Site Security Target - EASL

Rev. 1.6 — 24 November 2022 **Objective evaluation document**

Revision History

Revision history

Revision number	Date	Description
1.0	09.04.2021	Initial version of the document, created first Version by NXP.
1.1	17.05.2021	Reduction of non-necessary material
1.2	06.07.2021	Brightsight comments update
1.3	08.07.2021	Adjust mapping of Evaluation Documentation
1.4	14.06.2022	Updated for re-certification
1.5	20.09.2022	Brightsight comments update
1.6	24.11.2022	Update classification, and typos

Classification

Public

1 SST Introduction

This document is based on the Eurosmart Site Security Target Template [1] with adaptations such that it fits the site.

This Site Security Target is intended to be used by only one specific client, namely NXP Semiconductors. Therefore, the term 'client' in this document refers directly to NXP Semiconductors.

1.1 Reference

Title: Site Security Target_EASL_SST

Version: 1.6

Date: 24th November 2022

Company: Electronic Assembly Services Ltd

Name of site: EASL

EAL: SARs taken from EAL6

1.2 Identification of the Site

The site EASL Corporation is located at:

Electronic Assembly Services Ltd.
24 Tournament Way
Ivanhoe Industrial Est.
Ashby-de-la-Zouch
Leicestershire
LE65 2UU

The type of site is: Board Assembly.

1.3 Site Description

1.3.1 Physical Scope

The entire building specified in Section 1.1 are in the scope of the SST. EASL receive secured materials and have no knowledge or interaction with the content. EASL is purely for the assembly of NXP materials. All NXP assets are constantly stored in the secured area therefor EASL have no knowledge or access to NXP IP.

1.3.2 Logical Scope

The building specified in Section 1.1 supports activities of many other organizations, but only the assembly of NXP assets are in the scope of this SST. No classified logical information is transferred between EASL and NXP. Activities of other organizations are not in scope of this SST.

The following services and/or processes provided by the site, are in the scope of the site evaluation process.

- Receipt, identification, registration and storage of ICs
- ICs packaging process including SMT process, X-Ray, Depannel, Soldering, Under fill and Cleaning.

The complete logical flow of the security ICs at the site is covered by the SST. In addition, the management of the security products related processes and the site security are also covered by the SST. The product flow of the security products on the site starts with the receipt of parts of the TOE (raw materials) up to the packing and handover for shipment of the finished security products.

The site does not directly contribute to the development of the intended TOE in the sense of Common Criteria. The intended TOE is then delivered to the client. As this is regarded as internal shipment, it is covered under aspect ALC_DVS.2 instead of ALC_DEL.1 that covers the delivery to an external customer which the site does not conduct.

The following life-cycle phases of the security products are subject of the SST.

- Life cycle phase 4: IC Packaging (according to the PP [6])
- Security IC packaging (and testing)

2 Conformance Claim

This SST is conformant with Common Criteria Version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, [2]

- Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, [3]

For the evaluation, the following methodology will be used:

- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017., [4]

This SST is CC Part 3 conformant.
There are no extended components required for this SST for the EASL Site.
The evaluation of the site comprises the following assurance components[1]:

- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

[1]*The activities of the site are not directly related to production and shipping of secure products. Therefore, this site does not claim conformance to ALC_DEL. The site does not contribute to ALC_TAT and does not have any negative impact to it. Therefore, this site does not claim conformance to ALC_TAT.*

3 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site. Goal is to achieve and hold a high security level to counter attacks with high attack potential at the site.

3.1 Assets

The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security concepts and the associated security measures as well as key and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the list of assets below.

The integrity of any machine or tool used for production is not considered as an asset. However, appropriate measures are defined for the site to ensure this important condition. These items consist of commercial available hardware and software which are programmed and customised by the site.

The following assets are handled at the site:

- documentation related to the assembling of the security products (intended TOE)
- product specifications e.g. product quality engineering documents, product documents
- evaluation documents
- Security ICs
- rejected material: Security ICs

There can be further client specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. They are handled in the same way as the other assets to prevent misuse, disclosure or loss of these sensitive items or information..

