elaborated by | Collaborations by | Verified by | Approved by |
|---|---|---|---|---|
| **Global I&N – NTI** | **Gennaro Fiorenza<br>Daniel Garcia Miralles** | - | **Gennaro Fiorenza<br>Christian Noce** | **Fabio Giammanco** |



| Revision | Data | List of modifications |
|---|---|---|
| 01 | 06.12.2018 | First approved edition |

**INDEX**

## TABLES

# 1 ACRONYSM

a. **IED** Intelligent Electronic Device

b. **RTU** Remote Terminal Unit

c. **SCADA** Supervisory Control And Data Acquisition

d. **ICS** Industrial Control System

e. **JTAG** Joint Test Action Group

f. **PCB** PRINTED CIRCUIT Board

g. **ROM** Read Only Memory

h. **NRND** Not Recommended for New Design

i. **SNMP** Simple Network Management Protocol

j. **OT** Operational Technology

k. **CVSS** Common Vulnerability Scoring System

l. **TCP** Transmission Control Protocol

m. **NTP** Network Time Protocol

n. **DNS** Domain Name System

o. **SSH** Secure Shell

p. **SQL** Structured Query Language

q. **PKI** Public Key Information

r. **GS** Global Standard

## 2 SCOPE OF THE DOCUMENT

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 – GSTPXXX product family and description**

| GSTPXXX type | Product family code | Description |
|---|---|---|
| All | GSTPXXX | Protection and control devices |

# 3 NORMATIVE REFERENCES AND BIBLIOGRAPHY

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

## 3.1 For all countries

| | |
|---|---|
| IEC 61850 series | Communication protocols for IED at electrical substation |
| 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<br>ENEL Operational Technologies (OT) security guideline on industrial control systems |

# 4 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 GSTPXXX 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 SCADA 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.

# 5 IED CYBER SECURITY REQUIREMENTS

Hardware and Software cyber security requirements are summarized in this chapter.

In responding to the cyber security requirements described below, the Supplier must describe any security functions or feature proposed for each requirement.

Supplier must also provide high-level evidence of the implementation methods planned to meet the minimum prerequisites following referred, making clear, in particular, any significant differences from the standard mechanisms typically used for this purpose, including with regard to the OS platform or the hardware components selected.

## 5.1 Hardware security requirements of the device

In consideration of the public cyber security guidelines, typical interface in IEDs, such as, for example, JTAG, programming PIN, debug PIN, RS232 PIN and, generally, interfaces with the system or its components, represent potential points of compromise of the devices since they have physical access to it, so the following are required:

**(R.5.1.1)** The provision of hardened enclosures containing the board (PCB). For example, anti-tamper techniques can be used (equipping the box with active sensors, which are able to allow any tamper event real time transmission or to store the event itself, in case of remote communication unavailability, non-standard format screws, etc... In general any kind of solution must avoid an easy disassembly of the protection and track any unauthorized hardware handling.

**(R.5.1.2)** Hardware memory supports (for example, flash ROM) to 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).

**(R.5.1.3)** The debug/program interfaces PINs must be removed from the board. If necessary, it's allowed only the footprints, without descriptive labels and declaring their presence to Enel.

**(R.5.1.4)** Top side markings must be restricted to what is strictly necessary.

**(R.5.1.5)** Ethernet ports in IEDs (copper or optical) are able to provide various ways of access to the system. During the device operation, such Ethernet ports must be the only access and management method and any other interface must be removed or disabled.

Unused Ethernet ports must be disabled by software configuration. Eventually and if necessary, it should be possible to enable again these interfaces by software configuration. In case of Enel request, testing or troubleshooting samples, board or test components, such as, for example, samples dedicated to Enel laboratories, previous physical security requirements ((R.5.1.1) – (R.5.1.5)) could not be applied.

**(R.5.1.6)** Furthermore, during the definition of the logic architecture of the device, the Supplier must use modern microcontrollers with enough computing resources able to support the operating system update, maintenance and to provide the security requested in this specification. Therefore, when Enel will purchase the protections, the Supplier must declare and provide devices equipped with microcontrollers which are not defined "outdated" (i.e. End-of-Support, End-of-Life, Legacy or NRND), from the purchasing time to the next five (5) years. This condition enables the software development and maintenance stream setting.

## 5.2 Firmware security requirements

The term "firmware" refers to any kind of software running on the protections.

