Security Target for

W77Q16/32 Secure Flash Memory

Version 1.5,

dated 2022-03-02

Winbond Electronics Corporation

Version Control

Version	Date	Description
1.0	*2021-07-15*	*First release*
1.1	*2021-08-*	*Added IEC62443 mapping and rationale*
1.2	-2021*10-03*	*Adding NIST-8259A mapping and rationale*
1.3	*2021-11-23*	*Fixing* Action item list version
1.4	*2022-01-06*	*Fixing* Action item list version 2.0
1.5	*2022-03-02*	*Fixing A.I. 2022-02-14, 2020-02-21 CB comment*

Table of Contents

1 Introduction 4
1.1 ST Reference....4
1.2 Platform Reference 4
1.3 Included Guidance Documents 4
1.4 Platform Functional Overview and Description 4
2 Security Objectives for the Operational Environment 9
2.1 Compliance to the Protection Profile....9
2.2 Generation of device's Individual Identifier....9
2.3 Protection of the Platform Keys....9
2.4 Secure Communication with the Platform....10
2.5 Boot protected by Platform 10
2.6 Genuine Software Update....10
3 Security Requirements and Implementation....11
3.1 Security Assurance Requirements 11
3.1.1 Complete functional specification (ADV_FSP.4)....11
3.1.2 Operational user guidance (AGD_OPE.1) 11
3.1.3 Preparative procedures (AGD_PRE.1)....11
3.1.4 Flaw Reporting Procedure (ALC_FLR.2) 12
3.1.5 Independent testing: conformance (ATE_IND.1) 12
3.1.6 Vulnerability Analysis (AVA_VAN.2) 12
3.2 Security Functional Requirements 13
3.2.1 Verification of Platform Identity....13
3.2.2 Verification of Platform Instance Identity 13
3.2.3 Attestation of Platform Genuineness 13
~~3.2.4 Secure Update of Platform~~ 14
3.2.5 Secure Update of Application 14
3.2.6 Secure Communication Enforcement....14
3.2.7 Secure Communication Support....14
3.2.8 Physical Attacker Resistance....15
3.2.9 Cryptographic Keystore 16
3.2.10 Secure Storage 17
3.2.11 Secure Encrypted Storage....17
3.2.12 Residual Information Purging 17
3.2.13 Reliable Index....18
3.2.14 Secure Initialization of Platform 18
4 Mapping and sufficiency rationales....19
4.1 SESIP2 sufficiency....19
4.2 IEC62443-4-2 Mapping....20
4.2.1 Sufficiency of Subset of IEC62443-4-2 Requirements 20
4.2.2 Features for Final Product towards IEC62443-4-2 Compliance....26
4.3 NIST-8259A Mapping 27
5 References 39

1 Introduction

The Security Target describes:

- The Platform (in this Section),
- The objectives for the operational environment (in Section 2), that are required for Platform to fulfill its security requirements.
- The exact security properties of the Platform (in Section 3), as evaluated against [GP-SESIP].
- The Security Target claims conformance to "SESIP profile for Secure External Memories" as defined in [GP-SPE].
- Claimed assurance level is SESIP2.

1.1 ST Reference

See the Title page

1.2 Platform Reference

Commercial Name	*SpiFlash® TrustME™ Secure Flash Memory*
Product Name	W77Q16/32
Version	C

1.3 Included Guidance Documents

Reference	Name	Version
[Datasheet]	*W77Q Data Sheet, Winbond Technology Ltd*	*Version A6*
[OPE]	*W77Q16JW/W77Q32JW Secure Flash Operational User Guidance, Winbond Technology Ltd*	*Version C*
[PRE]	*W77Q16JW/W77Q32JW Secure Flash Preparative User Guide, Winbond Technology Ltd*	*Version C*
[SM]	*W77Q Security Manual, Winbond Technology Ltd*	*Version A7*

1.4 Platform Functional Overview and Description

The Platform consists of:

- HW IC Part number (see Section 1.2) delivered in known good die and assembled forms, via Courier.
- The associated IC documentation (see section 1.3) delivered in PDF, via e-mail.

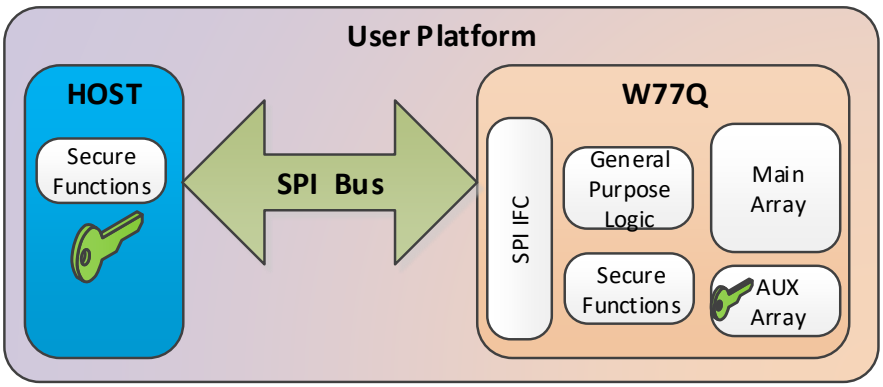
Platform Description

The Platform is an external memory Flash IC dedicated to be embedded into systems that need protection of their memory contents. In particular, the Platform is dedicated to the secure storage of the code and data for IoT applications.

