European Network for Cyber Security

Enexis DALI Project
Security Requirements

Final Version

14 July 2016

ENCS

Table of Contents

1 Introduction

In the Distribution Automation Light (DALI) project, Enexis is preparing to set up remote monitoring of all of its 35,000 substations. For this purpose, they will procure DALI boxes that will be placed in each station. In 2016 Enexis will start a large scale pilot. This document contains the security requirements for the DALI boxes that will be procured in this pilot.

The requirements are based on the ENCS distribution automation RTU requirements, which were previously used for the Enexis MS-D tender. Enexis has conducted a market survey and a risk assessment to adjust the requirements to the more restricted uses cases in the DALI project.

1.1 How to Read the Requirements

Each requirement is labelled with an identifier (such as SPR.01, or SFR.02) referring to the section it is in, and consists of the following three items:

- **Minimum Requirement:** A *mandatory requirement* is a compulsory need that a system, device, component, or entity must meet. Statements in the requirements of this document are compulsory for the vendor.
- **Awarding Criteria:** A*warding Criteria* are weighed and scored in the evaluation, but do not lead to direct exclusion of the vendor from the tender process. The weights and scores are not defined in this document but will be set by the utility starting the tender process.
- **Recommended Assurance:** *Recommended assurance* provides guidance for quality control. The vendor can see how the implementation of the requirement will be tested in a standard testing facility. Appendix A provides brief remarks and references concerning the most common testing procedures.

Items may be left out for a particular requirement if they are not used.

After these three items, further clarification on the requirement is given. The clarification can define certain terms, give examples of what is and is not allowed by the requirements, or give a recommendation on implementing the requirement. A requirement does not have to be implemented as in the recommendation, as long as a the Vendor provides a good justification on why their implementation meets the requirement (see requirement SUR.01 in Section 5).

The requirements use standard terminology from security and distribution automation where possible. If there is a possibility for confusion about a term, it will be defined in the clarification of the first requirement where it is used, and printed in bold there.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

1.2 Architecture and Scope

The security requirements see the DALI box as a black box. The requirements only concern securing the interfaces of the DALI box with other systems, in particular the interface with the central systems.

The security requirements can be implemented in different architectures within the DALI box. Three options are shown in the figure below. In this picture the RTU is the component in the DALI box that collects data from the sensors, and controls the public lighting. The modem is the component that provides connectivity to the LTE network.