The Supplier must provide devices equipped with firmware, which is compliant to the security requirements described in the following paragraphs and especially according to three main issues:

a. **Device updating:** the firmware must be able to be updated (if necessary, in its entirety) with security patches, designed to mitigate security bugs of any component (i.e. libraries, operating systems binary releases, kernel, applications, etc.). Moreover, it must be possible to add new security features on the

operating devices (in the field). Instances of possible additional security features could be, for example, a SNMP daemon or Radius centralized authentication support.

b. **Security hardening**: the firmware must be configured in secure mode, as described in the following sections.

c. **Basic software required on the IED protections**: devices supplied may be connected to the remote management platforms of Enel OT devices; therefore, they must be equipped with the proper software.

### 5.2.1 Device updating service

**(R.5.2.1.1)** Legacy or unpatched software on board can be affected by serious vulnerabilities, which can be exploited by a Threat Actor, such as a malware or an attacker, to perform unauthorized actions within the system, making changes to the calibration parameters or the activation/deactivation of the switches. Such vulnerabilities may be also unknown at the time the device is provided.

To avoid this kind of security problems and in order to limit as possible the risk, the Supplier must support firmware security updates **for the complete duration of the contract**. It means as long as the contract is in being, the Supplier must provide support by analyzing new vulnerabilities and releasing software updates (security patches) designed to resolve security problems. This activity is subject to Enel check.

The security patching could be needed:

a. after a Security Assessment by Enel or a third-party company;

b. when a new vulnerability, with impacts on the systems/devices, has discovered (by bulletins, CERTs, communities, …), for example, zero-day vulnerabilities;

c. in case of a targeted computer attack;

d. when, proactively, the Supplier itself considers the need for applying a security patch.

The Supplier must be ready to release the security patch within 1 month from the ENEL request. In advance and by its own means, the Supplier must check the security patches on any device, which is provided within the contract with Enel.

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.

**(R.5.2.1.2) Firmware update status expected on release of the supply**

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.

Unless explicitly authorized by Enel, the provided applications, installed on the devices, must not run security vulnerabilities classified as CVSS v3>4 (please refer to https://www.first.org/cvss/). In the event of failure to meet this prerequisite, any mitigation and the respective update costs shall be Supplier responsibility.

**(R.5.2.1.3) Distribution methods of the update packages**

In case of need of update-packages delivery on field devices, Enel will carry it out.

The Supplier is required to provide protections with an update function, with, at least, the following functional characteristics:

a. It should be possible to promptly upload and install the update by using the management web interface of the protection;

b. 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:

c. Hash verification of the transferred update package to the device before installation.

d. Compatibility verification of the update package with the firmware update status (including the resolution of dependencies)

e. 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.

f. Robustness of the update process. If the update is not correctly installed, the device system must automatically perform the roll-back procedure.

g. Protection from brick/lock states during the update procedure.

h. Tracking of the update activity, including data, state and result (by using syslog as described in sections ((R.5.2.2.1), (R.5.2.2.5), and 5.2.3).

i. 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 the possibility to find, in remote substations, low-performance telecommunication connection, where possible, the updates must 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.

In case of security update request by Enel and application by the Supplier, also devices already released by the Supplier must include the new updated firmware.

**(R.5.2.1.4)** Optionally, the Supplier can propose a “repository” type updating method by which the devices, once authorized, autonomously 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.

### 5.2.2 Security hardening

In this section the security conditions (hardening), that IED must comply with, are listed. These configurations can reduce the vulnerability risk and the perimeter of compromise of the device.

**(R.5.2.2.1) Hardening Guideline:**

The supplier must configure in the device only daemons or network services (IP) authorized by ENEL, these will be:

a. Web Server on https by using TCP port 443: Web/API interface to control the device.

b. Secure Shell on SSH by using TCP 22 port: administrative access to the device.

c. Services and protocols strictly related to the applicative communication of the device (example, protocol IEC 61850).

d. Syslog client by using UDP port 514: as transmission logging protocol.

e. 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).

The use of any other network service available in the device must be authorized by ENEL only after a deep analysis of the motivation provided by the supplier.

**(R.5.2.2.2)** All the physical management access interfaces to the device, not required by this GS and not removed during hardware design, must be disabled by software (i.e. added network interface like serial…). In this way the interface will not be available in any state or condition of the device.