Platform Security Features

- ***Secure separation*** between *Test mode* and *User mode*. More precisely, Test mode entry is cryptographically protected – an unauthorized switch from User mode to Test mode erases all protected user data and all TSF data;
- Protection against **leakage and physical** attacks;
- ***Confidentiality, Authenticity*** and ***integrity*** of Secret User Data;
- ***Authenticity*** and ***integrity*** of Authenticated User Data;
- ***Integrity protection*** of the flash content by error detection codes (CRC-32);
- Memory **Rollback** protection, **Reliable Index** and **Clone Replace Protection;**
- ***Secure Communication Channel*** with the host device and a remote operator;
- ***Memory Access Control*** of the flash content by implementing an access control policy with different levels of authorization, typically:
    - Integrity Protection
    - Write Protection
    - Rollback Protection
    - Plain Access Read
    - Plain Access Write
    - Plain Access Authenticated
- Protection of the **secure boot of the Host Device and secure update** process;
- Secure Key-Provisioning Mechanism.

The platform scope is depicted in the following diagram.



The Platform includes only the W77Q16/32 device. In particular, the Platform does not comprise the following:

- The Host device that will embed the Platform and will be needed to run the Platform in order to stimulate the TSF
- SPI Bus for the communication between the Host device and the Platform

Platform Physical Characteristics

- Performance:
  - Up to 133 MHz Standard/Quad SPI clocks (STR mode)
  - Up to 66 MHz Standard/Quad SPI clocks (DTR mode)
  - Up to 66 MB/s continuous data transfer rate (plain text)
  - Up to 6 MB/s encrypted and authenticated data transfer rate
- Endurance:
  - More than 100,000 erase/program cycles
  - More than 20-year data retention
- Operating conditions:
  - Single 1.65 to 1.95V supply
  - 2mA active current, <1µA Power-down (typ.)
  - -40°C to +85°C or 105°C operating range

Platform Forms of Delivery

The table below lists possible forms of the delivery. The difference between these forms is only packaging. The silicon is the same in all cases.

NO	TYPE	IDENTIFIER	PART NUMBER	DELIVERY METHOD
FORM OF DELIVERY : KNOWN GOOD DIE FORM				
1	HW	IC Part number	W77Q16JWW	Via Courier
2	HW	IC Part number	W77Q32JWW	Via Courier
FORM OF DELIVERY : KNOWN GOOD DIE REDISTRIBUTION LAYER (RDL) FORM				
1	HW	IC Part number	W77Q16JWR	Via Courier
2	HW	IC Part number	W77Q32JWR	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN SOP16 300MIL (THICKNESS 2.64 MM)				
1	HW	IC Part number	W77Q16JWSF	Via Courier
2	HW	IC Part number	W77Q32JWSF	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN SOP8 208 MIL (THICKNESS 2.16MM)				
1	HW	IC Part number	W77Q16JWSS	Via Courier
2	HW	IC Part number	W77Q32JWSS	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN VSOP8 208 MIL (THICKNESS 1.0MM)				
1	HW	IC Part number	W77Q16JWST	Via Courier
2	HW	IC Part number	W77Q32JWST	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN SOP8 150 MIL (THICKNESS 1.75 MM)				

NO	TYPE	IDENTIFIER	PART NUMBER	DELIVERY METHOD
1	HW	IC Part number	W77Q16JWSN	Via Courier
2	HW	IC Part number	W77Q32JWSN	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN VSOP8 150 MIL (THICKNESS 0.9 MM)				
1	HW	IC Part number	W77Q16JWSV	Via Courier
2	HW	IC Part number	W77Q32JWSV	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN WSON8 6X5 (THICKNESS 0.8 MM)				
1	HW	IC Part number	W77Q16JWZP	Via Courier
2	HW	IC Part number	W77Q32JWZP	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN TFBGA24 8X6 (5X5-1 BALL ARRAY)				
1	HW	IC Part number	W77Q16JWTB	Via Courier
2	HW	IC Part number	W77Q32JWTB	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN TFBGA24 8X6 (6X4 BALL ARRAY)				
1	HW	IC Part number	W77Q16JWTC	Via Courier
2	HW	IC Part number	W77Q32JWTC	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN XSON10 4X4 (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q16JWXF	Via Courier
2	HW	IC Part number	W77Q32JWXF	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN XSON8 4X4 (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q16JWXG	Via Courier
2	HW	IC Part number	W77Q32JWXG	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN XSON8 2X3 (THICKNESS 0.4 MM)				
1	HW	IC Part number	W77Q16JWXH	Via Courier
2	HW	IC Part number	W77Q32JWXH	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN USON8 4X3 (THICKNESS 0.6 MM)				
1	HW	IC Part number	W77Q16JWUU	Via Courier
2	HW	IC Part number	W77Q32JWUU	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN USON8 2X3 (THICKNESS 0.6 MM)				
1	HW	IC Part number	W77Q16JWUX	Via Courier
2	HW	IC Part number	W77Q32JWUX	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN USON8 4X4 (THICKNESS 0.6 MM)				
1	HW	IC Part number	W77Q16JWUZ	Via Courier
2	HW	IC Part number	W77Q32JWUZ	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.54 MM)				
1	HW	IC Part number	W77Q16JWBY	Via Courier
2	HW	IC Part number	W77Q32JWBY	Via Courier
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q16JWBJ	Via Courier
2	HW	IC Part number	W77Q32JWBJ	Via Courier