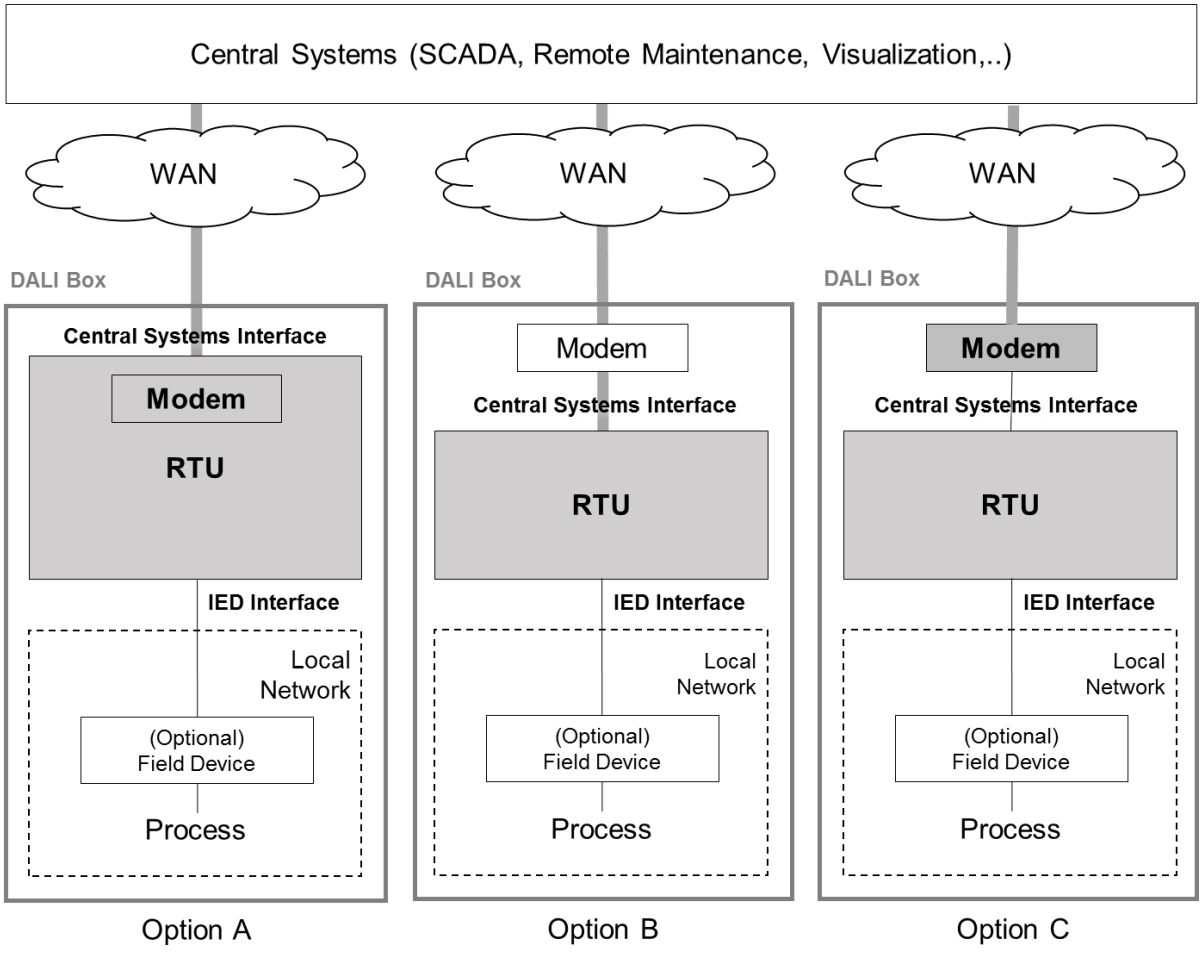

Figure 1: Architectures for the DALI box.

The thick gray line between the central system and the modem presents the part of the connection that is secured by encryption and authentication (see Section 2.3), for instance by a TLS connection or an IPsec tunnel. In Option A, the modem is integrated into the RTU, and the secure connection ends on the integrated device. In Option B the modem is external to the RTU, and the secure channel ends on the RTU. In Option C, the modem is also external, but the secure connection ends on the modem. *All three architectures are allowed in the DALI project.*

The components to which the requirements apply in each architecture are colored grey in the diagram above. In Options A and B the requirements apply to the RTU, as that is where

the secure connection ends. In Option C they also apply to the modem, as the modem is also responsible for the RTU security. To not have to distinguish between both cases in each requirement, the requirements are formulated in terms of the DALI box as a whole.

The security requirements all concern the **central systems interface** that connects the RTU to the Salvador central system, and central maintenance applications. This interface can be implemented either through WAN connection over LTE, or by the RJ45/Ethernet connection to an external router or switch in the substation. (See the communication requirements.) The security requirements do not distinguish between these two options.

The central systems interface is the only interface for which the communication leaves the DALI box. The requirements do not concern internal interface, such as the IED interface that connects the RTU to IEDs and other devices within the DALI box.

The DALI box *should not have a local maintenance interface* that allows service engineers to locally connect to the RTU. Hence, there are no security requirements for such an interface.

Requirements also sometimes reference different functions on the RTU:

- The **firmware update** function refers to changing the firmware or any other software installed on the RTU.
- The **configuration** function refers to changing any setting on the RTU, including network settings, I/O settings, and the security configuration.
- The **sensor reading** function refers to accessing data from sensors connected to the RTU.
- The **control** function refers to sending commands to any actuators, such as switches or breakers, connected to the RTU.

The functions include access to data related to each function.

1.2.1 Stakeholders

The stakeholders concerned with the procurement and product lifecycle of the DALI box are *Purchasers* and *Vendors*. This document uses the term *Purchaser* as replacement for utility, distribution system operator (DSO), grid operator or similar. The term *Vendor* stands for the party that sells the RTU. The document does not distinguish between a vendor and a manufacturer in case these are two separate entities. Ultimately, the Vendor is held responsible for the security features of the product, i.e., the DALI box. In particular, the Vendor has to ensure that all components procured from a supplier satisfy the requirements in this document.

2 DALI Box Security Requirements

This section contains the technical requirements to keep the DALI box itself secure. Care has been taken to align this requirements with common standards and best practices for security for devices used in the industrial control systems domain, such as the BDEW White Paper Requirements for Secure Control and Telecommunication Systems [4], the DHS Cyber Security Procurement Language for Control Systems [5], NERC CIP [6], the IEC 62351 series [7] and IEC 60870-5-7 [8], the IEC 62443 series (former ISA-99) [9], IEEE P1686 [10], and the WIB Process control Domain Security Requirements for Vendors [11].

2.1 Future-Proof Design

The requirements in this section concern future-proof designs for the DALI box.

SFR.01 Future-Proof Design

Minimum Requirements	1. The DALI box SHALL have sufficient reserves in memory and computing power to allow updates to security functions that security experts anticipate are necessary during the DALI box's lifecycle.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Testing the performance of the DALI box for algorithms and protocols anticipated for future use.

In this document a **security function** refers to any function on the DALI box that is needed for it to be operated securely. Security functions include access control, authentication, and encryption. All functions needed to implement the security requirements in this document shall be considered as security functions.

There are several sources of expert forecasts on what security functions are needed in the future. It is recommended that Vendors consult these sources when determining which algorithms and protocols are needed in the future.

The ENISA documents on algorithms, parameters, and key sizes [12] marks some algorithms as suitable for future use, while others are only suitable for legacy use. If legacy algorithms are used by the DALI box, there should be sufficient resources to update it to an algorithm in the same category suitable for future use.

Recommendations on which key sizes provide sufficient security in the future are available from e.g. NIST [18], BIS [38], and ANSSI [38]. One way to show that sufficient computational resources are available, is to show that the DALI box can support the key sizes required by these document at the end of the DALI box's lifecycle.

The German Federal Office for Information Security (BSI) classifies IPsec and IKEv2 options in [15]; for each option BSI states a year until which the option is considered secure. The label "2021+" means that the option is considered secure until the year 2021 and beyond.