**(R.5.2.2.3)** The firmware configuration must follow security configuration guidelines (based on software choice) for:

a. SSH service

b. Web server identified by supplier

c. Linux Operating System

These guidelines, if not clearly indicated by ENEL during the contract preliminaries, can be chosen by the Supplier from public guidelines, but they must be communicated to ENEL.

Examples of public guidelines to the following website:

d. https://linux-audit.com/audit-and-harden-your-ssh-configuration/ ( SSH service)

e. https://geekflare.com/nginx-webserver-security-hardening-guide/https://geekflare.com/apache-web-server-hardening-security/ ( Web server identified by supplier)

f. https://www.cyberciti.biz/tips/linux-security.html (Linux Operating System)

**(R.5.2.2.4)** Only following IP Communications are allowed without encryption:

a. Update clock by NTP and/or PTP (if present)

b. Log messages sent by Syslog

c. Communications between applications using automation standards (i.e. IEC 61850) or IoT protocols (i.e. mqtt)

If not approved by ENEL, any other communication protocols in the device must use security protocols supporting only encryption algorithms identified as secure during the entire service life of the device, as indicated in the ENISA document: “Algorithms, key size and parameters report 2014 (please ref. to https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014).

If the Supplier, for any technical reason, will propose different encryption algorithms considered secure at the time of the supply but not secure for the entire device service life, then, a method to update the device to make secure the ‘unsecure’ algorithm must be communicated by the Supplier.

**(R.5.2.2.5) Logging:**

Logs generated by the protections can be an essential element to Enel, in order to identify any attempt to compromise the ICS network. For this reason, the Supplier must provide protections with logging features. 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).

Following an essential list of events that must be logged by the device:

a. Authentication information through SSH (both success and failure).

b. Application authentication information (both success and failure).

c. User escalation.

d. Command execution through “su/sudo” commands.

e. User creation/modification (both system and application).

f. Forced system restarts.

g. Services/daemons crash.

In addition:

h. The use of the log files already provided by the operating system should be preferred rather than the creation of new ones. For example, using “audit logs” for access tracking to the system and system operations as dmesg, messages, kernels, boot, http/apache2 etc.

i. 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.

j. Logs must be sent and archived in compressed mode (for example, service through the logrotate service).

Additionally, the device must be able to send logs to at least two different log collection servers (syslog servers).

### 5.2.3 Basic software required on the IED protections

**(R.5.2.3.1)** IED will be connected to the remote management system of Enel’s OT devices. In order to guarantee the compliance the device must be provided with the following software applications, including all the related dependencies:

a. Enel will provide NTP client for clock synchronism and the configuration of the NTP servers (the same for PTP synchronization).

b. Network configuration with domain name resolution and the configuration of the DNS servers will be provided by Enel.

c. Personal Firewall (IPTABLES) feature. Initially, the policies will be set in the “permit-all” mode.

d. Syslog-ng daemon for the local collation of the logs and able by configuration to send also the logs to a remote server.

## 5.3 Code security

**(R.5.3.1)** The entire application code must be developed in accordance with secure development Frameworks. Enel suggests to adopt the “Stance” framework (http://www.stance-project.eu/media/Public_Deliverables/ STANCE_SLAB_DEL_D1.1_R0.47.pdf).

In any case Supplier must provide evidence of how cyber security requirements identified in chapter 8 have been taken in consideration.

Enel places particular emphasis on the security of the code of network services or daemons. Mainly because these components are the first elements under cyber security compromise risk.

## 5.4 WEB/API interface

**(R.5.4.1) Authentication interface in-depth**

Particular attention must be given to the device application interfacing methods, mainly with regard to users/passwords management (anywhere where applied).

In general, the device must be compatible with the following requirements:

a. The introduction of password complexity requirements (change password).

b. The provision of time-based lock-out credentials management techniques.

c. The definition of at least two user profiles, Administrator and Operator, necessary and enough for device management.

d. Anti-brute-force login protection (time lock).

e. Credential change via remote batch commands.

f. Possibility to ensure unique passwords, for example, by incorporating in the password itself part or the entire serial number of the device. In this case, Enel will notify to the Supplier, in the design stage of the protection, its intention.

**(R.5.4.2) Device** WEB applications or API produced by the Supplier must be free of vulnerabilities according to the OWASP Top Ten Application Security Risks (https: // www.owasp.org/index.php/Category: OWASP_Top_Ten_Project).