NO	TYPE	IDENTIFIER	PART NUMBER	DELIVERY METHOD
FORM OF DELIVERY : ASSEMBLED DEVICE IN 12-BALL WLCSP (THICKNESS 0.5 MM)				
1	HW	IC Part number	W77Q16JWBK	Via Courier
2	HW	IC Part number	W77Q32JWBK	Via Courier
FORM OF DELIVERY : ASSOCIATED IC DEDICATED DOCUMENTATION				
1	PDF	Operational User Guidance [8]	Version C	Mail
2	PDF	Preparative Procedure [9]	Version C	Mail
3	PDF	Security Manual [10]	Version A7	Mail
4	PDF	Datasheet [7]	Version A6	Mail

2 Security Objectives for the Operational Environment

In order for the Platform to fulfill its security requirements, the operational environment (technical or procedural) described in this section.

2.1 Compliance to the Protection Profile

According to the Protection Profile [GP-SPE], the Platform must fulfil the following objectives:

- The application shall verify the correct version of all platform components it depends on
  Application Note: This requirement must be fulfilled as describe in [PRE] Section 3.2.
- The application shall support the invocation of an update mechanism, if such mechanism, exists in the platform.
  Application Note: This requirement is further expounded in Section 2.6
- The application shall implement the secure channel defined in "Secure Communication Enforcement", including detection of failed authenticity and integrity check.
  Application Note: This requirement is further expounded in Section 2.4
- The application shall store data to be protected for authenticity, integrity, or confidentiality in the area that is indeed protected for authenticity/integrity/confidentiality.
  Application Note: This requirement is further expounded in Section 2.4 and 3.1.
- The application can where relevant implement a freshness/anti-rollback protection using a "Reliable Index" provided by the platform
  Application Note: This requirement is not relevant here, since the freshness and anti-rollback protection is done by the Platform, not by an application. Reference to [OPE] section 2.2.1.

2.2 Generation of device's Individual Identifier

Before a Platform instantiation is used, it shall be allotted with its own unique ID.
The device is provided by Winbond with a pre-programmed ID, namely the 64-bit Winbond ID (WID), that is unique per device. In addition, the device can be programmed with a customer-specific ID, as described in [OPE] Section 2.3

2.3 Protection of the Platform Keys

Security procedures shall be used by the Platform operators to maintain the confidentiality and the integrity of the Platform keys, as described in [OPE] Section 3. Namely:

- The keys shall be generated with the required amount of entropy.
- The provisioning of the Device Master Key shall be done in a secure environment where the communication with the Platform is protected from eavesdropping.

Note: Provisioning of all other keys is protected by the Platform based on the confidentiality of the Device Master Key

- Keys stored in the authorized Host device and shared with the Platform shall be protected by the Host device

- Keys stored at the authorized Remote Operator and shared with the Platform shall be protected by the operator

2.4 Secure Communication with the Platform

The authorized Host device and an authorized Remote Operator shall support the trusted communication channel with the Platform protecting the confidentiality, integrity, and freshness of the transmitted data, as described in [OPE] Section 2.2.
Note: Data freshness means that the stored and transmitted data is always the one resulting in the last change carried out by the authorized user on the Platform.

2.5 Boot protected by Platform

The Host device boots from code stored on the Platform in a dedicated memory section, as described in [OPE] Section 2.5.

2.6 Genuine Software Update

The Host device update of the code stored on the Platform is carried out by an authorized Remote-Operator using the protective mechanisms of the Platform, as described in [OPE] Section 2.6.
Note: The secure Software Update is delivered in encrypted and genuine protected form by the authorized issuer together with its security attributes.

3 Security Requirements and Implementation

The claimed assurance and functional requirements package is **SESIP2** as defined in [GP-SESIP] and [GP-SPE]

3.1 Security Assurance Requirements

3.1.1 Complete functional specification (ADV_FSP.4)

In accordance with the requirement for a complete functional specification (ADV_FSP.4) the developer has provided the document [FSP], where the entire TSF is represented (full set of SFRs) and the SFRs are traced to the TSFIs. Moreover, related to each TSFI, the following information is given:

- Identification and description of all parameters
- Description of purpose and method of use
- Description of actions
- Description of error messages that may result from an invocation of the TSFI

3.1.2 Operational user guidance (AGD_OPE.1)

In accordance with the requirement for an operational user guidance (AGD_OPE.1), the developer provided the operational user guidance [OPE] for the Platform. This guidance includes the following information:

- The user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- How to use the available interfaces provided by the Platform in a secure manner.
- Available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- Security-relevant events.
- Modes of operation of the Platform (TEST mode and USER mode).
- Security rules to be followed in order to fulfil the security objectives for the operational environment.

