Site Security Target Lite
For Sigurd Hukou

Sigurd Microelectronics Corp.

History of changes

Version	Date	Author(s)	Changes
01	2017-06-01	David Yen	Initial Version
02	2017-06-20	David Yen	Revise 1.1.1 & 1.1.2 & Table 7.2 Version and Date
03	2017-08-31	David Yen	Change Document Security Level from Confidential to General

Table of Contents

List of Tables

1. SST Lite Introduction

The SST Lite describes the security features of a site and therefore defines the scope of the site. This chapter is divided into the sections "SST Lite reference and Site reference" and "Site description".

1.1 SST Lite Reference and Site Reference

1.1.1 SST Lite Reference

Document title:	Site Security Target Lite for Sigurd Hukou
Author:	David Yen
Version number:	03
Effective Date:	2017-08-31

1.1.2 Reference number: MCCH-0000-0002 Rev. 03 Site Reference

Name of the site:	Sigurd Microelectronics Corp. (hereinafter referred to as SIGURD)
Location:	Sigurd HuKou Site
Organization:	Sigurd Microelectronics Corp.
Product type:	Wafers and dice with security ICs

1.2 Site Description

1.2.1 Physical Scope of the Site

The production site of SIGURD locates in HuKou site, which is located in the county of Hsinchu in

Taiwan.

Location: HuKou Site (hereinafter referred to as **SIGURD)**

No. 1, Siwei Road. Hsinchu Industrial Park, HuKou, Hsinchu, Taiwan R.O.C.

SIGURD provides Wafer Test and Final Test of smart ICs for security products.

The location consists of 2 buildings, which are inter-connected and surrounded by a fence, there are guarded with surveillance and secured by security guards, restrictions and access control from main gate and side gate.

The services of SIGURD site includes Wafer Test and Final Test of smart ICs for both security and non-security products. The entry of Secure Area is restricted by strict access control system. The non-security products are developed explicitly excluded from Secure Area. The site comprises the production facilities, warehousing and material dispatch, customer service, equipment maintenance, engineering, configuration control, as well as the IT office for the site.

The infrastructure such as test systems and the quality management, human resources and security are controlled and maintained from this location. These functions are used by this site as well by the other production sites of SIGURD.

1.2.2 Logical Scope of the Site

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

- Receipt, identification, registration and storage of un-sawn wafers as well as ICs
- Wafer and ICs testing process including baking, Lead Scan ,Visual Mechanical & packing
- Final test of wafers/packed ICs including Functional testing, DC testing, Mix-signal testing, pre-personalization (if necessary)
- Warehousing and dispatch of finished wafers and ICs
- Scrap units return to client for scrap/reject wafer ,dice & ICs on requests by the client

The complete logical flow of the security ICs and Smart Card related devices (i.e. security products) at the site is covered by the SST Lite. In addition, the management of the security products related processes and the site security are also covered by the SST Lite. 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 site ensures a reproducible test flow process within the limits defined. The test flow parameters and data applied are subject of the configuration management. Using the received wafers and test data, the site does conduct testing and pre-personalisation. 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 Lite.

- Life cycle phase 4: Wafer & IC Testing (according to the PP [6] & [7])
  - ✓ Security wafer & IC testing
  - ✓ Pre-personalisation if necessary

2. Conformance Claims

The evaluation is based on Common Criteria Version 3.1, release 4

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012, [1]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012, [2]

This SST Lite is CC part 3 conformant.

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 4, September 2012, [3]
- Supporting Document, Site Certification, October 2007, Version 1.0, Re-vision 1, CCDB-2007-11-001 [4]
- Guidance for Site Certification, Version 1.1 , 2013-12-04 [5]

The evaluation of the site comprises the following assurance components:

ALC_CMC.5, ALC_CMS.5, ALC_DEL.1[1], ALC_DVS.2, ALC_TAT.3[2] and ALC_LCD.1.

The assurance level chosen for the SST Lite is compliant to the Protection Profile [6] & [7] and therefore suitable for security ICs.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class "Life-cycle Support". For the assessment of the security measures attackers with high attack potential are assumed. Therefore this site supports product evaluations of products up to EAL6.

The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) [6] & [7]. Therefore the scope of the evaluation is suitable to support product evaluations up to assurance level EAL6 conformant to Part 3 [2] of the Common Criteria.

[1] The site does not provide contributions to ALC_DEL.1. However, the component is included here to support the reuse of the evaluation results and to enable the justification of the evaluator regarding ALC_DEL.1.

[2] The site does not provide contributions according to the definition of ALC_TAT.3. However, the component is included here to support the reuse of the evaluation results and to enable the justification of the evaluator regarding ALC_TAT.3.

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 Asset

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 development, production and testing 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 SIGURD.