3.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. The intended TOE protects itself in life-cycle phase 7. However, during the production and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

The following threats are considered:

T.Smart-Theft: An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive assets. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered. In addition the attacker may be able to use specific working clothes of the site to camouflage the intention.

T.Rugged-Theft: An experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access sensitive areas and manipulate or steal sensitive assets.

T.Unauthorised-Staff: Unauthorised employees or subcontractors get access to assets, so that the confidentiality and/or the integrity of the intended TOE is violated.

T.Staff-Collusion: An attacker tries to get access to assets handled at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment. The target is to steal assets during the shipment/delivery process to gain access to TOE data.

3.3 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6. The chosen policies support the understanding of the production flow and the security measures of the site. In addition, they allow an appropriate mapping to the Security Assurance Requirements (SAR).

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated assembly flows and the security measures that are in the scope of the evaluation.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the received delivery can be identified and destroyed.

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organizational “two-employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are either destroyed at the site or sent back to the client (depending on the production-setup). This site does not provides secure destruction procedures for complete scrap ICs. All sent back procedures are under internal quality management control. The transport of configuration items from the site to the client is Policy Description considered as internal shipment.

P.Transport-Prep: Technical and organisational measures shall ensure the correct labelling of the product. A controlled internal shipment and the external delivery will be applied. The transport supports traceability up to the acceptor. If applicable or required this policy will include measures for packing if required to protect the product during transport.
The forwarder will be assigned by client or the site depends on different client and different trade terms. Internal shipment covers the transport of parts of the intended TOE or sensitive configuration items to the client and the transport to the inlay manufacturer as well (which is to be covered by the evaluation according to “Development security“, ALC_DVS.2).

3.4 Assumptions

A.Item-Identification: For the processing of NXP material the client shall provide information

A.Internal-Shipment: The recipient (client) of the product is identified by the address of the client site. The destination of the transport can be configuration item specific as part of the product setup. The client defines the requirements for packing of the security products in case the standard procedure is not applicable.

A.Product-Integrity: The self-protecting features of the devices are fully operational and it is not possible to influence the configuration and behavior of the devices based on insufficient operational conditions or any command sequence generated by an attacker or by accident.

A.External-Shipment: The forwarder is selected by the client and the shipping and tracing of the shipment is under control of the client.

The assumptions are outside the sphere of influence of the site. They are needed to provide the basis for an appropriate production process, to assign the product to the released production process and to ensure the proper handling, storage and destruction of all configuration items related to the intended TOE.

4 Security Objectives

The Security Objectives are related to physical, technical, and organizational security measures, the configuration management as well as the internal shipment and/or the external delivery.

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces two or three levels of access control (GREEN, YELLOW, RED area) to sensitive areas of the site. The access control measures ensure that only registered employees and can access restricted areas. Sensitive deliveries are handled in restricted areas only.

O.Security-Control: Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (assets). After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack.

O.Internal-Monitor: The site performs security management meetings at least every six months. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure a sufficient protection.

O.Maintain-Security: Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.

O.Control-Scrap: The site has no measures in place to destroy sensitive configuration items so that they do not support an attacker. Rejected or defect devices are returned to the client.

O.Staff-Engagement: All employees who have access to sensitive material and who can interact with deliveries are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job whatever is applicable for this site.

O.Zero-Balance: The site ensures that all sensitive products are separated and traced on a package unit basis. Two employee’s acknowledgement during hand over is applied for all shipments. According to the agreed production flow all materials delivered are securely destroyed.

O.Reception-Control: Upon reception of any material an immediate incoming inspection is performed on the packaging with the delivery weight confirmed. The inspection comprises the received amount, their package identification and the assignment of the items to a related internal process.