This gives a prediction of which IPsec options the DALI box should be able to support during its lifecycle.

If for a protocol used by the DALI box a newer version of the protocol specification is available or is being prepared, this version also gives information on security function the DALI box may need to support in the future.

2.2 Cryptographic Algorithms and Protocols

The requirements in this section concern how to choose cryptographic tools and key lengths.

SPR.01 Cryptographic Algorithms and Key Lengths

Minimum Requirements	1. The DALI box SHALL use for security functions only cryptographic algorithms for which a description is publicly available, and which have been thoroughly reviewed by independent cryptographers. 2. The DALI box SHALL not use for security functions a choice of cryptographic algorithms, protocols, and parameters if there are vulnerabilities known for it. 3. If for a security function algorithms are available in [12], the DALI box SHALL use one of these algorithms. 4. The DALI box SHALL use from [12] only those cryptographic algorithms, and parameters considered suitable for legacy or future use. 5. The DALI box SHALL implement the algorithms in [12] exactly as they are described there without any modifications.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor can be used to establish that only allowed cryptographic algorithms, protocols, and parameters are used. • Functional security tests can be used to verify that the algorithms are implemented as described in [12]. Certifications, such as the NIST Cryptographic Algorithm Validation Program (CAVP) [23], are also available to test that the protocols are implemented according to specification.

A **cryptographic protocol** is a protocol used for security functions, such as authentication, or protecting confidentiality or integrity. Cryptographic protocols are implemented using cryptographic algorithms, such as symmetric and asymmetric ciphers, and hash functions, which again depend on certain cryptographic parameters, such as the key size.

It is allowed to use non-cryptographic algorithms or algorithms for which vulnerabilities are known if they are not used for security functions. For instance, cyclic redundancy check (CRC) codes can be used by the DALI box to detect accidental errors in the transmission

of a message. They should however not be used to check against deliberate modifications by attackers (as required in SIR.02) as there are vulnerabilities known for them.

Vulnerabilities are considered known if they are in a public vulnerability database, or if an advisory on them has been published. The ENISA report [12] provides a good overview of the state-of-the-art for cryptographic algorithms.

To interpret the requirement, it is important to distinguish between cryptographic protocols and communication protocols, such as TLS, IPsec or IEC 104. Communication protocols usually use several cryptographic protocols to implement their security features. Often they offer different options for each feature. For instance, the TLS protocol allows both RSA and (elliptic curve) Diffie-Hellman for key exchange, and allows for different key sizes for each protocol. If vulnerabilities are known for some of the cryptographic options allowed by a communication protocol, it does not mean the communication protocol should not be used. Instead, only secure options should be used, and others disabled. For instance, when TLS is used, care should be taken to only enable cipher suites allowed by [12].

For several communication protocols commonly used in DALI boxes there are vulnerabilities known for all the cryptographic protocols used in older protocol versions. In that case the older protocol version should not be used. Examples are:

- All versions of SSL and TLS versions before 1.2 have known vulnerabilities. If the DALI box uses TLS, it must use version 1.2 or greater.
- SNMP versions before version 3 have known vulnerabilities.

Communication protocols with known vulnerabilities can be used if they are encapsulated in other protocols that provide the security functions, such as IPsec, OpenVPN, or TLS. Many industrial protocols, such as IEC 60870-5-104, do not implement any security. Such protocols should therefore always be encapsulated in secure lower layer protocols.

SPR.02 Cryptographic Random Number Generation

Minimum Requirements	1. The DALI box SHALL use a dedicated cryptographic pseudo-random number generator, as defined in FIPS 186-2 [24], FIPS 140-2 (Annex C) [26], AIS 20 [26], or AIS 31 [27], to generate random numbers used for security functions.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Proof of the implementation could be the reports of a standardized test procedure such as the NIST Cryptographic Algorithm Validation Program (CAVP) [23]. • NIST SP 800-22 [39] provides a standardized test suite to look for biases found in non-cryptographic random number generator during a black-box test.

Random values are used for security function for instance in the generation of digital signatures and cryptographic keys, or in authentication protocols.

The basic random number generators in many programming languages, such as the `rand()` function in the C programming language, do not satisfy the requirements in the mentioned standards. For Linux-based systems one can instead use `/dev/random`. The German BSI recommends in [28] to use kernel versions starting from 2.6.21.5, 3.2, 3.5, 3.6 and 3.7. It is recommended to monitor vulnerabilities in implementations and update kernels accordingly.

2.3 Communication Security

The requirements in this section concern communication security for the DALI box. For SCADA traffic the requirements in this section can be implemented in several ways:

- On the network layer, using for instance IPsec or OpenVPN;
- On the transport layer, using TLS; or
- On the application layer.

For IEC 60870-5-104 the IEC 62351 standard defines encryption and authentication using TLS in IEC 62351-3, and authentication on the application layer in IEC 62351-5. The requirements however also allow DALI boxes to use IPsec tunnels to protect IEC 60870-5-104 traffic.

As explained in Section 1.2, the communication security requirements may be implemented on the RTU (Options A and B), or on an external communications modem (Option C).