The following assets are handled at the site:

- documentation related to the testing of the security products (intended TOE)
- probe cards and load boards
- product specifications e.g. Test plan and electrical design
- rejected dice/ICs/wafers
- scripts, data, and keys needed for the pre-personalization process
- test programs which may include authentication data for testing
- wafers (dice)

- Engineering samples
- Hard drive & USB token

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 development, production, test and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

The following threats are considered:

Table 3.1 – Threats for the Site

Threat	Description
T.Smart-Theft	**An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration items. 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.** This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get unregistered or defect devices that can be used to further investigate the functionality of the device and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk. It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control

Threat	Description
	and surveillance. In general an access control concept with two or three levels shall be implemented. If two levels are implemented, the more restrictive level of the access control shall prevent the simple access using a lost or stolen access token. Other restrictions may be the need for parallel access by two employees. The technical measures shall include automated measures to support the surveillance.
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 configuration items.** Although this attack is applicable for each site the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are considered to be sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing or personalization state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential. Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the splitting of sensitive data like keys provide additional support against such attacks. Also the unique registration of the products can support the protection if they can be disabled or blocked.
T.Computer-Net:	**A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as test data or other sensitive production data or modify the testing or production process at the site.** A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow to attack a product or manipulate a product or retrieve information to allow or change the configuration or the personalization. In addition, a successful access to a company network

Threat	Description
	leads to loss of reputation of the company processing the product or the company that produces the product. Such attackers are considered to have high attack potential because the attacker may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company. Therefore, also for the company network a protective concept with more than one level is expected. This shall comprise a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users shall have individual accounts which require authentication using e.g. a password. For specific tasks or processes standalone networks may be required. The protection must be supported by appropriate measures to update and maintain the computer and network systems and analyze logs that may provide indications for attack attempts.
T.Accident-Change	**An employee, contractor or student trainee may exchange products of different production lots or different clients during production by accident.** Employees, contractors or student trainees that are not trained may take products or influence production systems without considering possible impacts or problems. This threat includes accidental changes e.g. due to working tasks of student trainees or maintenance tasks of contractors within the development, production or test area. Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of different clients or different products of the same client are mixed during production. This also includes the disposal of security products using the standard flow and not the controlled destruction.

Threat	Description
T.Unauthorised-Staff	**Employees or subcontractors not authorized to get access to products or systems used for production get access to products or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.** Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. sensitive test and/or configuration data within the test center. Also other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to start an attack. The disposal of defect equipment and/or sensitive configuration items must be considered. The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to this different measures are required.
T.Staff-Collusion	**An attacker tries to get access to material processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.** Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorized employees and the split of sensitive knowledge like personalization keys can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.
T.Attack-Transport	**An attacker might try to get data, specifications or products during the internal shipment. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment process to allow a modification, cloning or the retrieval of confidential information at later life cycle states. Confidential information comprises design information, test documentation and test**

Threat	Description
	data as far as classified as sensitive. The protection of the internal shipment is based on the configuration of the products that are provided to SIGURD. SIGURD assumes that the configuration items are protected according to assumption A.Product-Integrity.

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 test and assembly flows and the security measures that are in the scope of the evaluation.

Table 3.2 – OSP addressed by the Site

Policy	Description
P.Config-Items	**The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.** The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receipt and the item each item is assigned to an internal unique identification. This holds also for test programs and other items that are provided to the site for local use. For configuration items that are created, generated or developed at the site the naming and identification must be specified.

Policy	Description
P.Config-Control	**The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client.** The product setup includes the following information (i) identification of the product, (ii) properties of the product when received at the site (iii) properties of the product when internally shipped, (iv) classification of the items (which are security relevant), (v) who (SIGURD or the client) is responsible for destruction of defect devices, (vi) how the product is tested after assembly, (vii) any configuration of the processed item as part of the services provided by the site, (viii) which address is used for the internal shipment.
P.Config-Process	**The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for the assembly and testing of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by a site.** The documentation with the process descriptions and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases automated tools are used to support the processes at the site. This comprises e.g. scripts or batch routines developed by the site and a commercial data base system. This comprises also service levels and quality parameters. The documentation that includes the process descriptions and the security measures of the site is under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases automated tools are used to support and control the production process of the site. This comprises e.g. scripts or batch routines developed by the site to track the test flow process of the intended TOE. This can also comprise service levels or quality parameters.
P.Reception-Control	**The inspection of incoming items done at the site ensures that the**

Policy	Description
	received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data is available to process the items. The incoming inspection is performed with several conducted steps considering different and identification configuration parameters of wafer received and supported by automated tools for the subsequent production process. They are considered as sensitive configuration items that must be tracked at the site.
P.Accept-Product	**The testing and quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.** The site does comprise testing and sampling according to defined test plans and testing. Automated measures are in place including utilization of tracking tools.
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-eye 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 provides secure destruction procedures for complete scrap wafers and/or dice. A destruction process is mandatory and will be agreed between the client and the site who is responsible for the destruction of defect devices. All processes contributing to the destruction and/or sent back procedures are under internal quality management control. The transport of configuration items from the site to the client is considered as internal shipment.

Policy	Description
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).
P.Data-Transfer	**Any data in electronic form (e.g. product specifications, test programs, test program specifications, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition measures are used to control the integrity of the data after the transfer.**
P.Secure-Scrap	**Deletion of data in electronic format (e.g. product specifications, test programs, test program specifications, release information etc.) that is classified as sensitive or higher security level by the client will perform secure delete.** **For preservation media (e.g. servers/hard drive), disk scrap by physically breaking up and disposal.**

3.4 Assumptions

The site is operating in a production flow and therefore must rely on preconditions provided by the previous site. This means, each site relies on the materials and information received by the previous site/client. This is reflected by the assumptions which are to be fulfilled by the client.