O.Internal-Transport: The recipient of a physical configuration item is identified by the assigned client address. The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

4.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

4.1.1 Mapping of Security Objectives

Table 1. Security Objectives Rationale

Threat and OSP	Security Objective	Note
T.Smart-Theft	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security**	The combination of security measures (physical, technical and organizational) ensure a detection of attacks and allows adequate reaction to prevent or limit damage.
T.Rugged-Theft	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security**	The combination of security measures ensure a detection of attacks and allows adequate reaction to prevent or limit damage.
T.Unauthorised-Staff	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security** **O.Staff-Engagement** **O.Zero-Balance** **O.Control-Scrap**	Physical access control measures limit the access to sensitive areas to authorised person only.
T.Staff-Collusion	**O.Internal-Monitor** **O.Maintain-Security** **O.Staff-Engagement** **O.Zero-Balance** **O.Control-Scrap**	Control procedures and personal accountability hinder collusion or allow to identify such attempts.
T.Attack-Transport	**O.Internal-Transport**	The measures allow detecting attack attempts.
P.Zero-Balance	**O.Internal-Monitor** **O.Staff-Engagement** **O.Zero-Balance** **O.Control-Scrap**	All functional and nonfunctional products are in the scope of the traceability.
P.Reception-Control	**O.Reception-Control**	Ensures only correctly identified products are released for production.

P.Transport-Prep	**O.Internal-Tansport**	Ensures only correctly identified products are securely prepared for shipping.

5 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

6 Security Assurance Requirements

Sites using this SST may require an evaluation against evaluation assurance level EAL6. Therefore, the Security Assurance Requirements are a superset of the SARs included in the Security IC Platform Protection Profile [6].

The Security Assurance Requirements (SAR) is chosen from the class ALC (Lifecycle support) as defined in [3]:

- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

The transport of parts of the intended TOE or sensitive configuration items between different development/production sites are to be covered by "Development security" (ALC_DVS.2)

6.1 Application Notes and Refinements

The description of the site certification process [5] includes specific application notes. The main item is that a product that is considered as intended TOE (i.e. any TOE type) is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

6.1.1 Overview and Refinements regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to (i) the „development environment”, (ii) to the „TOE” or „TOE design and implementation”. The component ALC_DVS.2 „Sufficiency of security measures” requires additional evidence for the suitability of the security measures.

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorized persons only, scrap must be controlled and destroyed.
Based on these requirements the physical security as well as the logical security of the site are in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

If the transfer of assets between two sites involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as

internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguish to ensure the correct subject of the evaluation.

6.1.2 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PP [6] provides a life-cycle description there specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialisation is performed at the site or not.

The PP [6] does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products are assembled and the functional devices are delivered to the client. The defective devices are returned to the client.

6.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [3] to the Security Objectives defined in this SST. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, this process is based on the assumption that the received configuration items are appropriately labelled and identified, refer to A.Item-Identification.

Note: The content elements that are changed from the original CEM [4] according to the application notes in the process description [5] are written in italic. The term TOE can be replaced by configuration items in most cases. In specific cases it is replaced by product (in the sense of “intended TOE”).

The site has a process in place to ensure an appropriate and consistent identification of NXP materials before delivery to EASL.

Table 2. Rationale for ALC_DVS.2

Security Objective	SAR	Rationale
O.Physical-Access **O.Security-Control** **O.Alarm-Response** **O.Staff-Engagement** **O.Maintain-Security** **O.Control-Scrap** **O.Zero-Balance** **O.Internal-Monitor** **O.Reception-Control** **O.Internal-Transport**	ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an attacker is controlled according to O.Control-Scrap. All devices including functional and non-functional are traced according to O.Zero-Balance and assisted by O.Internal-Monitor. The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O.Reception-Control. The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport.
O.Internal-Monitor **O.Maintain-Security** **O.Zero-Balance** **O.Reception-Control** **O.Internal-Transport** **O.Alarm-Response**	ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitoring O.Alarm-Response, and O.Maintain-Security. All devices including functional and non-functional are traced according to O.Zero-Balance. The reception and incoming inspection supports the detection of attacks during the transport of the security products to the site according to O.Reception-Control. The delivery to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport.

