# Documentation of Security Requirements

Prepared by: Robin Massink
**DNV GL,**
Utrechtseweg 310 (Business Park Arnhem), Arnhem 6800 ET, Netherlands

DNV GL Headquarters, Veritasveien 1, P.O.Box 300, 1322 Høvik, Norway. Tel: +47 67 57 99 00. www.dnvgl.com

# 1 DOCUMENT HISTORY

| Version | Date | Description |
|---|---|---|
| 0.1 | 2013-09-12 | Initial document |
| 1.0 | 2013-10-14 | GW Changed approach to fill security requirements/functions |

# 2 INTRODUCTION

This document describes the cyber security requirements for Smart grid equipment. Statements in this document are used as foundation for DNV GL security testing service.
In the scenario of "white box testing", a good knowledge of the implementation is needed to build a customized testing session and leads to more accurate test results. The DNV GL Health test service is able to validate each of the requirements in detail, and issue a detailed test report with findings, threats and mitigation recommendations

Please contact Robin.Massink@dnvgl.com for detailed standard references, more information, or read up about the service at; www.dnvkemautilityfuture.com/dnv-gl-explains-the-importance-of-cyber-security-health-testing-of-scada-systems

# 3 SCOPE

The security requirements are based on, and will be limited to the following scope:

*1.3 Standards / regulations*

ISO/IEC 15408:2008 part 2:

- FDP – User data protection (chapter 10)
- FIA – Identification and authentication (chapter 11)
- FPT – Protection of the TSF (chapter 14)
- FTA – TOE access (chapter 16)
- FTP – Trusted path/channels (chapter17)

NIST IR 7628:2010
IEEE 1686:2007
IEC62443 / WIB
NERC-CIP
IEC62351
DNV GL Best practices

# 4 MAPPING OF THE STANDARD SECURITY REQUIREMENTS

## 4.1 Electronic access control

| Security requirement | Short description[1] |
|---|---|
| SR.ACCESS_CONTROL | The DUT shall enforce use of unique ID and password for access to the configuration data. |
| SR.ACCESS_CONTROL_NO_BYPASS | The DUT shall have no means, undisclosed to the implementing entity, whereby the user-created ID/password control can be defeated or circumvented. |
| SR.ACCESS_CONTROL_IDENTIFY | The minimum number of unique user-access ID/password combinations shall be ten (10). |
| SR.UNIQUE_IDENTIFY | identity of accessing party during configuration, view or modification of audit/device/users |
| SR.ACCESS_CONTROL_RULES | The DUT shall have functionality to set rules for complex passwords. This includes:<br>• Minimal length<br>• At least one uppercase and one lower case letter<br>• At least one number<br>• At least one non-alphanumeric character (e.g., @, %, &, *, etc.) |
| SR.ACCESS_CONTROL_ROLES | The DUT shall be able to distinguish between the following user roles: System, Application and User with which shall be able to utilize one or more functions based on the individual account. |
| SR.PASSWORD_DISPLAY | Only user IDs shall be displayed in screens, audit logs, and other records and configuration files. It shall not be possible to cause DUT passwords to be displayed through any means. |
| SR.ACCESS_TIMEOUT | The DUT shall have a time-out feature that automatically logs out a user who has logged in after a period of user inactivity. |
| SR.PROTECTED_PORTS | Only required ports shall be open for access through the management interface. |

[1] The security requirements are tested against one or more specific standard references. The short description shown here is not to be considered exhaustive but aims to give the reader a user-friendly way to fill the table without referring directly to all the standards statements. The reader can request the standard references separately