Table 3.3 – Assumptions for the client

Assumption	Description
A.Item-Identification	Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.
A.Product-Spec	The product developer must provide appropriate specifications and guidance for the assembly and testing of the product. This comprises bond plans for an appropriate assembly process as well as test requirements and test parameters for the development of the functional tests or a finished test program appropriate for the final testing. The provided information includes the classification of the delivered items, documents and data.
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.Testdata-Support	The client must provide test data and optional pre-personalisation data via a secure connection to the site in correct data format. The client is responsible for the secure transfer of data into the security network. The data must be prepared in a way, so that site is able to directly get the data from the client in order to process it using their testers.

The assumptions are outside the sphere of influence of SIGURD. 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

4.1 Security Objectives

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

Table 4.1 – Security objectives for the Site

Objective	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures enforce the access of authorized staff only and allow a sufficient separation of employees to enforce the "need to know" principle. The access control supports the limitation for the access to sensitive areas including the identification andrejection of unauthorized people. The site enforces two or three levels (level 0 to level 2) of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Security products are handled in restricted areas only. The site provides a secured space within secure area where a client may place any network connection equipment to support A.Testdata-Support.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance. Responsibilities and measures for responding to alarms are defined. 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.

Objective	Description
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 (asset). After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.
O.Internal-Monitor	The site performs security management meetings at least every three 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 are 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 authorized employees have access to sensitive areas as well as computer/network systems to ensure the protection of the networks and computer systems based on the appropriate configuration.

Objective	Description
O.Locical-Access	The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into a production network and an office network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and related systems is restricted to authorize employees that work in the related area or that are involved in the configuration tasks or the production systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.
O.Logical-Operation	All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.
O.Config-Items	The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the client. Also the internal procedures and guidance are covered by the configuration management.

Objective	Description
O.Config-Control	The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. Minor changes are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the classification and release of changes. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be changed by authorized personnel only. Automated systems support configuration management and production control.
O.Config-Process	The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the configuration of test programs and the assembly of the products, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site.
O.Acceptance-Test	The site delivers configuration items that fulfil the specified properties. Parameter checks, functional and visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.
O.Staff-Engagement	All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production flow are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

Objective	Description
O.Zero-Balance	The site ensures that all security products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. All devices are tracked until they are either shipped or destructed locally.
O.Reception-Control	Upon reception of products an immediate incoming inspection is performed. The inspection comprises the received amount of products and the identification and assignment of the product to a related internal production 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.
O.Data-Transfer	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.
O.Control-Scrap	The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker. Rejected or defect devices are either destructed locally or they are returned to the client.

4.2 Relation between Security Objectives and the Security Problem Definition

This SST Lite includes a Security Objectives Rationale with two parts. The first part includes a tracing which shows how the threats and OSPs are covered by the Security Objectives. The second part described in chapter 7.3 includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions defined in this Site Security Target cannot be used to cover any threat or OSP of the site. They are seen as pre-conditions fulfilled either by the site providing the sensitive configuration items or by the site receiving the sensitive configuration items. Therefore, they do not contribute to the security of the site under evaluation.

Table 4.2 – 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**	Adequate reaction on an attack is ensured by these measures.
T.Rugged-Theft	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security**	Adequate reaction on an attack is ensured by these measures.
T.Computer-Net	**O.Internal-Monitor** **O.Maintain-Security** **O.Logical-Access** **O.Logical-Operation** **O.Staff-Engagement**	The measures prevent an interfering access to the internal network.
T.Accident-Change	**O.Logical-Access** **O.Logical-Operation** **O.Config-Items** **O.Config-Control** **O.Config-Process** **O.Acceptance-Test** **O.Staff-Engagement** **O.Zero-Balance**	The automated measures and the control procedures avoid this threat.
T.Unauthorised-Staff	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Internal-Monitor** **O.Maintain-Security** **O.Logical-Access** **O.Logical-Operation** **O.Staff-Engagement** **O.Config-Control** **O.Zero-Balance** **O.Control-Scrap**	Physical and logical access control limits the access to the assigned tasks. Control procedures and personal accountability hinder uncontrolled access.
T.Staff-Collusion	**O.Internal-Monitor**	Control procedures and personal

Threat and OSP	Security Objective	Note
	O.Maintain-Security **O.Staff-Engagement** **O.Zero-Balance** **O.Data-Transfer** **O.Control-Scrap**	accountability hinder uncontrolled access.
T.Attack-Transport	**O.Internal-Transport** **O.Data-Transfer**	The measures allow detecting attack attempts.
P.Config-Items	**O.Reception-Control** **O.Config-Items**	All relevant items are covered by the control.
P.Config-Control	**O.Config-Items** **O.Config-Control** **O.Logical-Access**	The scope comprises the introduction of production flows and their controlled change.
P.Config-Process	**O.Config-Process**	The scope comprises the production flow processes and the documentation of the site.
P.Reception-Control	**O.Reception-Control**	The control ensures the correct identification and assignment of configuration items. Further a correct pairing is ensured.
P.Accept-Product	**O.Config-Control** **O.Config-Process** **O.Acceptance-Test**	Ensures the compliance of the finished product with the specifications.
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.Transport-Prep	**O.Config-Process** **O.Internal-Transport** **O.Data-Transfer**	The correct destination address, the controlled packing and the tracing of the transport ensure the correct shipment.
P.Data-Transfer	**O.Data-Transfer**	All data received or transmitted is handled accordingly in an appropriate security level.
p.secure-scrap	**O.control-scrap**	All data in electronic format is deleted by secure delete program.