During the control, the Supplier must consider the last version available of the OWASP Top Ten list at the time of the supply.

## 5.5 SCADA/ICS applications

**(R.5.5.1)** The Supplier must provide evidence of the implementation of appropriate software/plugins (by way of example https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis) of static code analysis aimed at identifying potential security vulnerabilities or risks. In the case of existing security vulnerabilities disclosed by the static code analysis tool, they must be solved or justified by the Supplier.

The Supplier must implement the application communication modes including, even if not initially enabled, all the security functions envisaged by the reference protocol standards for communication with the SCADA infrastructure.

## 5.6 Cyber security - assessments

**(R.5.6.1)** Enel reserves the right, **for the entire service life**, to carry out security assessments on the protections. As example, it may be carried out directly by Enel, or through third-party specialist, Vulnerability Assessment, Penetration Test or Code Inspection activities.

If, **in the product release/approval phase**, and for a subsequent period of 6 months, Enel reveals security differences compared to the requirements stated in this document, the Supplier must release an update to align the firmware configuration with the identified not-compliance prerequisites.

The Supplier, **for the entire service life**, must assist Enel in the security fixing/upgrade activity with the aim of:

a. ensuring the mitigation of security problems encountered during the Security Assessment activities;

b. ensuring the maintenance of the desired security level

The assistance of the supplier must not be limited to the application code developed by himself, it must also include all the firmware components, including the components acquired externally.

# 6 CYBER SECURITY REQUIREMENTS BIDDING FORM

Supplier/Bidder must fill following table, related to cyber security requirements described in Chapter 5.

**Table 2 – IED Cyber Security –** Requirements Level of respect

| N. | Technical Specification | Mandatory | Yes | No | Not Applicable | Remarks for any deviation |
|---|---|---|---|---|---|---|
| **5.1 Physical security requirements of the device** | | | | | | |
| (R.5.1.1) | Anti-tamper solution | X | | | | |
| (R.5.1.2) | Welding memory slots | X | | | | |
| (R.5.1.3) | PIN-board removal | X | | | | |
| (R.5.1.4) | Top side marking limited | X | | | | |
| (R.5.1.5) | Management access only by Ethernet ports | X | | | | |
| (R.5.1.6) | Microcontroller end-of-support/life over 5 years | X | | | | |
| **5.2 Firmware security requirements** | | | | | | |
| (R.5.2.1.1) | Device updating service | X | | | | |
| (R.5.2.1.2) | Supply Firmware update status | X | | | | |
| (R.5.2.1.3) | Update packages distribution method | X | | | | |
| (R.5.2.1.4) | Repository | | | | | |
| (R.5.2.2.1) | Hardening guideline | X | | | | |
| (R.5.2.2.2) | Disablement of management access interfaces | X | | | | |
| (R.5.2.2.3) | Security configuration guidelines | X | | | | |
| (R.5.2.2.4) | Not encrypted traffic allowed and conditions | X | | | | |
| (R.5.2.2.5) | Logging | X | | | | |
| (R.5.2.3.1) | Basic software required | X | | | | |
| **5.3 Code security** | | | | | | |
| (R.5.3.1) | Secure code development framework | X | | | | |
| **5.4 WEB/API interface** | | | | | | |
| | Authentication interface in-depth | X | | | | |
| (R.5.4.2) | OWASP web application compliance | X | | | | |
| **5.5 SCADA/ICS applications** | | | | | | |
| (R.5.5.1) | Static code analysis | | | | | |
| **5.6 Cyber security assessments** | | | | | | |
| (R.5.6.1) | VAPT and code inspection | X | | | | |

# 7 ENEL CYBER SECURITY GUIDELINE NO. 12 – ADDITIONAL REQUIREMENTS

In addition to IED Cyber Security Requirement (Chapter 5), the latest version of the ENEL Operational Technologies (OT) security guideline on Industrial Control Systems (Cyber Security Guideline no. 12) must be consider by the Supplier. The Supplier will receive this document during the procurement phase (par. 9.1), so it is expected from Supplier the compilation of the following form (Table 3) about the requirements level of respect.

The IED Cyber Security requirements (Chapter 5) shall be applied in compliance with this OT security guideline, which in any case prevail over these requirements.