SCR.01 Confidentiality

Minimum Requirements	1. The DALI box SHALL protect the confidentiality of communication on the central systems interface by encrypting it using a protocol allowed by SPR.01.
Recommended Assurance	• This requirement is verified in a functional security test. The test should in particular ensure that the allowed cryptographic algorithms are supported and that disallowed algorithms are rejected.

SCR.02 Message Integrity and Authentication

Minimum Requirements	1. The DALI box SHALL verify the integrity of application layer messages received on the central systems interface using a message authentication algorithm allowed by SPR.01. 2. If the DALI box detects that a message has been modified or if it cannot verify the integrity of the message, it SHALL reject or drop the message. 3. The DALI box SHALL allow parties it communicates with on the central systems interface to verify the integrity of application layer

	messages it sends by using a message authentication algorithm allowed by SPR.01. 4. The DALI box SHALL be able to determine that the sender of a message is a specific host in the DA system.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the DALI box supports the required functionality. • Carrying out a penetration test can be used to determine if the DALI box verifies message integrity under all conditions.

This requirement concerns cryptographic message integrity. CRC checksums are not allowed by requirement SPR.01. Instead message integrity should be verified using a message authentication code (MAC) or a block cipher in authenticated encryption mode, such as Galois Counter Mode (GCM). Algorithms for these are available in [12]. The entire application layer message should be given as input to the message authentication algorithm. No fields should be left out.

The integrity of messages without application layer payload, such as acknowledgements, does not have to be protected. Headers from lower layer protocols also do not have to be protected (unless it is needed to meet requirement SCR.03).

If IPsec is used to fulfil this requirement, the Encapsulating Security Payload (ESP) should use one of the authenticated cipher modes (AES-GCM or AES-CCM). Alternatively, the Authentication Header (AH) should be configured using one of the allowed cryptographic algorithms (see SPR.01).

A message is dropped if the DALI box does not send a reply. A message is rejected if the DALI box replies with an error message or NACK.

Authentication concerns being able to determine the source of a message. By using a MAC or a block cipher in authenticated encryption mode, the DALI box checks that a message is sent by a host that has access to the key used for them.

SCR.03 Message Freshness

Minimum Requirements	1. The DALI box or modem SHALL be able to detect replay attacks on the central systems interface. 2. If the DALI box detects that a message is replayed, it MUST reject or drop the message.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor on the mechanisms used to protect against replay attacks. • Functional testing can be used to verify if the mechanisms are indeed implemented.

To prevent replay attacks all messages should be secured by one of the following means:

- By adding a counter.
- By adding an authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm.

VPN technologies such as IPsec need to explicitly enable replay protection in combination with message authentication (SCR.02).

SCR.04 IPsec Interoperability

Minimum Requirements	***If the DALI box uses IPsec for encryption and authentication on the central systems interface*:** 1. The DALI box SHALL support the following IPsec settings: a. For encryption 256 bit ENCR_AES_CBC b. For authentication: SHA_256_128 HMAC c. For key establishment: Diffie-Helman with a 2048-bit MODP Group d. Support for both pre-shared keys (PSK), and certificates 2. The DALI box SHALL apply filtering on the IP-traffic on the WAN interface. 3. The DALI box SHALL be fully compliant with IKEv2 (RFC7296). 4. The DALI box SHALL act as an IPsec initiator: it SHALL establish tunnel connections to the VPN servers automatically. 5. The DALI box SHALL automatically re-establish closed or disconnected IPsec tunnels. 6. The DALI box SHALL support assignment of virtual IP addresses through the IKEv2 configuration payload.
Awarding Criteria	7. The DALI box SHOULD support two parallel IPsec tunnels to allow it to connect to the two different control centers of Enexis.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor on the mechanisms used to protect against replay attacks. • Functional testing can be used to verify if the mechanisms are indeed implemented.

Note that the requirement *does not require that the DALI box supports IPsec*. Other solutions, such as TLS, are also allowed for encryption and authentication. The requirement only applies to the RTU if it supports IPsec.

The requirement is included to allow for easy integration of the DALI box into the existing Enexis IPsec infrastructure. The two IPsec tunnels are required for the RTU to connect to the two different control centers that Enexis has.

2.4 Software Security

The requirements in this section concern the security of software updates. **Software** in this section refers to any executable files installed on the DALI box, including firmware, applications, operating systems, libraries, web application code, scripts, patches and updates.

SSR.01 Remote Software Updates

Minimum Requirements	1. The DALI box SHALL support remote software updates. 2. The DALI box SHALL support remotely updating all security functions. 3. The DALI box SHALL support remotely updating the drivers of the RJ45 interface.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor.

SSR.02 Software Integrity

Awarding Criteria	1. The DALI box SHOULD verify the integrity of software before it is installed. 2. The DALI box SHOULD reject software if it detects it has been modified, or it cannot verify the software's integrity.
Recommended Assurance	• The functional requirement can be verified by testing the implemented firmware-update functions.

Integrity is usually verified by calculating a hash value of the software. Hash functions are described in the ENISA document [12] (see SPR.01).

SSR.03 Software Non-Repudiation

Awarding Criteria	1. The DALI box SHOULD support non-repudiation for software: it SHOULD be able to prove that the software came from the Vendor.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor on the mechanisms used for non-repudiation. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the non-repudiation mechanisms.