| | |
|---|---|
| SR.NO_DEFAULT_PASSWORDS | The DUT shall provide functionality to change passwords; default passwords shall always be changed. |
| SR.NO_DEFAULT_PASSWORDS_WIRELESS | The DUT shall provide functionality to change passwords on all wireless interfaces; default passwords shall always be changed. |
| SR.ACCESS_LIST_COMMUNICATION | The DUT shall provide functionality to prevent/allow connections from a defined type of devices/addresses. |
| SR.MAX_NUMBER_UNSUCCESFUL_LOGIN | When the defined number of unsuccessful authentication attempts has been<br>met, the DUT shall be able to take appropriate specific actions. |
| SR.RE_AUTHENTICATE | The DUT shall re-authenticate an external entity under defined conditions |
| SR.SECURE_SENSITIVE_DATA | The DUT shall explicitly deny access of subjects to objects based on the following additional rules:<br>- the Gateway Administrator is not allowed to read consumption data or the Consumer Log,<br>- nobody must be allowed to read the symmetric keys used for encryption. |
| SR.BANNER | Appropriate Use Banner —devices shall display an appropriate use banner on the user screen upon all interactive access attempts. That provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance. |
| SR.LAST_LOGIN | The DUT notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon. |

## 4.2 Security audit

| Security requirement | Short description |
|---|---|
| SR.FIRMWARE_VERSION | The DUT shall provide capability to read the firmware version. |
| SR.AUDIT_STORAGE_CAPACITY | The audit trail facility shall store at least 2048 events before the circular buffer begins to overwrite the oldest event with the newest event. |
| SR.AUDIT_NO_MODIFY | There shall be no capability to erase or modify the audit trail. |
| SR.AUDIT_NO_REMOVE | It shall not be possible to remove the storage media of the audit trail without permanently damaging the DUT beyond the capability of field repair. |
| SR.AUDIT_CONFIGURE | It shall be possible to configure which types of events that shall be included in the audit trail. |
| SR.STORAGE_RECORD | For each audit trail event, the following information shall be recorded:<br>• Event record number<br>• Time and date<br>• The user ID logged in to the DUT at the time of the event<br>• Event type and result |
| SR.EVENT_TYPE | The following events shall  be supported when applicable:<br>Login<br>Manual logout<br>Timed logout<br>Value forcing<br>Configuration access<br>Configuration change<br>Firmware change<br>ID/password creation or modification<br>ID/password deletion<br>Audit-log access<br>Time/date change<br>Alarm incident |
| SR.FULL_LOG_FILE | In case of an almost full log file, an alarm shall be generated |
| SR.REPLAY_NOTIFY | In case a replay attack is issued, the DUT will be able to detect this and notify the appropriate entity |

| | |
|---|---|
| SR.TAMPER_NOTIFY | The DUT shall provide unambiguous detection and notification of physical tampering that might compromise the DUT. |
| SR.LOGICAL_ATTACK_NOTIFY | In case a logical attack is issued, like DOS attack, or a known vulnerability is being exploited, the DUT will be able to detect this and notify the appropriate entity |

## 4.3 Supervisory monitoring of security events

| Security requirement | Short description |
|---|---|
| SR.FW_VERSION_REMOTE | The DUT shall provide capability to read the firmware version remotely. |
| SR.SEC_MONITORING_REALTIME | The DUT shall monitor security-related activity and make the information available through a real-time communication protocol for transmission to a supervisory system. |
| SR.SEC_MONITORING_SYSTEM | The supervisory system shall be either a SCADA system or network management system such as Simple Network Management Protocol (SNMP). |
| SR.SEC_MONITORING_NO_DISTURB | Configuration port activity shall not interfere with nor disable the supervisory monitoring port with the exception of a configuration or firmware change requiring a reboot of the DUT. |
| SR.SEC_MONITORING_ALARMS | The following activities shall cause a unique alarm occurrence:<br>• Unsuccessful login attempts<br>• Reboot<br>• Attempted to use of unauthorized configuration software |
| SR.ALARM_CHANGE | Alarm points shall have momentary change detect capability so that the occurrence of an event will be reported on the next scan of the DUT by the supervisory system. The DUT shall report each occurrence as an individual alarm. |

| | |
|---|---|
| SR.EVENT_AND_ALARM_GROUPING | A means shall be provided to allow the user to group events and alarms. If a point is assigned to a group, only the group alarm shall be sent to the supervisory system upon the occurrence of that point. Individual points shall be assignable to a group in any combination.<br>As a minimum, two groups shall be provided. One group shall be for events, and the other group shall be for alarms. |
| SR.SUPERVISORY_PERMISSIVE_CONTROL | The DUT shall provide a mechanism that, when enabled, requires independent supervisory permission prior to performing actions or requests in the field and/or remotely.<br>All diagnostic ports shall have the ability to be enabled and disabled remotely through a supervisory control command. |