**Table 3 – Guideline no. 12 -** Requirements level of respect

| | | | | Compliance | | | |
|---|---|---|---|---|---|---|---|
| **Family** | **ID** | **Baseline** | **Advanced** | **Yes** | **No** | **Not Applicable** | **Remarks for any deviation** |
| ***Configuration Management*** | | | | | | | |
| | R.1 | *x* | | | | | |
| | R.2 | *x* | | | | | |
| | R.3 | *x* | | | | | |
| | R.4 | *x* | | | | | |
| ***HW Systems and Networking Equipment*** | | | | | | | |
| | R.5 | *x* | | | | | |
| | R.6 | *x* | | | | | |
| | R.7 | *x* | | | | | |
| | R.8 | *x* | | | | | |
| ***Virtualization*** | | | | | | | |
| | R.9 | *x* | | | | | |
| | R.10 | *x* | | | | | |
| | R.11 | *x* | | | | | |
| | R.12 | | *x* | | | | |
| ***Initial System Configuration*** | | | | | | | |
| | *Removal of Unnecessary Services and Programs* | | | | | | |
| | R.13 | *x* | | | | | |
| | R.14 | *x* | | | | | |
| | R.15 | *x* | | | | | |
| | *Default System Permissions and User Accounts* | | | | | | |
| | R.16 | *x* | | | | | |
| | R.17 | *x* | | | | | |
| | R.18 | *x* | | | | | |
| | *Installing Operating Systems, Applications, and Third-Party Software Updates* | | | | | | |
| | R.19 | *x* | | | | | |
| | R.20 | *x* | | | | | |
| | R.21 | *x* | | | | | |
| | R.22 | *x* | | | | | |
| ***Threat and Vulnerability Management*** | | | | | | | |
| *Vulnerability Assessment* | | | | | | | |
| | R.23 | *x* | | | | | |
| | *Antivirus/Antimalware Detection and Protection* | | | | | | |
| | R.24 | *x* | | | | | |
| | R.25 | *x* | | | | | |
| ***Patch Management*** | | | | | | | |
| | R.26 | *x* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | R.27 | x | | | | | |
| | R.28 | x | | | | | |
| | R.29 | x | | | | | |
| ***Network Infrastructure*** | | | | | | | |
| | R.30 | x | | | | | |
| | R.31 | x | | | | | |
| | R.32 | x | | | | | |
| | R.33 | x | | | | | |
| | R.34 | x | | | | | |
| | R.35 | x | | | | | |
| | R.36 | | x | | | | |
| | R.37 | | x | | | | |
| | R.38 | | x | | | | |
| ***Centralized Remote Access*** | | | | | | | |
| | R.39 | x | | | | | |
| | R.40 | x | | | | | |
| | R.41 | x | | | | | |
| ***Access Control*** | | | | | | | |
| | R.42 | x | | | | | |
| | R:43 | x | | | | | |
| | R.44 | x | | | | | |
| | R.45 | x | | | | | |
| | R.46 | x | | | | | |
| | R.47 | x | | | | | |
| | R.48 | | x | | | | |
| | R.49 | | x | | | | |
| | R.50 | | x | | | | |
| | R.51 | | x | | | | |
| | R.52 | | x | | | | |
| ***Authentication and Authorization Management*** | | | | | | | |
| | R.53 | x | | | | | |
| | R.54 | x | | | | | |
| | R.55 | x | | | | | |
| | R.56 | x | | | | | |
| | R.57 | x | | | | | |
| | R.58 | x | | | | | |
| | R.59 | x | | | | | |
| | R.60 | x | | | | | |
| | R.61 | x | | | | | |
| ***Auditing*** | | | | | | | |
| | R.62 | x | | | | | |
| | R.63 | x | | | | | |
| | R.64 | x | | | | | |
| | R.65 | x | | | | | |
| | R.66 | x | | | | | |
| | R.67 | x | | | | | |
| | R.68 | x | | | | | |
| | R.69 | x | | | | | |
| | R.70 | x | | | | | |
| | R.71 | | x | | | | |
| | R.72 | | x | | | | |
| ***Monitoring*** | | | | | | | |
| | R.73 | x | | | | | |
| | R.74 | x | | | | | |
| | R.75 | x | | | | | |
| | R.76 | x | | | | | |
| | R.77 | x | | | | | |
| | R.78 | | x | | | | |
| ***Network Communications Security*** | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | R.79 | *x* | | | | | |
| | R.80 | *x* | | | | | |
| | R.81 | *x* | | | | | |
| | R.82 | *x* | | | | | |
| | R.83 | *x* | | | | | |
| | R.84 | | *x* | | | | |
| | R.85 | | *x* | | | | |
| | R.86 | | *x* | | | | |
| | R.87 | | *x* | | | | |
| | R.88 | | *x* | | | | |
| | R.89 | | *x* | | | | |
| | R.90 | | *x* | | | | |
| | R.91 | | *x* | | | | |
| | R.92 | | *x* | | | | |
| | R.93 | | *x* | | | | |
| | R.94 | | *x* | | | | |
| ***Secure Software Coding*** | | | | | | | |
| | R.95 | *x* | | | | | |
| | R.96 | *x* | | | | | |
| | R.97 | *x* | | | | | |
| ***Backup and Disaster Recovery*** | | | | | | | |
| | R.98 | *x* | | | | | |
| | R.99 | *x* | | | | | |
| | R.100 | *x* | | | | | |
| | R.101 | *x* | | | | | |
| | R.102 | | *x* | | | | |
| | R.103 | | *x* | | | | |
| | R.104 | | *x* | | | | |
| ***Guidance documents*** | | | | | | | |
| | R.105 | *x* | | | | | |
| ***Maintenance and Warranty requirements*** | | | | | | | |
| | R.106 | *x* | | | | | |
| | R.107 | *x* | | | | | |
| | R.108 | *x* | | | | | |
| | R.109 | *x* | | | | | |
| | R.110 | *x* | | | | | |
| | R.111 | | *x* | | | | |
| ***Security Design*** | | | | | | | |
| | R.112 | *x* | | | | | |
| | R.113 | *x* | | | | | |
| | R.114 | *x* | | | | | |
| | R.115 | *x* | | | | | |
| | R.116 | | *x* | | | | |
| | R.117 | | *x* | | | | |
| | R.118 | | *x* | | | | |
| | R.119 | | *x* | | | | |