Non-repudiation means that a sender of the software should not be able to deny that he sent it. It is normally implemented using digital signatures. A hash value of the software

is calculated, and signed using public-key cryptography. The private key is kept by the Vendor (see SDR.03). The public key for the validation of the signature can be installed on the DALI box during the manufacturing process. SDR.08 defines Production Security & Credential Provisioning. It is not needed to keep the public key secret. Measures should be taken to make sure the correct key is installed however.

It is not necessary that the Purchaser establishes a Public Key Infrastructure (PKI) at the Central System for this purpose. The Vendor has to store the private software signing key.

2.5 System Hardening

The requirements in this section concern hardening of the DALI box.

SHR.01 Software Service Hardening

Minimum Requirements	1. The DALI box SHALL have all unneeded services and applications removed, or disabled if removal is not possible. 2. The DALI box SHALL not use services or applications for security functions if there are vulnerabilities known for them. 3. The DALI box SHALL use only communication protocols that are needed to meet the functional requirements. 4. The DALI box SHALL not have an interface for local maintenance.
Recommended Assurance	• Vulnerability scanners can automatically check devices for known vulnerabilities. • Carrying out a penetration test can provide further assurance that this requirement is adequately implemented. • If high-impact functions are disabled in the DALI boxes code, the Purchaser can request a code review from the Vendor.

Examples of unused services and application that should be removed or disabled are:

- Testing and debugging applications used for initialization or testing during the production process.
- Webservers used as graphical user interfaces (GUIs) or for maintenance purposes if maintenance is normally done through a specialized application.
- FTP servers used during installation.
- Drivers for hardware that is not in the DALI box.
- A telnet service when SSH is also available.
- NTP or DNS servers if these are not used by other devices in the substation.

Vulnerabilities are considered known if they are in a public vulnerability database, or if an advisory on them has been published.

Webservers/GUIs are often prone to code injection, buffer overflows and other vulnerabilities, they pose a high risk when directly accessible from a remote connection. The OWASP list [30] provides a good overview of known web vulnerabilities.

SHR.02 Account Hardening

Minimum Requirements	1. The DALI box MUST NOT contain active default, guest and anonymous accounts. 2. The DALI box MUST NOT allow remote access to root accounts on the DALI box. 3. The DALI box SHALL have Vendor-owned accounts removed where feasible.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented.

2.6 Resilience

The requirements in this section concern resilience of the DALI box and the communication sent and received by the DALI box.

SRR.01 Input Validation

Minimum Requirements	1. The DALI box SHALL verify that all input it receives is valid. 2. The DALI box SHALL reject or drop input that is invalid or for which the validity cannot be verified.
Recommended Assurance	• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.

Input can be for instance entries into fields of a web interface, commands typed on a terminal interface, or messages the DALI box receives on one of its interfaces.

A message is considered **valid** if it meets all protocol specifications, it makes sense for the DALI box's configuration, and it meets all requirements the DALI box has on data sizes. Examples of validity checks include checks of syntax, data format, and value ranges. The DALI box should also check if registers or data objects reference by a message exists, and if the data fits into internal buffers allocated for it. The requirement applies to all network protocol layers, including the wireless protocols, TCP/IP stack, and application layer protocols.

SRR.02 Fail-Secure Operation

Minimum Requirements	1. The DALI box SHALL be fail-secure, i.e., it SHALL be designed to fail in a manner that limits any security compromise of its own operation and security compromise of other devices.

	2. The DALI box SHALL not leak confidential information, such as keys or credentials, during a failure. 3. The DALI box SHALL protect the integrity of security critical data during failures. 4. The DALI box SHALL not allow access controls to be bypassed remotely during failures. 5. The DALI box SHALL restore availability after software failures as soon as possible.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance of the design robustness.

Point 5 can be addressed by implementing a watchdog functionality that allows the device to maintain a secured operational state in case of a failure.

Examples for relevant failures are:

- Integrity errors, e.g. of configurations or log files;
- Failures during execution of cryptographic functions;
- Failures during validation of login credentials;
- Failures when entering data (wrong data format, wrong data length, invalid commands etc.).

3 Support for Secure Operation

The requirements in this section concern access control and logging of security events, two services needed to securely operate the DALI box.

3.1 Access Control and User Authentication

The requirements in this section concern access control for the DALI box.

SAR.01 Basic Access Control

Minimum Requirements	1. The DALI box SHALL restrict access to the configuration and firmware update functionality by using passwords or cryptographic keys.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the DALI box.

A user name and password login mechanism is sufficient to meet the requirement. More advanced mechanisms, such as public key authentication and challenge-response protocols, are also allowed.

3.2 Key and Credential Management

The requirements in this section concern the management of keys and credentials stored on the DALI box.

SKR.01 Key and Credential Updates

Minimum Requirements	1. The DALI box MUST support remote updates of all credentials and cryptographic keys.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the DALI box.

Because the DALI box supports key updates, it is possible to give each DALI box individual keys. It is strongly recommended that this is done by Purchasers operating the DALI box.

Using different keys for different services can for instance be achieved by using TLS with a different key for each service.