5. Extended Components Definition

No extended components are currently defined in this SST Lite.

6. Security Requirements

Sites using this SST Lite 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] & [7].

The Security Assurance Requirements (SAR) is chosen from the class ALC (Lifecycle support) as defined in [2]:

- CM capabilities (ALC_CMC.5)
- CM scope (ALC_CMS.5)
- Delivery (ALC_DEL.1)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

The Security Assurance Requirements listed above fulfil the requirements of [4] because hierarchically higher components are used in this SST Lite. In addition, the minimum set of SAR is extended by SAR of the assurance components for "Delivery" (ALC_DEL.1), "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), whereas the transport of the finished intended TOE to the consumer is dealt with in "Delivery" (ALC_DEL.1).

ALC_DEL.1 covers the packing and shipment. The site is only responsible for the packing. The shipment itself is outside the responsibility of the site. The component is included to support the reuse of the evaluation results and to enable the justification of a TOE evaluation regarding ALC_DEL.1.

6.1 Application Notes and Refinements

The description of the site certification process [4] 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 Lite the associated processes for the handling of products are in the focus and described in this SST Lite. These processes are subject of the evaluation of the site.

6.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dice and/or packaged products (e.g. modules/inlays) is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dice and/or packaged products, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It is ensured, that wafers, dice or assembled devices removed from the production stage (i) are returned to the production stage from where they were removed or (ii) are securely stored and destroyed.

According to [4] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. The application notes in [4] are defined for ALC_CMC.5. The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as on the site security measures.

The configuration control and a defined change process for the procedures and descriptions of the site under evaluation are mandatory. The control process must include all procedures that have an impact on the evaluated production processes as well as on the site security measures.

The life-cycle described in [6] & [7] is a complex production process. Only parts of this production process are normally provided at a specific site. In such a case the control of the product during such a production process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be under configuration management for these cases.

The configuration items for the considered product type are listed in section 3.1. The CM documentation of the site is able to maintain the items listed for the relevant life-cycle step and the CM system is able to track the configuration items.

A CM system is employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures are in place to maintain the integrity and confidentiality of the configuration items.

6.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

The scope of the configuration management for a site certification process is limited to the documentation relevant for the SAR for the claimed life-cycle SAR and the configuration items handled at the site.

In the particular case of a security IC the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 3.1 that are considered as “TOE implementation representation” include:

- logical design data
- physical design data
- IC dedicated software

In addition, process control data, test data and related procedures and programs can be in the scope of the configuration management.

6.1.3 Overview and Refinements regarding Delivery Procedure (ALC_DEL)

The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE or parts of it (ii) to the consumer or consumer's site (Composite TOE Manufacturer). The CC assurance component ALC_DEL.1 requires procedures and technical measures to maintain the confidentiality and integrity of the product. The means to detect modifications and prevent any compromise of the Initialisation Data and/or Configuration Data may include supplements of the Security IC Embedded Software.

In the particular case of a security IC more "material and information" than the TOE itself (which by definition includes the necessary guidance) is exchanged with clients or consumers. Since the TOE can be externally delivered after different life-cycle phases (phases 4 or 5) the Site Security Target must consider the data that is exchanged by the sites either as part of the product or separate as input for further production steps.

Since the assurance component ALC_DEL.1 is only applicable to the external delivery to the consumer, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS refer to the CEM [3], paragraph 1087. However, the component ALC_DEL.1 is included here to support the reuse of the evaluation results and to enable the justification of the evaluator on the classification of the delivery.

6.1.4 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-personalisation data must be guaranteed, access to any kind of samples (client specific samples or open samples) development tools and other material must be restricted to authorised persons only, and scraps must be controlled and destroyed.

Based on these requirements the physical security as well as the logical security of the site is 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 configuration items 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 be clearly distinguished to ensure the correct subject of the evaluation.

6.1.5 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] & [7] 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] & [7] 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 scrapped or also returned to the client.

6.1.6 Overview and Refinements regarding Tools and Techniques (ALC_TAT)

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyse and implement the TOE. The component ALC_TAT.3, “Compliance with implementation standards-all parts”, requires definition and evidence for the suitability of the tools and techniques used for the development process of the TOE.

Since no TOE development and production in the sense of the Common Criteria is performed on the Smart Card Production Site, there are no development and production tools to be described. Especially, no compilation of products is performed. Therefore there is no risk of misconfigurations due to not well-defined tools or ambiguous statements or comments that have to be addressed. However, the component is included here to support the reuse of the evaluation results and to enable the justification of the evaluator regarding ALC_TAT.3.

6.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [2] to the Security Objectives defined in this SST Lite. 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 [3] according to the application notes in the process description [4] 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").

Table 6.1 – Security Assurance Rationale

SARs	Objectives	Rationale
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.	**O.Config-Items**	All products assembled at SIGURD get a unique client part ID automatically generated by a data base as defined by O.Config-Item.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	**O.Reception-Control** **O.Config-Item** **O.Config-Control** **O.Config-Process**	Incoming inspection according O.Reception-Control ensures product identification and the associated labelling. This labelling is mapped to the internal identification as defined by O.Config-Item. This ensures the unique identification of security products. O.Config-Control ensures that each client part ID is setup and releases based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorized staff. O.Config-Process provides a configured and controlled production process.
ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	**O.Reception-Control** **O.Config-Items** **O.Config-Control**	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications. O.Config-Items comprise the internal unique identification of all items that belong to a client part ID. Each product is setup according to O.Config-Control comprising all necessary items.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	**O.Reception-Control** **O.Config-Items** **O.Config-Control**	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications.