# 8 SECURITY CODE DEVELOPMENT CATEGORIES

## 8.1 Code injection through direct memory access

All the vulnerabilities that allow modification or reading out of memory through an input validation problem, typical for native code. Memory could include the stack or the heap, arrays or general memory segments like in case of the write-what-where attack. The aim is usually to inject a code into the memory through a buffer overflow or through any other buffer operation, and then execute this code.

## 8.2 Code injection and control flow manipulation

All attacks that aim at injecting some well picked and formed input that will be turned to executable commands (SQL, shell, etc.) at the end in the vulnerable code, or will trigger a change in the desired control flow, making certain parts of the code execute, which would not do so otherwise.

## 8.3 Data injection

The root cause of the Data injection attacks is the possibility for the hackers to inject some data through some of the inputs. In this case however this data is not turned to code, but simply allows access or modification of some other data or resources for the benefit of the hackers, typically causing confidentiality or integrity breach.

## 8.4 Denial of service by input

Hackers may be able to deny service to legitimate users by flooding the application with malicious requests, but flooding attacks can often be defused at the network layer. More problematic are bugs that allow an hacker to overload or crash the application using a small number of requests. Such bugs allow the hackers to specify the quantity of system resources their requests will consume or the duration for which they will use them.

## 8.5 Integer representation problems

Most – if not all – of programming languages are suffering from certain integer representation problems. Most of them will do integer arithmetic overflow on native integer types without any notifications, leaving the code vulnerable by allowing an hacker to circumvent certain validations based on integers. Similarly, casting integers between signed and unsigned representations and between various sized (e.g. short, long) can also cause problems that can be exploited by hackers through circumventing protections.

## 8.6 General code correctness

General code correctness issues that are relevant to any development platform and languages. These include dereferencing NULL pointers/references, which if triggered by the hackers can cause – if nothing else – denial of service by crashing the application. Not taking care appropriately of the portability of the code and the usage of deprecated or obsolete APIs can also open the door for various vulnerabilities.

## 8.7 Dangerous constructs in C/C++

In native code, more specifically in C/C++ we have a number of dangerous constructs that can lead to vulnerabilities. These mainly include memory allocation issues and iman adapt usage of certain functions from some commonly used libraries.

## 8.8 Password and key management

Storing and managing secrets is one of the main challenges in computer secrets. Programmers tend to forget that the code that they write should be considered public (anyone can read and understand their code through reverse engineering), and therefore should not contain any secrets. Security functionality always involve some secrets, but the principle is simple: data that contain the secrets should be protected rather than the code to accomplish any security features. Password and keys should be protected by appropriate cryptography, so that even if an hacker is able to steal the password/key database, it would be hard enough to reveal all secrets in feasible time.