3.1.3 Preparative procedures (AGD_PRE.1)

In accordance with the requirement for preparative procedures (AGD_PRE.1), the developer provided the Preparative User Guides [PRE] for the Platform. This guide includes the following information:

- Necessary steps for secure acceptance of the delivered Platform in accordance with the developer's delivery procedures.
- Necessary steps for secure installation of the Platform and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment.

3.1.4 Flaw Reporting Procedure (ALC_FLR.2)

Due to the Platform type (Memory Flash IC), and due to the fact that the Platform is a platform part with no software (no OS and no application), the SFR “Secure update of platform” is not applicable, since updates to the Platform are not possible, only replacement of the Memory Flash IC.

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), the developer has defined procedures described in [FLR] covering the following points:

- Reporting
- Evaluation.
- Solution.
- Communication.

Whenever a third party detects an issue, it is expected that the third party will contact the composite product vendor and this will further notify Winbond through the URL: https://www.winbond.com/hq/support/technical-support/?__locale=en.

3.1.5 Independent testing: conformance (ATE_IND.1)

In accordance with the requirement for Independent testing conformance (ATE_IND.1), the developer provides the Platform, the experimental set-up and the related documentation [ATE] for testing.

3.1.6 Vulnerability Analysis (AVA_VAN.2)

In accordance with the requirement for a Vulnerability Analysis (AVA_VAN.2), the developer provides the Platform and the necessary experimental set-up for testing.

3.2 Security Functional Requirements

The platform fulfills the security functional requirements as described in this Section.

Requirements mandated by [IEC62443-4-2] and [NIST-8259A] are identified in the description of each SFR as **refinements in bold**. Also, the TSS descriptions describe which portions of how the SFRs are met and how the IEC62443-4-2/ NIST-8259A requirements are satisfied are *identified in italics*.

3.2.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

Self-assessment:

- The Platform provides the secure acceptance procedure described in [PRE] Section 2.
- The same document lists the expected version numbers for all delivered parts of the Platform.

3.2.2 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

Self-assessment:

- Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-programmed globally unique 64-bit Winbond ID (WID).
- In addition, the device can be programmed with a customer-specific 128 bit ID (SUID), as specified in [SM] Section 5.3.4.
- The IDs can be read off the device by GET_WID and GET_SUID commands respectively, as specified in [SM] Section 5.2.1 and 5.2.2, *thus satisfying DI, DI2.*

3.2.3 Attestation of Platform Genuineness

The platform provides an attestation of the "Verification of Platform Identity" and "Verification of Platform Instance Identity", in a way that ensures that the platform cannot be cloned or changed without detection.

Self-assessment:

The process of device identification described in [OPE] Section 2.3 involves a cryptographic challenge-response possible as soon as the unique identifier is programmed to the TOE (with the default Device Master Key) and coming to the full strength after the specific Device Master Key is set, as specified in [PRE] Section 3.3.

~~3.2.4 Secure Update of Platform~~

~~The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.~~

3.2.5 Secure Update of Application

The application can be updated to a newer version in the field such that the integrity, authenticity, and confidentiality of the application is maintained.

Self-assessment:

The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2.

3.2.6 Secure Communication Enforcement

The platform ensures the application can only communicate with **the platform** over the secure communication channel(s) supported by the platform using **the protocols described in the SFR "Secure Communication Support" for data requested to be protected for confidentiality, integrity, or authenticity**

Self-assessment:

The memory is split into eight sections and the limits of each section as well as its security attributes are defined in the TOE Metadata (Global Memory Configuration, Global Mapping Table, and Section Configuration Registers).

The protected User Data is defined as one of the following (or a combination of both):

- **Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality.
- **Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication.

Any plain data access is prevented to the section that contain the protected User Data.

3.2.7 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates **the Host device or an authorized Remote Operator and the Platform** and protects against **disclosure (plaintext data disclosure by bus probing), modification (Man-in-the-Middle), hammering** (a.k.a. brute-forcing) **and replay** of messages between the endpoints, using **the secure SPI bus commands and the following security measures:**

- A fresh session key is used for each session in a way that provides mutual authentication at both ends of the communication channel
- In order to avoid key repetition, the TOE implements non-repetitive counters, namely a non-volatile Session Counter and a Transaction Counter, see Section 3.2.13
- The transmitted data (in both directions) and the command address are encrypted and signed.
    - The encryption key is generated for each transaction from the Session Key and the Transaction Counter to prevent replay attacks.
    - The signature is a calculated as a MAC tag with a combination of the Session Key and the Transaction Counter to prevent replay attacks.

Self-assessment:

Most commonly, the following subjects interact with the TOE:

- The *Host Device* that embeds the TOE and communicates with it through a SPI Bus.
- An authorized *Remote Operator*, that communicates with the TOE through the Host Device.

There are two Section Master Keys are associated with each memory Section, that allow two logical communication channels for each Section with different access rights. Although the communication between the TOE and the Remote Operator is done through the same SPI bus, the logical channel separation (i.e., the different keys for different channels) guarantee the security of the communication even if the Host Device is compromised.

The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel.