## 4.4 Secure state

| Security requirement | Short description |
|---|---|
| SR.FAIL_SECURE | The DUT shall preserve a secure state if any fatal errors occur. |
| SR.FAIL_KNOWN_STATE | The DUT fails to a known state for defined failures. |
| SR.SECURE_INITIAL | The DUT shall be delivered from the developer to the customer in a secure configuration, e.g. without any temporary accounts used by the developer. |
| SR.SECURE STARTUP | The DUT shall enter its secure state before any operation |
| SR.FLASH_INTEGRITY | Firmware quality assurance shall be in compliance with IEEE Std C37.231.3<br>The DUT monitors and detects unauthorized changes to software and information.<br>BR: During system testing and commissioning the Vendor's system shall verify that access to and use of selected data in control system repositories is adequately protected. |
| SR.SECURE_FIRMWARE_UPDATE | The DUT shall ensure that updated of the firmware can only be done if the source contains a defined level of trust |

| | |
|---|---|
| SR.SECURE_DATA_AT_REST | The DUT shall have stored data integrity monitoring, and will take appropriate action is a violation is detected |
| SR.MALWARE_PROTECTION | The DUT shall have adequate malware protection |
| SR.ERROR_HANDLING | The DUT—<br>1. Identifies error conditions; and<br>2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries. |
| SR.SELF_TEST | The DUT shall run a suite of self-tests during initial start-up, periodically during normal operation, or at the request of the authorized user, at the conditions under which self-test should occur to demonstrate the correct operation of DUT. |

## 4.5 Configuration software

| Security requirement | Short description |
|---|---|
| SR.SOFTWARE_AUTHENTICATION | The DUT shall have a means to authenticate that the configuration software being used to access or change the configuration is a copy that has been authorized by the user. |
| SR.CONFIG_PASSWORD | The configuration software shall be ID/password-controlled so that the software cannot be accessed without the proper ID/password combination.<br>A minimum of ten (10) individual ID/password combinations shall be provided for each copy of the configuration software program. Under no circumstances shall the configuration software cause the passwords of the software itself or the DUT to be displayed in readable text. |
| SR.CONFIG_LEVEL | DUT configuration software shall have the ability to assign features to specific users. At a minimum, the functions and features of SR.CONFIG_VIEW, SR.CONFIG_STORE and SR.FULL_ACCESS will be supported |

| | |
|---|---|
| SR.CONFIG_VIEW | In view configuration data mode, a user can only view configuration data. No changes to the configuration can be made. |
| SR.CONFIG_STORE | In change configuration data mode, the user can change and save configuration data to be uploaded to the DUT at a later point in time |
| SR.FULL_ACCESS | In full-access mode, all functions, including ID/password changes and user assignment levels, can be made |
| SR.RESTORE_CONFIG | It shall be possible to restore configurations that have been lost on the DUT for some reason. |

## 4.6 Time

| Security requirement | Short description |
|---|---|
| SR.TIMESYNC | The DUT uses internal system clocks to generate time stamps for audit records. |
| SR.TIMESYNC_TRUST | The DUT shall be able to use reliable/secure time sources. And within required accuracy |