SARs	Objectives	Rationale
		O.Config-Item comprises the internal unique identification of all items that belong to a client part ID. Each product is setup according to O.Config-Control comprising all necessary items.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	**O.Config-Control** **O.Config-Process** **O.Logical-Access** **O.Logical-Operation**	O.Config-Control assigns the setup including processes and items for the production of each client part ID. O.Config-Process comprises the control of the production processes. O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff.
ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.	**O.Config-Process** **O.Zero-Balance** **O.Acceptance-Test**	O.Config-Process comprises the automated management of the production processes. O.Zero-Balance ensures the control of all security products during production. O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.
ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	**O.Reception-Control** **O.Logical-Access**	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications for all security products. O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorised staff.
ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.	**O.Config-Items** **O.Config-Control** **O.Config-Process**	O.Config-Items comprises the internal unique identification of all items that belong to a client’s part ID. O.Config-Control describes the management of the clients part IDs at the site.

SARs	Objectives	Rationale
		According to O.Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.9C The CM system shall support the audit of all changes to the *CM items* by automated means, including the originator, date, and time in the audit trail.	**O.Config-Items** **O.Acceptance-Test** **O.Config-Control** **O.Config-Process**	O.Config-Items comprise the internal unique identification of all items that belong to a client part ID. O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site. O.Acceptance-Test provides an automated testing of the functionality and supports the tracing.
ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	**O.Config-Control** **O.Config-Process**	O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the *product* is generated.	**O.Reception-Control** **O.Logical-Access** **O.Config-Control** **O.Config-Process**	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications. O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorised staff. O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	**O.Config-Control** **O.Config-Process**	According to O.Config-Control the setup of each client part ID includes an associated CM plan including the release. O.Config-Process ensures the reliability of the processes and tools based on dedicated CM

SARs	Objectives	Rationale
		plans.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product*.	**O.Config-Control** **O.Config-Process**	O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	**O.Reception-Control** **O.Config-Items** **O.Config-Control** **O.Config-Process**	O.Reception-Control supports the identification of configuration items at SIGURD. O.Config-Items ensures the unique identification of each product produces at SIGURD by the client part ID. O.Config-Control ensures a release for each new or changed client part ID. O.Config-Process ensures the automated control of released products
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	**O.Reception-Control** **O.Config-Control** **O.Config-Process** **O.Zero-Balance** **O.Internal-Transport**	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced. This is supported by O.Zero-Balance ensuring the tracing of all security products. O.Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence.
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	**O.Config-Control** **O.Config-Process**	O.Config-Control comprises a release procedure as evidence. O.Config-Process ensures the compliance of the process.
ALC_CMS.5.1C The configuration list includes	**O.Config-Items** **O.Config-Control**	Since the process is subject of the evaluation no products are part of the configuration list.

SARs	Objectives	Rationale
the following: *clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle; development and production tools*; security flaws; and development tools and related information. The CM documentation shall include a CM plan.	**O.Config-Process**	O.Config-Items ensures unique part IDs including a list of all items and processes for this part. O.Config-Control describes the release process for each client part ID. O.Config-Process defined the configuration control including part IDs procedures and processes.
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.	**O.Config-Items** **O.Config-Control** **O.Config-Process** **O.Reception-Control** **O.Internal-Transport**	Items, products and processes are uniquely identified by the data base system according to O.Config-Items. Within the production process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process. The identification of received products is defined by O.Reception-Control. The labelling and preparation for the transport is defined by O.Internal-Transport.
ALC_CMS.5.3C *For each configuration item*, the configuration list shall indicate the developer/*subcontractor* of the item.	**O.Config-Items**	SIGURD does not involve subcontractors for the assembly of security products. According to O.Config-Item all configuration items for secure products are identified.
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	**O.Physical-Access** **O.Security-Control** **O.Alarm-Response** **O.Logical-Access** **O.Logical-Operation** **O.Staff-Engagement**	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. The logical protection of data and the configuration management is provided by

SARs	Objectives	Rationale
integrity of the TOE design and implementation in its development environment.	**O.Maintain-Security** **O.Control-Scrap**	O.Logical-Access and O.Logical-Operation. The personnel security measures are provided by O.Staff-Engagement. Any scrap that may support an attacker is controlled according to 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. Application Note: According to [5] "Guidance for Site Certification, Version 1.1, section 3.3" and usage of CC version 3.1 this content element is obsolete now.	**N/A**	N/A
ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *product*. Application Note: For formal reasons [4] has been used and that according to [5] "Guidance for Site Certification, Version 1.1, section 3.3" this content clement is moved to ALC_DVS.2.2C from CC 3.1	**O.Internal-Monitor** **O.Logical-Operation** **O.Maintain-Security** **O.Zero-Balance** **O.Acceptance-Test** **O.Reception-Control** **O.Internal-Transport** **O.Data-Transfer**	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.Logical-Operation and O.Maintain-Security. All devices including functional and non-functional are traced according to O.Zero-Balance. O.Acceptance-Test supports the integrity control by functional testing of the finished products. The reception and incoming inspection supports the detection of attacks during the transport of the security products to SIGURD