3.2.8 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

Self-assessment:

To protect against physical manipulation, the Platform includes the following security mechanisms:

- The bus connecting the Flash array and the Platform internal HW logic is hidden by layers of HW logic
- The checksum fields (CRC32) protect the stored keys, configuration information and the registers. When violation is detected, access is blocked, key usage is prevented, and status indication is raised.

Dedicated countermeasures in the key generation mechanism (see [SM] Section 3.2.2) protects the TOE against the inherent or intentional leak of the keys used in TOE operations.

3.2.9 Cryptographic Keystore

The platform provides the application with a way to store **the keys and TOE Metadata** such that not even the application can compromise the **authenticity, integrity and confidentiality** of this data. This data can be used for the cryptographic operations **to establish the secure channel and to control the memory access**.

Self-assessment:

The following keys and TOE Metadata fields are protected by the Platform:

- *Device Master Key* – used for secure key provisioning and memory configuration, protected in terms of integrity and confidentiality
- *Per-Section Keys* – used to access the section's data and its security functions, protected in terms of integrity and confidentiality*:*
    - *restricted Section Master Keys (read-only Section access)*
    - *non-restricted Section Master Keys (full Section access)*

  The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key.
- *TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key):
    - Winbond Device ID
    - Secure Unique Device ID
    - Global Memory Configuration
    - Global Mapping Table
    - Section Configuration Registers
- *Monotonic Counter* – used for replay protection, protected in terms of integrity (namely, it changes only in one direction – always incremented)

- The Keystore memory is not addressable by Read, Write and Erase commands. It can be accessed only through the Key Provisioning, protected as described in [PRE] Section 3.4.1.

3.2.10 Secure Storage

The platform ensures that all data stored by the application, except for **non-Authenticated User data**, is protected to ensure its authenticity and integrity as specified in **Secure Communication Enforcement** with a platform instance unique key of key length **128 bits**.

Self-assessment:

The Authenticated User Data is defined in the Self-assessment subsection of Secure Communication Enforcement. Any command modifying the content of a Section with Authenticated User Data shall be properly signed by a key derived from the Master Key of this section.

3.2.11 Secure Encrypted Storage

The platform ensures that all data stored by the application, except for **non-Secret User data**, is encrypted as specified in **Secure Communication Enforcement** with a platform instance unique key of key length **128 bits**.

Self-assessment:

The Secret User Data is defined in the Self-assessment subsection of Secure Communication Enforcement.
The secret data may be accessed only by a Secure Read command that reads it encrypted by a key derived from the Master Key of this section

3.2.12 Residual Information Purging

The platform ensures that **user data, configurations and keys**, with the exception of **None**, is erased using the method specified in **the guidance** before the memory is used by the platform or application again and before an attacker can access it.

Self-assessment:

This requirement is interpreted hereby to ensure that the User Data is not disclosed or manipulated via the features available in the TEST mode. Test Mode entry is protected in the following manner:

- When first entering TM, the entire Flash is erased, including user data, configurations and keys, and device management data (Monotonic Counter, Winbond Unique ID, etc.).

- Test mode entry is disabled before the device is shipped. When re-entering TM (after it was previously disabled), the device is Formatted before switching to TM.
- This formatting is skipped if user sets the Fault Analysis Mode entry flag in a cryptographically protected user register. This flag should be set only after user has removed any sensitive information stored on the device.

3.2.13 Reliable Index

The platform implements a strictly increasing function.
Self-assessment:

- The platform implements a 64-bit Monotonic Counter mechanism described in [SM] Section 3.2.1. The counter is used in key generation and signature calculation in a way that protects the secure communication from replay attacks.
- In addition, the Platform ensures that the version tag for the new FW version in Secure FW update is increasing. This ensures rollback protection for secure code updates.

3.2.14 Secure Initialization of Platform

The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to non-operational state.

Self-assessment:

The security policy initialization process verifies the integrity and the authenticity of the TSF data that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of physical manipulation of the TOE.

When an error is detected during the initialization process before the working State is reached, the TOE becomes locked and must enter Test Mode to resume regular initialization.

4 Mapping and sufficiency rationales

4.1 SESIP2 sufficiency

Assurance Class	Assurance Families	Coverage and Rational
ASE: Security Target evaluation	*ASE_INT.1 ST Introduction*	The ST reference is in the Title, the Platform reference in the "Platform Reference", the Platform overview and description in Platform Functional Overview and Description.
	ASE_OBJ.1 Security requirements for the operational environment	The objectives for the operational environment are described in the "Security Objectives for the Operational Environment" Section. Thereby the references to the guidance documents where these objectives are addressed are provided
	ASE_REQ.3 Listed Security requirements	The relevant SFRs from [GP-SESIP] are described "Security Functional Requirements". "~~Secure update of platform~~" not included (justification in ALC_FLR.2)
	ASE_TSS.1 Platform Summary Specification	All SFRs are listed in "Security Requirements and Implementation", and for each SFR the implementation and verification is defined in "Security Functional Requirements" Section.
ADV: Development	*ADV_FSP.4 Complete functional specification*	The [FSP] document precisely specifies all the platform's interfaces with a sufficient level of details, including direct error messages
AGD: Guidance documents	*AGD_OPE.1 Operational user guidance*	The [OPE] document provides a description of secure operation of the Platform and security rules to fulfil with security objectives for the operational environment.
	AGD_PRE.1 Preparative procedures	The [PRE] document provides a description of secure acceptance procedures and installation.
ALC: Life-cycle support	*ALC_FLR.2 Flaw reporting procedures*	The [FLR] document provides the flaw reporting and remediation procedure Since updates to the Platform are not possible, the for SFR "Secure update of platform" is removed.
ATE: Tests	*ATE_IND.1 Independent testing: conformance*	The [ATE] document provide evidence for testing. The Platform, the experimental set-up and the test plan has been delivered for the laboratory independent testing.
AVA: Vulnerability assessm	*AVA_VAN.2 Vulnerability analysis*	All delivered documentation, Platform and experimental set-up are the input for the vulnerability analysis to be performed by the laboratory.