## 4.7 Traffic control

| Security requirement | Short description |
|---|---|
| SR.CORRECT_PORT_CONTROL | It shall be possible to configure values for the digital input/output/management communication ports, and define criteria for disabling/enabling ports. |
| SR.BOUNDARY_PROTECTION | The DUT monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;<br>The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information |
| SR.TRUSTED_PATH | The DUT establishes a trusted communications path between the user and the DUT. |

| | |
|---|---|
| SR.NO_EAVESDROP | The authentication mechanisms in The DUT obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. |
| SR.SECURITY_PARAMETER_TRANSMIT | The DUT reliably associates security parameters with information exchanged between the enterprise information systems and the DUT. |
| SR.FIREWALL | The DUT shall be able to deny traffic by default, and allow explicitly. This shall apply for all information flow. |

## 4.8 Separation of functions

| Security requirement | Short description |
|---|---|
| SR.SEPARATE_FUNC_SEC | The DUT shall isolate security and non-security functions |
| SR.INFORMATION_REMNANTS | The DUT prevents unauthorized or unintended information transfer via shared DUT resources. |
| SR.SEPARATE_FUNC_MGMT | The DUT shall separate user from management function interfaces |

## 4.9 Hardening

| Security requirement | Short description |
|---|---|
| SR.HARDEN_DOC | The DUT will be provided with correct and executable documents for secure implementation. |
| SR.TAMPER_RESIST | The DUT shall resist conceivable physical tampering scenarios to the DUT by responding automatically such that the security functions are always enforced. |

## 4.10 Robustness

| Security requirement | Short description |
|---|---|
| SR.ROBUSTNESS | The DUT will be able to handle malformed traffic on all protocols and interfaces without getting in a nonresponsive state,<br>observe link state and a monitor like ICMP, processor usage, I/O if available and/or OPC |
| SR.PRIORIZE_RESOURCES | The DUT will prioritize resources for most important functions |

| | |
|---|---|
| SR.DOS | The DUT shall be able to handle DOS attacks, and in case of resulting failure of communication, will be able to recover |
| SR.KNOWN_VULNERABLE | The DUT shall be resilient against know and applicable vulnerabilities |

## 4.11 API

| Security requirement | Short description |
|---|---|
| SR.API_ABUSE | The API of the DUT shall be designed in such a way that the ability to abuse it is minimized |
| SR.INPUT_VALIDATION | The DUT employs mechanisms to check information for accuracy, completeness, validity, and authenticity. |
| SR.NO_DANGEROUS_API | The DUT shall ensure that the API does not contain functions that can be used to compromise the DUT in a physical or functional way |

## 4.12 Documentation

| Security requirement | Short description |
|---|---|
| SR.LIST_SECURITY_FEATURES | The DUT shall have a comprehensive list of audit logs, events and alarms generated by the device that can be utilized for security purposes |

## 4.13 Management

| Security requirement | Short description |
|---|---|
| SR.KEY_MANAGEMENT | The DUT shall demonstrate that encryption keys and pre-shared keys input to devices are managed to ensure they are protected and accessible with the appropriate permissions. |

## 4.14 Encryption

| Security requirement | Short description |
|---|---|
| SR.ENCRYPTION_APPLICATION | Encryption modules in the DUT are implemented and certified according to applicable industry accepted standards |

## 4.15 Conformance

| Security requirement | Short description |
|---|---|
| SR.PROTOCOL_CONFORMANCE | If formal conformance testing is available, the DUT shall be tested accordingly |

# 5 GLOSSARY

| Term | Meaning |
|---|---|
| DUT | Device Under Test |
| ICMP | Internet Control Message Protocol |
| OPC | OLE for Process Control |
| OLE | Object Linking and Embedding |
| API | Application programming interface |
| SNMP | Simple Network Management Protocol |

# 6 REFERENCES

| Document | Version |
|---|---|
| NIST IR 7628: | 2010 |
| IEEE 1686: | 2007 |
| IEC 62443 | draft |
| WIB M2784 PCS VendorSecurity | V2 |
| IEC 62351 | - |
| NERC-CIP | Version 3 |
| ISO/IEC 15408 part 2 | 2008 |