SARs	Objectives	Rationale
		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. Sensitive data received by SIGURD as well as sensitive data sent by SIGURD is encrypted according O.Data-Transfer to ensure access by authorised recipients only.
ALC_LCD.1.1C The lifecycle Definition documentation shall describe the model used to develop and maintain the TOE.	**O.Config-Control** **O.Config-Process**	The processes used for identification and manufacturing are covered by O.Config-Control and O.Config-Process.
ALC_LCD.1.2C The lifecycle model shall provide for the necessary control over the development and maintenance of the TOE.	**O.Acceptance-Test** **O.Config-Process** **O.Zero-Balance**	The site does not perform development tasks. The applied production process is controlled according to O.Config-Process, the finished client parts are tested according O.Acceptance-Test and all security products are traced according O.Zero-Balance.

Since this SST Lite references the PP [6] & [7], 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] & [7] is considered to be applicable for this site.

The performed production steps do not involve source code, design tools, compilers or other tools used to build the security product (intended TOE). Therefore the site does not use or maintain tools according to the definition of ALC_TAT.3. However the component included here to support the reuse of the evaluation results and to enable the justification of the evaluators regarding ALC_TAT.3.

The site always returns the security products back to the client that provided the security products for the assembly. SIGURD is always involved as subcontractor. There is no delivery of security products directly to the client regarding the next life cycle step. Therefore the transport of security products is always considered as internal transport.

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 wafer & IC testing services for smartcards and similar devices. 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 wafer test samples, packaged ICs and Smart Cards are fully operational. The recipient provides appropriate information for the internal shipment of wafers with ICs, semi-finished products containing these ICs, and finished products (i.e. Smart Cards) data as well as for the transfer of related data and documents.

The site will generate keys for different customers, and provide the specified key to customer for encryption of transferred security data.

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. As client's request, the site provides the secure space & independent network for clients to setup the consigned servers and testers. The client setup the servers through lease line which is separated from SIGURD's network. The SIGURD's operator just follows the client's instruction to operate the testers for testing process. Based on the provided specifications also the tests are configured. The test environment allows functional tests to verify the operation after completion of the assembly.

The release process for the optional pre-personalisation process comprises a verification of the initialised products by the client. The protection is based on the classification agreed with the client or printed on the received item or document. This comprises also the pre-personalisation data that is maintained as configuration item related to a product.

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 client need to specify whether the scrap need to be destroyed by the site or need to be sent back to the client.

The secure process data transfer for all kind of data are summarised in the confidential document named “Preconditions for SIGURD Services”, version 1.0, 2016/mm/dd. This document shall be handed to the client for following.

7.2 Services of the Site

SIGURD provides the services which covers parts of the life-cycle (as defined in [6] & [7]) phase 4 related to the wafer & IC testing of wafer with security ICs. In detail, the following services and related management procedures are provided:

- Testing of wafer or dice,

- Testing of security ICs,
- the related control of the test flow process,
- the storage and configuration management of untested and tested wafers,
- receiving of client data as well as packing and preparation for internal shipment,
- the handling of wafer map files, binary files, engineering data,
- controlled destruction of scrap/rejected wafers, and dice on request by the client,
- the operation of the required IT equipment,
- 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 wafers and dice with security ICs and processed dice. The site does conduct wafer test also considering pre-personalisation & IC Testing.

If the chips need to be classified by secure codes, then the secure codes will be controlled as a parameter of the test programs. The secure code control method is for the pre-personalisation process. The pre-personalisation of the products assembled at the premises is an optional service of the site. These data are for instance used for traceability and to secure shipment between phases of production. Assigned secure code will be written into chips during probing.

The complete product specific flow includes a functional test of each products as part of the acceptance process. The client handle the whole testing setup procedure. As client’s request, SIGURD only provide the space & network for clients to setup the consigned servers and testers. The client setup the servers through lease line which is separated from SIGURD’s network. The SIGURD’s operator just follows the client’s instruction to operate the testers for testing process. The testers will access the consigned servers to retrieve test programs through independent network. The operation environment of tester is also under client’s control.

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 provides secure destruction operations according to the request of client, or returns the scrap configuration items to client. At testing, any bad die on wafer will be marked using a digital wafer map file. Defective or rejected products are either returned to the client or they are destructed according to the defined secure destruction process. The client must decide during the product setup whether the rejects and defect devices on the wafer or ICs are also returned or if they shall be destructed by the site according to the secure destruction procedure. The site ships the wafers or dice or 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 wafers or dice or ICs.

7.3 Objectives Rationale

Table 7.1 provides an overview for the correspondence between Security objectives of the TOE / environment listed in chapter 4.1 and 4.2 to the threats and policies identified in chapter 3.2 and 3.3, and demonstrating that all threats and OSP are mapped to at least one security objective. The following chapters provide a more detailed explanation of this mapping.