4.2 IEC62443-4-2 Mapping

The IEC62443-4-2 Sufficiency Mapping has been organized in the following way:

- W77Q16/32 as a subcomponent, fulfils subset of IEC62443-4-2 requirements;
- W77Q16/32 provides services which support the overall component fulfilling IEC62443-4-2 requirements.

4.2.1 Sufficiency of Subset of IEC62443-4-2 Requirements

W77Q, as a subcomponent of a targeted IACS component, fulfills subset of the IEC62443-4-2 requirements, which provides support for the component.

Note that W77Q is not targeted as a standalone device and therefore not targeted to comply with the whole set of IEC62443-4-2. The applicable requirements and the mapping of SFR is provided to Table 1.

IEC62443-4-2 requires component developed and supported following the secure product development process described in IEC 62443-4-1.

Requirement	**Description**	**SL-C**				**Covered by**	**Refinement**
		1	**2**	**3**	**4**		
CCSC 4	Software development process: IEC62443-4-1 Compliance	x	x	x	x	Security Assurance Requirements (general)	
CR 1.1	Human user identification and authentication	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							• Section Configuration Registers
CR 1.1 (1)	Unique identification and authentication		x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table Section Configuration Registers
CR 1.1 (2)	Multifactor authentication for all interfaces			x	x	Cryptographic Keystore	
CR 1.2	Software process and device identification		x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness	
CR 1.2 (1)	Unique identification and authentication			x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness	
CR 1.3	Account management	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
							knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table Section Configuration Registers
CR 1.4	Identifier management	x	x	x	x	Cryptographic Keystore	*TOE Metadata* protected in terms of integrity (namely, they cannot be changed without knowing the corresponding Master Key): • Winbond Device ID • Secure Unique Device ID • Global Memory Configuration • Global Mapping Table Section Configuration Registers
CR 1.5	Authenticator management	x	x	x	x	Cryptographic Keystore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key.

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
CR 1.5 (1)	Hardware security for authenticators			x	x	Cryptographic Keystore Physical Attacker Resistance	
NDR 1.6	Wireless access management	x	x	x	x	Verification of Platform Identity & Attestation of Platform Genuineness	
NDR 1.6 (1)	Unique identification and authentication		x	x	x	Verification of Platform Instance Identity & Attestation of Platform Genuineness	
CR 1.9	Strength of public key-based authentication		x	x	x	Secure Communication Enforcement	
CR 1.9 (1)	Hardware security for public key based authentication		x	x	x	Secure Communication Enforcement	
CR 1.10	Authenticator feedback	x	x	x	x	Secure Communication Enforcement	Any plain data access is prevented to the section that contain the protected User Data
CR 1.11	Unsuccessful login attempts	x	x	x	x	Secure Communication Enforcement	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication
CR 1.14	Strength of symmetric key based authentication		x	x	x	Secure Communication Enforcement	*Use of session keys derived from the master key*
CR 1.14 (1)	Hardware security for symmetric key based authentication			x	x	Physical Attack Resistance & Secure Communication Enforcement	
CR 2.1	Authorization enforcement	x	x	x	x	Secure Communication Enforcement	

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
CR 2.1 (1)	Authorization enforcement for all users		x	x	x	Secure Communication Enforcement	
CR 2.6	Remote session termination		x	x	x	Secure Communication Support	*Fresh session keys usage*
CR 2.7	Concurrent session control			x	x	Secure Communication Support	*There is only the host device and the remote operator communicating the TOE through the Host Device. The amount of concurrent sessions is limited by the two master Keys associated to each memory section.*
CR 3.1	Communication integrity	x	x	x	x	Secure Communication Enforcement	
CR 3.1 (1)	Communication authentication		x	x	x	Secure Communication Enforcement	
CR 3.5	Input validation	x	x	x	x	Secure Communication Enforcement	
CR 3.7	Error handling	x	x	x	X	Secure Communication Enforcement	Any plain data access is prevented to the section that contain the protected User Data
CR 3.8	Session integrity		x	x	x	Secure Communication Enforcement	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication. Any plain data access is prevented to the section that contain the protected User Data
EDR/NDR 3.10	Support for Updates	x	x	x	x	Secure Update of Application	
EDR/NDR 3.10 (1)	Update authenticity and integrity		x	x	x	Secure Update of Application	
EDR/NDR 3.11	Physical tamper resistance and detection		x	x	x	Physical Attacker Resistance	