SKR.02 Password Storage

Minimum Requirements	1. The DALI box SHALL store passwords salted and hashed using a cryptographic hash function allowed by SPR.01.
Recommended Assurance	• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the DALI box.

Special protection is required for passwords. They should be the only truly confidential information stored on the DALI box. The requirements in this document are set up to allow for different keys for each DALI box. If the Purchaser indeed uses different keys in operations, attackers will benefit little from getting the keys out of the DALI box. They must already compromise the DALI box to get the key, and they cannot use the keys on other DALI boxes.

It is still preferred to use different passwords for each DALI box. Attackers that compromise the DALI box may still acquire passwords by capturing them when they are sent to the DALI box. Using different passwords does require support from the tools used for maintenance, and the central servers to remember the passwords. Engineers and operators cannot be expected to remember passwords for hundreds of DALI boxes.

3.3 Logging

The requirements in this section concern logging of events.

SLR.01 Logging Security Events

Minimum Requirements	1. The DALI box SHALL log security events in a locally stored log. 2. The DALI box SHALL take measures to prevent that attackers can modify, delete or overwrite the security log to hide their traces.
Recommended Assurance	• The implementation of logging mechanisms can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that attackers cannot bypass detection mechanisms or modify the security log.

In the requirements below **security events** are any events relevant to the secure operation of the DALI box. Security events include at least the following:

- User Activities:
  - Successful logins
  - Failed login attempts
  - Changes of security credentials
  - Unauthorized file access
- Possible signs of attacks:

- Resource exhaustion (DoS)
- Messages whose integrity could not be verified
- Invalid messages
- Attempted replay attacks
- Alarms on physical manipulations

- Updates or changes:
  - Firmware Updates or patches
  - Configuration Changes

3.4 Automated Configuration and Firmware Management

The requirements in this section concern the automatic updates of software and configuration on the RTU. As in section 2.4, **software** refers to any executable files installed on the DALI box, including firmware, applications, operating systems, libraries, web application code, scripts, patches and updates.

SMR.01 Batch Software Updates

Minimum Requirements	1. The DALI box SHALL allow batch software updates. 2. The Vendor SHALL supply the tools needed to perform batch software updates. The tools SHALL support upgrading groups of DALI boxes without further interaction.

SMR.02 Batch Configuration Changes

Minimum Requirements	1. The DALI box SHALL allow batch configuration changes after the initial installation. 2. The Vendor SHALL supply tools for batch configuration changes. 3. The batch configuration tools SHALL allow at least the following parameters to be changed based on data from a simple text file (csv or xml): a. The station name b. The transfer ratio of the transformers c. The placement of the short-circuit indicators d. The IPsec address e. The IPsec keys

4 Product Lifecycle and Governance

The requirements in this section concern the processes used for developing, manufacturing, and provisioning of the DALI box in a secure way.

There will be no recommendation regarding quality assurance for the requirements in this section. It is recommended that the Purchaser asks for documentation to verify the implementation of the requirements.

All requirements hold for the complete contractually agreed lifecycle of the DALI box. All requirements apply to the Vendor and suppliers. This includes in particular Third-Party Suppliers.

SDR.01 Information Security Management System

Minimum Requirements	1. The Vendor SHALL implement an information security management system (ISMS) the scope of which includes at least all systems used to develop, test, manufacture and provision the DALI boxes and any software and hardware tools needed for the maintenance of the DALI box.
Awarding Criteria	2. The Vendor SHOULD have regular audits of the ISMS performed by an accredited external auditor. 3. The Vendors SHOULD provide a proof of the audit to the Purchaser on request. 4. The Vendor SHOULD obtain an ISO 27001 certification for the ISMS. 5. The Vendor SHOULD make a proof of the certificate available on request. 6. The Vendors SHOULD share their security policies with the Purchaser.

Quality assurance certification schemes such as the ISO 9001 are not sufficient to meet this requirement.

SDR.02 Configuration Management System

Minimum Requirements	1. The Vendor SHALL employ a configuration management system for the administration of (changes of) hardware configurations and source code of devices. 2. The Vendor SHALL ensure that the configuration management system stores for each change an explanation, the author, the parts changed, and the time at which it was made.
Awarding Criteria	3. The Vendor SHOULD allow the purchaser to audit the configuration management system.

SDR.03 Secured Versioning

Minimum Requirements	1. The Vendor SHALL ensure that all released versions of hardware and firmware of the DALI box are uniquely identifiable. 2. The Vendor SHALL provide to the Purchaser a cryptographic hash value for each firmware version. 3. The Vendor SHALL be able to reproduce released versions within the contractually agreed product lifecycle, with traceability provided by the hash value(s) as identifier(s).
Awarding Criteria	4. The Vendor SHOULD digitally sign each firmware update supplied to the Purchaser. 5. The Vendor SHOULD protect the firmware signing keys as highly confidential data. 6. The Vendor SHOULD report it to the Purchaser if a firmware signing key is compromised.

SPR.01 gives references for allowed cryptographic hash functions, and digital signing algorithms.

The ISMS required by SDR.01 is normally used to determine the measures needed to protect the firmware signing key. Point 6 of this requirement means that a compromise of the confidentiality of the key should be treated as a high impact event in the ISMS.