## 8.9 Authentication problems

Some vulnerabilities and associated attacks aim at spoofing the identities in order to gain access to certain system resources.

Before we implement any security feature dependent on the actual entity (person or system) that uses the services of our code, we should unambiguously check the identity of that entity. Actually the definition of both confidentiality and integrity starts with “only the authorized users should…”, and there is authorization without authentication.

## 8.10 Authorization problems

Authorization is the controlled access to the resources, which always assumes that we have an authorized entity, for which a decision can be made to allow or deny the access. In this subcategory we have several vulnerabilities that make possible the circumvention of this control and allow hackers to gain undesired access to certain resources.

## 8.11 Session handling

Sessions are widely used to overcome the stateless of HTTP, making the session (or better to say the session ID) an asset that is to be protected. Preventing hackers from learning the session ID is one of the most important necessity in this domain, and many attack schemes exists. The session ID is usually stored in a cookie on the client side, making this a primary target of an attack.

## 8.12 Weak cryptography

Weak cryptography occurs when we use a cryptographic feature without an adapt care, but also includes the case when we forget to use it. Several popular cryptographic algorithms have become obsolete recently, as their weaknesses and vulnerable nature has been shown; so one should always know which are the “contemporary” and moreover, “future-proof” algorithms that are to be used. Also includes a wide range of problems regarding random number generation.

## 8.13 PKI violation

Without the authenticity of the public key hackers can commit a man-in-the-middle attack by spoofing one’s identity and faking the real owner of a private key. Public Key Infrastructure is designed to overcome this problem, and unambiguously link the public key with the identity information of its owner by using a certificate, which actually is the public key sealed together with the identity and signed by an authority. Handling such certificate needs an adapt care, and each certificate should undergo a complete validation before accepted as an information that establishes trust in its owner – without this validation hackers can still spoof identities despite the usage of PKI.

## 8.14 Privacy violation

Any data can be exposed, especially if not put to public but only for a limited set of people. Privacy violations occur when: private user information enters the program and when the data is written to an external location, such as the console, file system, or network.

## 8.15 Error handling

Security problems related to error handling: error reporting and checking, situations when using error states are better than throwing exceptions, and the issues regarding logging.

## 8.16 Exception handling

In the subcategory dealing with exception handling, the main issue is if and how the valid and consistent state of the code can be restored after an exception occurred. In this sense the most important question is what to do in the finalize block, but it is also about how to throw and to catch exceptions, and let them be propagated towards the callers, with some influence on code maintainability as well.

## 8.17 Race conditions

Race conditions appear because certain processes or threads running in parallel with each other do not execute sequentially. Forgetting about parallel execution, the correct order of execution (relative to each other) and the timing usually means incorrect functionality, which can be triggered and made use of by an hackers; often, these problems however lead to unbound waits.

## 8.18 Synchronization problems

In case of multi-threading, the synchronization of the states of the threads needs special care. This set of vulnerabilities refer to situations when the hackers can interfere to trigger contradictory or non-consistent states during the execution, which is not what the code expects to be at a given time, usually resulting in a behavior of the code outside of what has been specified and designed.

Problems in this domain (functional and from security point of view) are among the most hardly observable and detectable and therefore hardest to fix.

## 8.19 Covert channels

Covert channels are means of extracting some information from a system through a merely unintended way. In case of these vulnerabilities, the hackers can learn some secrets simply by observing the system from an aspect that was out of the intention of the designer or the developers. Typical examples include accessing the information stored in the system outside of the assumptions of the storage subsystem (covert storage attacks) and the timing attacks, when the information is retrieved by observing the execution time of certain algorithms that use secrets (like a private key). Additional emerging examples include observing temperature on chip-cards or their power consumption to learn the private key that they store.

# 9 MISCELLANEOUS

This chapter include further requirements, recommendations and additional information.

## 9.1 Clarification during procurement process

By summarizing, during the procurement process the following clarification will be provided to the supplier:

a. The Enel document, mentioned at § 3.1 and chapter 7, "*Cyber Security Guideline no. 12 – Version no.1 dated 11/09/2017 - ENEL Operational Technologies (OT) security guideline on industrial control systems"*.