Security Objective	SAR	Rationale
O.Zero-Balance	ALC_LCD.1.1C The lifecycle Definition documentation shall describe the model used to develop and maintain the TOE.	The site does not perform development tasks. The applied production process are controlled according to all security products are traced according O.Zero-Balance.
O.Zero-Balance	ALC_LCD.1.2C The lifecycle model shall provide for the necessary control over the development and maintenance of the TOE.	The site does not perform development tasks. The applied production process are controlled according to all security products are traced according O.Zero-Balance.

Since this SST references the PP [6], the life-cycle module used in this PP includes also the processes provided by this site. Therefore the life-cycle module described in the PP [6] is considered to be applicable for this site.

7 Site Summary Specification

The Site Summary Specification describes aspects of how the Site meets the SARs.

7.1 Preconditions Required by the Site

This section provides background information on the assumptions defined in section 3.4. These assumptions can be seen as guidance for the client regarding the information and deliverables which are needed to allow the production under conditions described in this Site Security Target.

The site provides packaging services for security ICs. The client must provide appropriate information (the items listed as Asset in chapter 3.1) for the services as mentioned in chapter 1.2.2. The client provides a method of unique identification for all items shipped to the site. It is assumed, that the self-protecting features of the packaged ICs is fully operational. The recipient provides appropriate information for the internal shipment of ICs, semi-finished products containing these ICs, finished products as well as for the transfer of related data and documents.

For the setup of the production process, the client deliveries the relevant specifications and product information. In general, the release process can only be finished, if the required information is provided by the client and the samples are approved by the client.

The site is not responsibility for any transport outside their premises. The client is responsible for delivery and transfer of the products. This comprises the selection of the forwarder and the provision of data for the verification of the transport order. Any transport from or to the site is under the control of the clients. The client must define the packing requirements needed to support the confidentiality and integrity of the TOE. For each product the client must provide the destination for the shipment. There can be further client specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. The site verifies the identity of the car and the driver based on the provided pre-announcement by the client before any charge is handed over. The preannouncement is performed for each transport. The tracing and further control is under the responsibility of the client.

Regarding a destruction of rejected, defect or obsolete security products during the production flow, the scrap need to be sent back to the client.

7.2 Services of the Site

The site provides the services which covers parts of the life-cycle (as defined in [6]) phase 4 related to the packaging and testing of security ICs. In detail, the following services and related management procedures are provided:

- Receipt, identification, registration and storage of ICs
- ICs packaging process including SMT process, X-Ray, Depannel, Soldering, Under fill and Cleaning.
- Management and maintenance of the security measures was well as all associated process descriptions.

The site maintains a management system as a basis for all security process and rules. Each product gets a unique ID. This ID is linked with the security ICs.
The site does not directly contribute to the development of the intended TOE in the sense of Common Criteria.

The site has a standard procedure for packing of finished products and preparation of shipment. If special packing requirements are provided by the client they are included in the process setup. The client is alerted if products are ready for transport because the transport must be organized by the client. Based on the alert the client provides information on the forwarder that is used for the verification of the forwarder before the handover of the products.

Further on, the site returns the scrap configuration items to client. Defective or rejected products are returned to the client. The site ships the ICs to a destination defined by the client using a packing procedure also defined by the client that ensures a secure handling of the security ICs.

7.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the Security Objectives.

O.Physical-Access

The site is surrounded by infrared fence and controlled by CCTV. The access to the building is only possible via access controlled doors. The locking of the gate, the enabling of the alarm system and the additional external control are graduated according to the running operation at the site. This considers the manpower per shift as well as the operational needs regarding receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into three security levels. The access control ensures that only registered persons can access sensitive areas. This is supported by O.Security-Control that includes the maintenance of the access control and the control of visitors. The physical security measures are supported by O.Alarm-Response providing an alarm system.

Thereby the threats T.Smart-Theft, T.Rugged-Theft can be prevented. The physical security measures together with the the security measure provided by O.Security-Control enforce the recording of all actions. Thereby also T.Unauthorized-Staff is addressed.