SDR.04 Vulnerability Handling Process

Minimum Requirements	1. The Vendor SHALL have an established and documented process to handle vulnerabilities. 2. The Vendor SHALL monitor information sources on vulnerabilities to determine if it has been affected. 3. The Vendor SHALL address vulnerabilities found by the Vendor itself, the Purchaser or system integrator, or external security researchers. 4. The Vendor SHALL disclose to the Purchaser all known vulnerabilities on the DALI box as soon as possible. 5. The Vendor SHALL communicate vulnerabilities to the Purchaser in a secure manner. 6. The Vendor SHALL issue a recommendation on how to mitigate a vulnerability as soon as possible. 7. The Vendor SHALL prioritize fixing vulnerabilities based on the potential impact to the Purchaser.

Standards are available to objectively assess the impact of vulnerabilities, such as CVSS [36]. These can be used as an aid to prioritize fixing vulnerabilities. It is however

recommended that the Vendor also takes into account the specific design of the DALI box, and how it is used by the Purchaser, when assessing the potential impact.

SDR.05 Security Updates and Patching

Minimum Requirements	1. The Vendor SHALL provide security updates or patches for the DALI box to fix high impact vulnerabilities found during the DALI box's lifecycle. 2. The Vendor SHALL test all security updates and patches prior to deployment.
Awarding Criteria	3. The Vendor SHOULD provide documentation that all security patches were tested and validated prior to deployment. 4. The Vendor SHOULD release a patch or firmware update for a vulnerability no more than three months after it was reported to the Vendor.

The Vendor is allowed to leave vulnerabilities with a low impact unpatched. Of course it is not recommended to do so. Low impact vulnerabilities should always be disclosed to the Purchaser by requirement SDR.04.

SDR.06 Security Training and Awareness

Minimum Requirements	1. The Vendor SHALL provide security training for the personnel. 2. The Vendor SHALL be able to document that the necessary knowledge to securely develop and securely produce products is in place. 3. The Vendor SHALL name a technical expert responsible for security-related matters who acts as contact person for the Purchaser. 4. The Vendor SHALL conduct a risk analysis of the firmware design and the corresponding system architecture.
Awarding Criteria	5. The Vendor SHOULD provide documented professional experience in the area of IT security or a security certification, e.g., CISSP or CISM.

5 Assurance

The requirements in this section concerns measures the Vendor should take to make sure the DALI box will work securely.

SUR.01 Security Documentation

Minimum Requirements	1. The Vendor SHALL provide documentation that describes in a traceable manner how each security requirements in this document has been implemented. 2. The Vendor SHALL document which cryptographic algorithms, protocols, and parameters are used for which security functions. 3. The Vendor SHALL document which cryptographic random number generator is used. 4. The Vendor SHALL provide a step-by-step description of the firmware update process. 5. The Vendor SHALL document all interfaces of the DALI box, including the protocols and services used on each interface. 6. If interfaces or services are disabled and not removed, the Vendor SHALL provide information on how they have been disabled. 7. The Vendor SHALL provide a list of all accounts enabled on the DALI box on delivery. 8. The Vendor SHALL provide a list of all security events logged by the DALI box. 9. The Vendor SHALL provide the above documentation together with its proposal. 10. The Vendor SHALL allow verification of the design evidence by an independent third party selected by the Purchaser.

The requirements in this document are formulated in a technology independent manner. The Vendor has different options to implement them. To allow the Purchaser to verify that the requirements are implemented correctly, it is important that they understand which option was chosen. For this purpose, the requirement above asks that the Vendor documents how the requirements have been implemented.

It is important that the documentation makes it easy to trace which part of the documentation describes the implementation of which requirement. This can be done for instance by providing a matrix that links each requirement to a description of its implementation.

If design evidence is sensitive from a security or competitive viewpoint, the Vendor can supply it under an NDA, as long as the NDA allows for verification of the design evidence by the Purchaser or an independent third party.

SUR.02 Security Testing

Minimum Requirements	1. The Vendor SHALL perform tests to verify that all the security requirements in this document have been implemented correctly. 2. The Vendor SHALL test the complete functional scope of the DALI box, including the communication chain between the DALI box and all connected field devices and the central systems. 3. The Vendor SHALL clearly document the security tests. 4. The Vendor SHALL test each firmware release to ensure that it does not contain known vulnerabilities. 5. The Vendor SHALL allow the Purchaser to contract an independent test lab to perform a penetration test on the DALI box.
Awarding Criteria	6. The Vendor SHOULD conduct robustness tests, such as fuzzing or flooding, on all protocols used by the device both on the application layer and on lower protocol layers. 7. The Vendor SHOULD conduct design and code reviews and provide the results to the Purchaser.

Examples of security tests to verify the requirements are given for each requirement under quality assurance.

Automated vulnerability scanners can be used to check the firmware for known vulnerabilities. If a web interface is used, it is also recommended to pay special attention to the vulnerabilities on the OWASP list of web vulnerabilities [30].

If testing information evidence is sensitive from a security or competitive viewpoint, the Vendor can supply it under an NDA, as long as the NDA allows for verification by the Purchaser or an independent third party.