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
EDR/NDR 3.12	Provisioning product supplier roots of trust		x	x	x	Cryptographic KeyStore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key
EDR/NDR 3.13	Provisioning asset owner roots of trust		x	x	x	Cryptographic KeyStore	The *Per-Section Keys* are provisioned via a secure channel protected by the *Device Master Key* and cannot be modified without knowing this key
EDR/NDR 3.14	Integrity of the boot process	x	x	x	x	Secure Initialization of Platform	The security policy initialization process verifies the integrity and the authenticity of the TSF data that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of physical manipulation of the TOE.
EDR/NDR 3.14 (1)	Authenticity of the boot process		x	x	x	Secure Initialization of Platform	The security policy initialization process verifies the integrity and the authenticity of the TSF data that describes the memory partition, per-section memory access policies, and the keys. This approach mitigates the threat of physical manipulation of the TOE.
CR 4.1	Information confidentiality	x	x	x	x	Secure Communication Enforcement	
CR 4.2	Information persistence		x	x	x	Residual Information Purging	

Requirement	Description	SL-C				Covered by	Refinement
		1	2	3	4		
CR 4.2 (2)	Erase verification			x	x	Residual Information Purging	When first entering TM, the entire Flash is erased, including user data, configurations and keys, and device management data (Monotonic Counter, Winbond Unique ID, etc.). Test mode entry is disabled before the device is shipped. When re-entering TM (after it was previously disabled), the device is Formatted before switching to TM. This formatting is skipped if user sets the Fault Analysis Mode entry flag in a cryptographically protected user register. This flag should be set only after user has removed any sensitive information stored on the device.
CR 4.3	Use of cryptography	x	x	x	x	Security Communication Support	*Use of session keys derived from the master key*

Table 1 IEC62443-4-2 requirements Sufficiency

4.2.2 Features for Final Product towards IEC62443-4-2 Compliance

W77Q is designed to be used as a part of system, or in IEC62443-4-2 terms, as a subcomponent of an IEC62443-4-2 component. The features described in the SESIP SFRs can be safely utilized as part of the IEC62443-4-2 compliance of the final product.

Note it is up to the integrator on whether a feature is used for IEC62443-4-2 compliance and correct utilization of the feature, and this session is for guidance and informative purpose, but not in the scope of the SESIP evaluation. The integrator is responsible on how to design and architecture a component to fulfill IEC62443 requirements leveraging W77Q integrated to fit the purpose and security requirements.

4.3 NIST-8259A Mapping

Device cybersecurity capabilities [NIST-8259A], are cybersecurity features or functions that computing devices provide through their own technical means.

The IoT device cybersecurity capability core baseline is a set of device capabilities generally needed to support commonly used cybersecurity controls that protect devices as well as device data, systems, and ecosystems.

W77Q16/32 is designed to be used as a part of system, as a subcomponent. It fulfils subset of [NIST-8259A].

W77Q16/32, as a storage/memory component fulfilled the relevant focal document element, based on OLIR Program [8259A-SESIP]:

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
Device Identification (DI)	**The IoT device can be uniquely identified logically and physically.**	Semantic	Intersects with	[3.1.1]	Verification of Platform Identity	N	The Platform provides the secure acceptance procedure described in [PRE] Section 2	
DI-1	**A unique logical identifier**	Semantic	Equal	[3.1.2]	Verification of Platform Instance Identity	Y	Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-programmed globally unique 64-bit Winbond ID (WID)	
DI-2	**A unique physical identifier at an external or internal location on**	Semantic	Intersects with	[3.1.1]	Verification of Platform Identity	N	The Platform provides the secure acceptance procedure described in	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	the device authorized entities can access						[PRE] Section 2	
DI-2	**A unique physical identifier at an external or internal location on the device authorized entities can access**	Semantic	Intersects with	[3.1.2]	Verification of Platform Instance Identity	N	Each device (i.e., a specific instantiation of the platform) is provided to the customer with a pre-programmed globally unique 64-bit Winbond ID (WID),	
Device Configuration (DC)	**The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.**	Semantic	Superset of	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	SESIP requirements for a security feature includes all related protections including configuration capabilities
DC-1	**The ability to change the device's software configuration settings**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides	SESIP requirements for a security feature include