O.Security-Control

Security guard and employee monitor the site and surveillance system 24/7. The CCTV system supports these measures because it is always enabled. Further on the security control is supported by O.Physical-Access requiring different level of access control for the access to security product.
This addresses the threats T.Smart-Theft and T.Rugged-Theft. Supported by O.Maintain-Security and O.Physical-Access also an internal attacker triggers the security measures implemented by O.Security-Control. Therefore also the Threat T.Unauthorized-Staff is addressed.

O.Alarm-Response
Security guard and responsible employee monitor the alarm system 24/7. The alarm system is connected to a control center that is manned 24 hours. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical Site resistance is lower than 5 minutes for a security event. That is able to provide enough time for guards and emergency contacts to control the event on-site.

This addresses the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff

O.Internal-Monitor
Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like Firewall, Virus protection and access control. Mayor changes of security systems and security procedures are reviewed in general management systems review meetings (per year). Upon introduction of a new process a formal review and release for mass production is made before being generally introduced.

This addresses T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Maintain-Security
The security relevant systems enforcing or supporting O.Physical-Access and O.Security-Control are checked and maintained regularly by the suppliers. In addition the configuration is updated as required either by employees (for the access control system) of the supplier. Logging files are checked at least monthly for technical problems and specific maintenance requests.

This addresses T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and T.Staff-Collusion

O.Staff-Engagement
All employees are interviewed before hiring. They must sign the terms and conditions of their employment contract and a code of conduct for the use of computers before they start working in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products. The security objective O.Physical-Access and support the engagement of the staff.

This addresses the threats T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance

O.Zero-Balance
Products are uniquely identified throughout the whole process. Further on the amount of ICs and for a production order is known. Handover and storage of security products is controlled by the 4-eyes principle and documented. Scrap and rejects are following the good products through the whole production process. At every process step the registration of good and scrapped/rejected products is updated. Before a production order is closed a zero balance calculation is documenting the history of good and bad parts of this order. This security objective is supported by O.Physical-Access, and O.Staff-Engagement.

This addresses the threats T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O.Reception-Control
At reception each configuration item including security products are identified by the shipping documents, packaging labels and information in the ERP system based on

shipment alerts from the clients. If a product cannot be identified it is put on hold in a secure storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seals of these boxes if applicable. Thereby only correctly identified products are released for production.

The OSPs P.Reception-Control are addressed by the reception control.

O.Internal-Transport
The recipient of a production lot is linked to the work order in the manufacture system and can only be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement of the client. This security objective is supported by O.Staff-Engagement.

The threat T.Attack-Transport and the OSP P.Transport-Prep are addressed by the internal transport.

O.Control-Scrap
Scrap is identified and handled in the same way as functional devices. They are stored internally in a secure location. The scrap is returned to the client using the same packing requirements as for functional products. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor.

Sensitive information and information storage media are collected internally in a safe location and destructed in a supervised and documented process
.
Supported by O.Physical-Access and O.Staff-engagement this addresses the threats T.Unauthorised-Staff and T.Staff-Collusion and the OSP P.Zero-Balancing

7.4 Security Assurance Requirements Rationale

The Security Assurance Rational is given in section 6.2. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in [23]. Therefore the following Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. In general the selected Security Assurance Requirements fulfil the needs derived from the Protection Profile [6]. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled

7.5 Assurance Measure Rationale

O.Physical-Access
ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore the Security Assurance Requirements are suitable to meet the objective.

O.Security-Control
ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment. Therefore the Security Assurance Requirements are suitable to meet the objective.

O.Alarm-Response
ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation including the initialization in its development and production environment. Therefore the Security Assurance Requirements are suitable to meet the objective.
ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

O.Internal-Monitor
ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore the Security Assurance Requirements are suitable to meet the objective.
ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

O.Maintain-Security
ALC_DVS.2.1C: requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Therefore the Security Assurance Requirements are suitable to meet the objective.
ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

O.Staff-Engagement
ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore the Security Assurance Requirements are suitable to meet the objective.