Table 7.1 – Mappings between the security objectives, and threats / OSP

Security Objectives Threats / OSPs	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Internal-Transport	O.Data-Transfer	O.Control-Scrap
T.Smart-Theft	V	V	V	V	V												
T.Rugged-Theft	V	V	V	V	V												
T.Computer-Net				V	V	V	V					V					
T.Accident-Change						V	V	V	V	V	V	V	V				
T.Unauthorised-Staff	V	V	V	V	V	V	V		V			V	V				V
T.Staff-Collusion				V	V							V	V			V	V
T.Attack-Transport															V	V	
P.Config-Items								V						V			
P.Config-Control						V		V	V								
P.Config-Process										V							
P.Reception-Control														V			
P.Accept-Product									V	V	V						
P.Zero-Balance				V								V	V				V
P.Transport-Prep										V					V	V	
P.Data-Transfer																V	
P.Secure-Scrap																	V

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 SIGURD's employee monitor the alarm system 24/7. The alarm system is connected to secure control room 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 resistance match to provide an effective alarm response.

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.Computer-Net, 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, O.Security-Control and O.Logical-Access 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.Computer-Net, T.Unauthorised-Staff and T.Staff-Collusion

O.Logical-Access

The internal network is separated from the internet with a firewall. The internal network is further separated into subnetworks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is logging into the system with his personalized user name and password.

The threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff as well as the organisational security policies P.Config-Control are addressed by the separation of network segments. The network segments are build and configured to prevent the misuse. Users have their own account with dedicated password and the account is limited to the access rights required by the job task and their responsibility following a strict “need to know principle”.

O.Logical-Operation

All logical protection measures are maintained and updated as required, at least once a month. Critical items such as virus scanners are updated daily. The backup is sufficiently protected and is only accessible for the administration.

This addresses the threats T.Computer-Net, T.Accident-Change and T.Unauthorised-Staff.

O.Config-Items

All product configuration information is stored in the database system. The information stored is covering used materials, process specifications, acceptance test instructions and specifications, test programs and packing instructions. Products are identified by unique ID number with is linked to the unique ID numbers of the associated configuration items.

This is addressing the threat T.Accident-Change and the OSP P.Config-Items, P.Config-Control

O.Config-Control

Procedures arrange for a formal release of specifications and test programs based on an engineering run. The information is also stored in the configuration database. Engineering Change

Procedures are in place to classify and introduce changes. These procedures also define the separation between minor (internal) and major changes and the relevant interactions and releases with clients if required. The ERP requires personalized access controlled by passwords. Each user has access rights limited to the needs of his function. Thereby only authorized changes are possible.

Supported by O.Config-Items this addresses the threats T.Accident-Change and T.Unauthorised-Staff as well as the OSP P.Config-Control, P.Accept-Product.

O.Config-Process

The released configuration information including production and acceptance specifications is automatically copied to every work order. The test program is automatically loaded to the test machine according to the configuration information of the work order.

This addresses the threat T.Accident-Change and the OSP P.Config-Process, P.Accept-Product and P.Transport-Prep.

O.Acceptance-Test

Acceptance tests are introduced and released based on the client approval. The tools, specifications and procedures for these tests are controlled by the means of O.config-Items and O.Config-Control. Acceptance test results are logged and linked to a work order in the manufacture system.

This addresses the threat T.Accident-Change and the OSP P.Accept-Product.

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 objectives O.Physical-Access, O.Logical-Access and O.Config-Items support the engagement of the staff.

This addresses the threats T.Computer-Net, T.Accident-Change, 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 functional and non-functional dice on a wafer 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, O.Config-Items and O.Staff-Engagement.

This addresses the threats T.Accident-Change, 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 and supported by O.Config-Items. 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.Config-Items and 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 and O.Config-Items.

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

O.Data-Transfer

Sensitive electronic information is stored and transferred encrypted using Public Key Infrastructure procedures.

Supported by O.Logical-Acces and O.Staff-engagement this addresses the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Transport-Prep and P.Data-Transfer.

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 either returned to the client using the same packing requirements as for functional products or it is destructed in a controlled and documented way. 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-Balance.

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 [2]. 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] & [7]. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled.

7.4.1 ALC_CMC.5

Content and presentation elements:

ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.

ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.

ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.

ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.

ALC_CMC.5.9C The CM system shall support the audit of all changes to the *CM items* by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the *product* is generated.

ALC_CMC.5.12C The CM documentation shall include a CM plan.

ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product*

ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.

ALC_CMC.5.15C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.

ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

The chosen assurance level ALC_CMC.5 of the assurance family "CM capabilities" is suitable to support the production of high volumes due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialised production process. The requirement for authorized changes support the integrity and confidentiality required for the products. Therefore these security assurance requirements meet the requirements for the configuration management.

7.4.2 ALC_CMS.5

Content and presentation elements:

ALC_CMS.5.1C The configuration list includes the following: *clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle; development and production tools*; security flaw; and development tools and related information. The CM documentation shall include a CM plan.

ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.5.3C *For each configuration item*, the configuration list shall indicate the developer*/subcontractor* of the item.

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures.

Since the site certification process focuses on the processes based on the absence of a concrete TOE these security assurance requirements are considered to be suitable.

7.4.3 ALC_DVS.2

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.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Application Note: According to [5] "Guidance for Site Certification, Version 1.1, section 3.3" and usage of CC version 3.1 this content element is obsolete now.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the *product*.

Application Note: For formal reasons [4] has been used and that according to [5] "Guidance for Site Certification, Version 1.1, section 3.3" this content clement is moved to ALC_DVS.2.2C from CC 3.1

The chosen assurance level ALC_DVS.2 of the assurance family "Development security" is required since a high attack potential is assumed for potential attackers. The configuration items and information handled at the site during production, assembly and testing of the product can be used by potential attackers for the development of attacks. Therefore the handling and storage of these items must be sufficiently protected. Further on the Protection Profile [6] & [7] requires this protection for sites involved in the life-cycle of security ICs development and production.