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	s all related protections including configuration capabilities
DC-2	**The ability to restrict configuration changes to authorized entities only**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	SESIP requirements for a security feature includes all related protections including configuration capabilities
Data Protection (DP)	**The IoT device can protect the data it stores and transmits from unauthorized access and modification.**	Semantic	Equal	[3.3.1]	Secure Communication Support	Y	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							for each type of the logical communication channel	
Data Protection (DP)	**The IoT device can protect the data it stores and transmits from unauthorized access and modification.**	Semantic	Equal	[3.3.2]	Secure Communication Enforcement	Y	**Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data confidentiality	
Data Protection (DP)	**The IoT device can protect the data it stores and transmits from unauthorized access and modification.**	Semantic	Equal	[3.6.1]	Secure Storage	Y	The Authenticated User Data is defined in the Self-assessment subsection of Secure Communication Enforcement. Any command modifying the content of a Section with Authenticated User Data shall be properly	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							signed by a key derived from the Master Key of this section.	
DP-1	**The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised**	Semantic	Superset of	[3.5.3]	Cryptographic KeyStore	N	The Keystore memory is not addressable by Read, Write and Erase commands. It can be accessed only through the Key Provisioning, protected as described in [PRE] Section 3.4.1.	
DP-2	**The ability for authorized entities to render all data on the device inaccessible by all entities, whether**	Semantic	Equal	[3.3.2]	Secure Communication Enforcement	Y	**Secret User Data** – Data (including executable codes) stored in the section of the Flash array that	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)						are defined as protected in terms of data confidentiality	
DP-3	**Configuration settings for use with the Device Configuration capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length**	Semantic	Intersects with	[3.5.3]	Cryptographic KeyStore	N	The Keystore memory is not addressable by Read, Write and Erase commands. It can be accessed only through the Key Provisioning, protected as described in [PRE] Section 3.4.1.	SESIP requirements for a security feature includes all related protections including configuration capabilities
Logical Access to Interfaces (LA)	**The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Secret User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							data confidentiality	
LA-1	**The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	
LA-1	**The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
LA-2	**The ability to logically restrict access to each network interface to only authorized entities (e.g., device authentication, user authentication)**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	
LA-2	**The ability to logically restrict access to each network interface to only authorized entities (e.g., device authentication, user authentication)**	Semantic	Intersects with	[3.3.2]	Secure Communication Enforcement	N	**Authenticated User Data** – Data (including executable codes) stored in the section of the Flash array that are defined as protected in terms of data integrity and authentication	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
LA-3	**Configuration settings for use with the Device Configuration capability including, but not limited to, the ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts**	Semantic	Intersects with	[3.3.1]	Secure Communication Support	N	The confidentiality and the integrity of the communication is protected as described above with the Session Key derived from the corresponding Master Key for each type of the logical communication channel	SESIP requirements for a security feature includes all related protections including configuration capabilities
Software Update (SU)	**The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
SU-1	**The ability to update the device's software through remote (e.g., network download) and/or local means (e.g., removable media)**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	
SU-2	**The ability to verify and authenticate any update before installing it**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	
SU-3	**The ability for authorized entities to roll back updated software to a previous version**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection,	

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
							as specified in [SM] Section 3.6.2	
SU-4	**The ability to restrict updating actions to authorized entities only**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	
SU-5	**The ability to enable or disable updating**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update mechanism with rollback protection, as specified in [SM] Section 3.6.2	
SU-6	**Configuration settings for use with the Device Configuration capability including, but not limited to: a. The ability**	Semantic	Intersects with	[3.2.4]	Secure Update of Application	N	The Platform stores the code and data for the Host device and provides the Secure Code Update	SESIP requirements for a security feature includes all related

Focal Document Element	Focal Document Element Description	Rationale	Relationship	Reference	Reference Document Element Description	Fulfilled By (Y/N)	Refinements	Comments
	to configure any remote update mechanisms to be either automatically or manually initiated for update downloads and installations b. The ability to enable or disable notification when an update is available and specify who or what is to be notified						mechanism with rollback protection, as specified in [SM] Section 3.6.2	protections including configuration capabilities
Cybersecurity State Awareness (CSA)	**The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only**				N/A for W77Q			Not covered by W77Q

5 References

[GP-SESIP] GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Version 1.1, Dated June 2021.

[GP-SPE] SESIP profile for Secure External Memories, version 1.0, September 2021, GPT_SPE_148.

[Datasheet] W77Q - Secure Serial NOR Flash Memory Data Sheet, Ver A6, Winbond Technology Ltd

[OPE] W77Q16JW/W77Q32JW Operational User Guidance, Ver C, Winbond Technology Ltd

[PRE] W77Q16JW/W77Q32JW Preparative Procedure, Ver C, Winbond Technology Ltd

[SM] W77Q - Secure Serial NOR Flash Memory Security Manual, Ver A7, Winbond Technology Ltd

[FSP] W77Q Secure Flash Memory Functional Specification, Ver C, Winbond Technology Ltd

[FLR] W77Q Secure Flash Memory: Flaw Remediation, Ver C, Winbond Technology Ltd

[ATE] ATE Tests Mapping Table , Ver A + W77Q Secure Flash Memory ATE Document, Ver A, Winbond Technology Ltd

[62443-1-1] IEC TS 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, edition 1.0, 2009, the International Electrotechnical Commission (IEC).

[62443-4-1] IEC TS 62443-4-1, Industrial communication networks - Network and system security - Part 4-1: Secure product development lifecycle requirements, edition 1.0, 2018, the International Electrotechnical Commission (IEC).

[62443-4-2] IEC TS 62443-4-2, Industrial communication networks - Network and system security - Part 4-2: Technical security requirements for IACS components, edition 1.0, 2019, the International Electrotechnical Commission (IEC).

[NIST-8259A] NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline, May 2020

[8259A-SESIP] OLIR Program: NIST-8259A-to-SESIP-v1.2 (1.0.0) Informative Reference Details, 08/17/2021