O.Zero-Balance
ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore the Security Assurance Requirements are suitable to meet the objective.
ALC_DVS.2.2C require the development security documentation to justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby these SARs are suitable to meet the security objective.

ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Reception-Control
ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Therefore the Security Assurance Requirements are suitable to meet the objective.

O.Internal-Transport
ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation. Therefore the Security Assurance Requirements are suitable to meet the objective.

O.Control-Scrap
ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation. Therefore the Security Assurance Requirements are suitable to meet the objective.

7.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The specifications and descriptions provided by the client are not part of the configuration management at the site.

The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

Security Objective	SAR	Rationale	Reference
O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Reception-Control O.Internal-Transport O.Control-Scrap O.Zero-Balance	ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	The development security documentation describes the physical (O.Physical-Access, O.Security-Control, O.Alarm-Response), procedural (O.Internal-Monitor, O.Maintain-Security, O.Control-Scrap), personnel (O.Staff-Engagement, O.Internal-Transport, O.Zero-Balance), security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its environment.	QAI004 QAI020 QAI058 QAI060 QAI023 QAI032 QAI121 QAI129 QAI130
O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Zero-Balance O.Reception-Control O.Internal-Transport O.Control-Scrap	ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Alarm-Response, O.Internal-Monitor, O.Internal-Transport, O.Reception-Control and O.Maintain-Security. All devices including functional and non functional are traced according to O.Zero-Balance. Defective devices are securely disposed according to O.Control-Scrap.	QAI020 QAI058 QAI023 QAI032 QAI121 QAI129 QAI130

Security Objective	SAR	Rationale	Reference
O.Zero-Balance	ALC_LCD.1.1C: The lifecycle Definition documentation shall describe the model used to develop and maintain the TOE.	The applied production process is controlled and devices are checked according to O.Zero-Balance.	QAI023 QAI032
O.Zero-Balance	ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the intended TOE.	The applied production process is controlled and devices are checked according to O.Zero-Balance.	QAI023 QAI032

8 Bibliography

8.1 Literature

The following documentation was used to prepare this SST:

[1] Site Security Target Template, Version 1.0, published by Eurosmart, Eurosmart, 21.06.2009.

[2] Common Criteria for Information Technology Security Evaluations, Part 1: Introduction and General Model; Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017.

[5] Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.

[6] Security IC Platform Protection Profile with Augmented Packages (BSI-CC-PP-0084-2014), Version 1.0, Eurosmart, 2014.

8.2 Definitions

Client
The term “client” is used in this SST to denote the IC manufacturer, which is a customer of EASL (EASL operates as an IC assembly for the IC manufacturer).

Consumer
The term “consumer” is used in this SST to denote the customer of the IC manufacturer, which the finished and functionally tested ICs are delivered to.

8.3 Abbreviations

The following abbreviations are used in this SST:

Term	Definition
ALC_CMC	
Assurance Class	Life-cycle support; Assurance Family: CM capabilities
ALC_CMS -	Assurance Class: Life-cycle support; Assurance Family: CM scope
ALC_DEL -	Assurance Class: Life-cycle support; Assurance Family: Delivery
ALC_DVS -	Assurance Class: Life-cycle support; Assurance Family: Development security
ALC_LCD -	Assurance Class: Life-cycle support; Assurance Family: Life-cycle definition
ALC_TAT -	Assurance Class: Life-cycle support; Assurance Family: Tools and techniques
CC -	Common Criteria
CM -	Configuration Management
CEM -	Common Methodology for Information Technology Security Evaluation EAL Evaluation Assurance Level
GDS -	Graphic Data System
IC -	Integrated Circuit
IT -	Information Technology
OSP -	Organisational Security Policy
PP -	Protection Profile
SAR -	Security Assurance Requirement
SMT -	Surface Mount Technology
SST -	Site Security Target
TOE -	Target of Evaluation

9 Legal information

9.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not
give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement
of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without
notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or

safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable
for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors
accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with
their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using

NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by
customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

9.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owner.