7.4.4 ALC_LCD.1

Content and presentation elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of security ICs the focus is limited to this site. However the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

7.4.5 ALC_DEL.1

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

The assurance family "Delivery" is not applicable because the products are returned to the client and this is considered as internal delivery.

7.4.6 ALC_TAT.3

Content and presentation elements:

ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.

ALC_TAT.3.2C The documentation of the development tool shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.3.3C The documentation of the development tool shall unambiguously define the meaning of all implementation-dependent options.

The assurance family "Tools and techniques" is not applicable because the tools used for the production process do not influence the behavior of the product. Therefore they are not considered under ALC_TAT.

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. Thereby 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. Thereby the Security Assurance Requirements are suitable to meet the objective.

O.Internal-Monitor

ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product. Thereby the Security Assurance Requirements are suitable to meet the 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. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product. Thereby the Security Assurance Requirements are suitable to meet the objective.

O.Logical-Access

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. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_CMC.5.7C requires that the CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the TOE is generated. Thereby the Security Assurance Requirements are suitable to meet the objective.

O.Logical-Operation

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. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product. Thereby the Security Assurance Requirements are suitable to meet the objective.

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. Thereby the Security Assurance Requirements are suitable to meet the objective.

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C.

ALC_CMC.5.3C requires that an adequate and appropriate review of changes to all configuration items. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items.

ALC_CMC.5.8C requires that the CM system shall clearly identify the configuration items that comprise the TSF.

ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the TOE. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. The CM documentation shall include a CM plan.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

ALC_CMS.5.3C requires that the developer of each TSF relevant configuration item is indicated in the configuration list. Thereby the Security Assurance Requirements are suitable to meet the objective.

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items.

ALC_CMC.5.8C requires that the CM system shall clearly identify the configuration items that comprise the TSF.

ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.10C requires that the CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C requires a CM documentation that includes a CM plan.

ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE.

ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requests evidence demonstrating that all configuration items have been and are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. In addition ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.

Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Config-Process

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. The provision of automated measures such that only authorised changes is made to the configuration items as required by ALC_CMC.5.5C.

ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.8C requires that the CM system shall clearly identify the configuration items that comprise the TSF.

ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

ALC_CMC.5.10C requires that the CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

ALC_CMC.5.13C requires that the CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requests evidence showing that all configuration items have been and are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. The CM documentation shall include a CM plan.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.

ALC_LCD.1.2C requires control over the development and maintenance of the TOE. The objective meets the set of Security Assurance Requirements.

Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.5.6C. ALC_CMC.5.9C requires that the CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. In addition ALC_LCD.1.2C requires control over the development and maintenance of the TOE. ALC_DVS.2.3C requires security measures to protect the confidentiality and integrity of the product during production. Thereby the combination of these Security Assurance Requirements is suitable to meet the 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. Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Zero-Balance

ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means.

ALC_CMC.5.15C requires evidence demonstrating that all configuration items have been and are being maintained under the CM system.

ALC_DVS.2.3C requires security measures that are necessary to protect the confidentiality and integrity of the product.

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_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items.

ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system.

ALC_CMC.5.7C requires that the CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

ALC_CMC.5.11C requires that the CM system shall be able to identify the version of the implementation representation from which the TOE is generated.

ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE.

ALC_CMC.5.15C requests evidence to demonstrate that all configuration items have been and are being maintained under the CM system.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

ALC_DVS.2.3C requires security measures to protect the confidentiality and integrity of the product during the transfer between sites.

Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Internal-Transport

ALC_DVS.2.3C requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product. This includes also the protection during the transport between production sides.

ALC_CMC.5.15C requests evidence to demonstrate that all configuration items have been and are being maintained under the CM system.

ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMS.5.2C according the unique identification of the packing as configuration item.

Thereby the combination of these Security Assurance Requirements is suitable to meet the objective.

O.Data-Transfer

ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product. This includes also the protection during the transport between production sides. Thereby 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. Thereby 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 of the evaluation documentation is as following:

Table 7.2 – Mapping of the Evaluation Documentation

ALC Family	SPEC. No.	Title	Version	Date
ALC_DVS	PCCH-0000-0001	Site Certification Evaluation-Development Security	03	2017-06-01
ALC_CMC &ALC_CMS	PCCH-0000-0002	Site Certification Evaluation-CM Capabilities and Scope	04	2017-06-20
ALC_LCD	PCCH-0000-0003	Site Certification Evaluation-Life-cycle Definition	01	2017-01-11

8. Reference

8.1 Literature

The following documentation was used to prepare this SST Lite:

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012

[3] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 4, September 2012

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

[5] Guidance for Site Certification, Version 1.1, 2013-12-04

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

[7] Security IC Platform Protection Profile, Version 1.0, BSI-PP-0035, June 15th, 2007

[8] Preconditions for Sigurd, version 1.0, 2016-mm-dd

8.2 Definitions

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

Consumer The term “consumer” is used in this SST Lite 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 Lite:

Table 8.1 – Abbreviations table

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
IC	Integrated Circuit
IT	Information Technology
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SIGURD	Sigurd Microelectronics Corp.
SST Lite	Site Security Target Lite
TOE	Target of Evaluation