SUR.03 Secure Coding Practices

Awarding Criteria	1. The Vendor SHOULD establish and enforce secure coding practices for the development of the DALI box following best practices. 2. The Vendor SHOULD establish an internal code review process that takes security into account. 3. The Vendor SHOULD use automated code analysis tools to find security vulnerabilities.

Examples of secure coding practices are the SEI CERT coding standards [40], available for different languages, and the MISRA C software development guidelines for embedded systems. [41]

6 References

[1] European Network for Cyber Security. Reference Architecture for Secure Distribution Automation. Deliverable D1.1 in the DA Member Project. Version 1.2, 2015.

[2] European Network for Cyber Security. Mapping of RTU Security Requirements. Deliverable D4.1 in the DA Member Project. Version 1.3, 2015.

[3] Internet Engineering Task Force. RFC 2119: Key words for use in RFCs to Indicate Requirement Levels, 1997. http://www.ietf.org/rfc/rfc2119.txt

[4] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Anforderungen an Sichere Steuerungs und Telekommunikationssysteme (Requirements for Secure Control and Telecommunication Systems), v.01, 2008 (English and German).

[5] Department of Homeland Security (DHS). Cyber Security Procurement Language for Control Systems. September 2009.

[6] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (last accessed on 17 January 2016)

[7] IEC 62351. Power systems management and associated information exchange – Data and communications security. Parts 1-8.

[8] IEC Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351).

[9] IEC 62443 and ISA99, Industrial Automation and Control Systems Security Standards.

[10] IEEE 1686 - Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.

[11] Wurldtech Achilles Practices Certification. Based on International Instrument Users Association (WIB) "Process control Domain: security requirements for vendors." Version 2.0, October-2010.

[12] ENISA European Network and Information Security Agency, Algorithms, key size and parameters report 2014, 2014. (last accessed on 17 January 2016)

[13] Internet Engineering Task Force. RFC 4301: Security Architecture for the Internet Protocol. https://tools.ietf.org/rfc/rfc4301.txt (last accessed on 17 January 2016)

[14] Internet Engineering Task Force. RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2), 2014. https://tools.ietf.org/rfc/rfc7296.txt (last accessed on 17 January 2016)

[15] Internet Engineering Task Force. RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2, 2008. http://www.ietf.org/rfc/rfc5246.txt (last accessed on 17 January 2016)

[16] Bundesamt für Sicherheit in der Informationstechnik. TR-02102-3: Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2). Bonn, Germany. Version 2015-01.

[17] Internet Engineering Task Force. RFC 5289: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), 2008. http://www.ietf.org/rfc/rfc5289.txt (last accessed on 17 January 2016)

[18] National Institute of Standards and Technology. Special Publication 800-57 Part 1 Rev. 3, Recommendation for Key Management, July 2012.

[19] IEC 60870-5-101. Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks. Second edition. 2003-02.

[20] IEC 60870-5-104. Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles. Second edition. 2006-06.

[21] National Institute of Standards and Technology. Special Publication 800-38C: Recommendation for block cipher modes of operation. The CCM mode for authentication and confidentiality (including updates as of 07-20-2007). 2007.

[22] National Institute of Standards and Technology. Special Publication 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. November 2007.

[23] National Institute of Standards and Technology. Cryptographic Algorithm Validation Program. http://csrc.nist.gov/groups/STM/cavp/ (last accessed on 17 January 2016)

[24] National Institute of Standards and Technology. Annex C: Approved Random Number Generators for FIPS PUB 140-2 [25], February 2012.

[25] National Institute of Standards and Technology. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001.

[26] Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German)

[27] Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013. (in German)

[28] Bundesamt für Sicherheit in der Informationstechnik. TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Bonn, Germany. Version 2015-01. (in German)

[29] Internet Engineering Task Force. PKCS #5: Password-Based Cryptography Specification Version 2.0, 2000. http://tools.ietf.org/rfc/rfc2898.txt (last accessed on 17 January 2016)

[30] Open Web Application Security Project. https://www.owasp.org/index.php/Data_Validation (last accessed on 17 January 2016)

[31] Bundesamt für Sicherheit in der Informationstechnik. TR-03116, Part 3, Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme. In German. Annually adapted. Bonn, Deutschland, Date: 2014.

[32] Ari Takanen, Jared DeMott, and Charlie Miller. Fuzzing for Software Security Testing and Quality Assurance (1 ed.). Artech House, Inc., Norwood, MA, USA, 2008.

[33] Electric Power Research Institute. National Electric Sector Cybersecurity Organization Resource. http://www.smartgrid.epri.com/nescor.aspx (last accessed on 17 January 2016)

[34] bcrypt. http://bcrypt.sourceforge.net/ (last accessed on 17 January 2016)

[35] scrypt. http://www.tarsnap.com/scrypt.html (last accessed on 17 January 2016)

[36] National Institute of Standards and Technology. NISTIR 7946. CVSS Implementation Guidance. April 2014.

[37] BSI, „TR-02102-1 v2015-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen," 2015

[38] ANSSI, „Mécanismes cryptographiques - Règles et recommandations, Rev 2.03," 2014.

[39] National Institute of Standards and Technology. Special Publication 800-22 Rev. 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010.

[40] SEI CERT Coding Standards, https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

[41] MISRA C software development guidelines for embedded systems, http://www.misra.org.uk/