
MICROCHIP

Public Site Security Target

MICROCHIP PHILIPPINES

102 Accuracy Drive corner Excellence Avenue
Carmelray Industrial Park I, Canlubang Calamba
City, Laguna 4028, Philippines.

Table des matières

Tables index

1. SST Introduction

1 The purpose of this document is to describe the security target for the Test of secure wafers and Integrated circuits at MICROCHIP PHILIPPINES site.

1.1. SST reference

Title	MICROCHIP PHILIPPINES Public Site Security Target
Document ID	MPHIL-PSST-2021.1
Version / date	1.0; April 4th, 2022
Company	MICROCHIP
Site Location	102 Accuracy Drive corner Excellence Avenue Carmelray Industrial Park I, Canlubang Calamba City, Laguna 4028, Philippines
Assurance level	EAL6 (ALC class only)
Evaluation Lab.	SERMA Safety and Security – ITSEF
Certification Body	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Table 1: SST references

1.2. Identification of the Site

2 The SST is referring to MICROCHIP PHILIPPINES site, located in Philippines, Laguna, that provided the Test of secure wafers and Integrated circuits and warehousing services. This SST is specific for site abbreviated as 'MPHIL' which is located at:

3 102 Accuracy Drive corner Excellence Avenue Carmelray Industrial Park I, Canlubang Calamba City, Laguna 4028, Philippines.

4 Main activity at this site is manufacturing of Non-secured[1] and Secured products consist of Wafer Probe, Backgrinding, Strip Test, Singulate Final Test, Tape and Reel, and Warehouse.

[1]The Non-secured product manufacturing is outside the scope of evaluation.

1.3. Site Description

5 This chapter defines the type of activities performed by MICROCHIP PHILIPPINES and targeted to be in the scope of a Site Certification as defined in CCDB-2007-11-001 - Supporting Document, Site Certification [4].

6 MICROCHIP PHILIPPINES is in charge of **Assembly and Test** manufacturing operations. The processes are the following:

Incoming raw Materials (ICs, Wafers and other materials*):*

- Secured and Non-secured materials will be received in boxes at receiving area, the site will key the incoming material into the system. Incoming deliveries of wafers and ICs are received at inbound area while other materials are received at loading dock which entries are accessed only by authorized persons. Upon receipt of wafers and ICs, the parts are checked against the delivery documents then transact in MES (Manufacturing Execution System). The wafers and finished assembly products have a unique identification code for traceability of each material. The wafer and ICs need to test are transferred to Incoming Quality Area.

Wafer Cage and Subcon Store (Pre-test WIP):

- Wafers and ICs that completed Incoming Inspection will be transferred the lot into the Wafer Cage or Subcon Store and will transact the lot into the MES (Manufacturing Executing System). Lots will be transferred to production once received request schedule. Traveler if applicable will be generated and attached prior transferring lot to production.

Die Bank*:*

- Wafers completed probing from production will be transferred to Diebank. The wafers are packed in lot box accompanied by tally sheet. Wafers received in Diebank will check the physical wafers against the log sheet monitoring and do the system transaction in MES. The wafers are transferred from lot box to a wafer jar sealed and will be stage while waiting for shipment request from the Subcon Planner.

Wafer Probe:

- Once lot is received from Die Bank wafer cage, the wafer probe operator will scan the barcode in the process traveler lot label. The barcode contains the lot ID which links to the MES for system check of the lot information. System will download the correct test program. The secure device test program resides in the production program server in the isolated network. The sever containing the serialization of the device is controlled by “MPHIL”.

Final Test:

- The key set for unit serialization is transferred to the server. During testing process the test operator scan the barcode in the process traveler, the system will provide the test program revision to use. This information is automatically sent to the tester and the test program will be retrieved from the isolated controlled server.

Destruction of secured scrap materials:

- The finished goods, rejected material and bad dies in the wafers are all tracked using the Zero Balancing from start of production to the end of the production and are also recorded electronically in the manufacturing production system. Product that are in customer site and need to be scrapped the MICROCHIP Customer Support or Sales shall be informed and will issue a Return Material Authorization (RMA) to the customer to have the product returned to MICROCHIP.
- Product or material that need to be disposed, the site will segregate the scrap product into proper containers and destruct according to relevant scrap procedure.

Outbound (Finish products shipment and Delivery):

- Picklist is generated thru the Baan System. Picklist printed will show the “Ship To”, Ship From location, label requirements and the shipping terms, ESD / PDD dates and some other requirements of the sales order. Warehouse personnel will physically pick the lots and do the picked-packed in Baan system and as well as the physical. Shipment date will depend on the ESD/PDD (earliest ship date /Plan delivery date) or the console day of the customer. Import and Export (Impex) team will call the forwarder or the nominated forwarder for pick-up. The goods will be loaded in the forwarders truck and once loaded, the security guard, the forwarder will sign on the manifest stating the date and time the cargo was picked-up. The truck will be padlocked.

7 These processes, limited to Secure products, are all part of the evaluation scope.

8 Measures are in place for security objectives:

- Access controls are implemented throughout MPHIL facility to prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets.
- Alarm systems and video surveillance cameras are utilized to monitor premises and prevent unauthorized access.
- The factory is surrounded with a fence and gate. The main entrance of the factory installed a car barrier for vehicle. Security person, turnstiles and CCTV are installed to scan people before entering in the building. The security control room for surveillance monitoring. Access controls, restricted access and CCTV surveillance cameras are also located at various location within MPHIL facility.
- Security guards are stationed at employee entrance, loading bay, shipping areas. Security checks/patrols are also conducted within day/night. The guards operated by 24 hours and 7 days a week.
- There are Four levels of security zone in the premises: level 1- Low Security Zone, level 2 – Medium Security Zone, level 3 – High Security zone and Level 4 – restricted Zone. Each area will be assigned to the security level according to:
  - Level 1 - Low Security Zone; No sensitive assets available (general employee's areas),
  - Level 2 - Medium Security Zone; Sensitive assets cannot be directly or entirely access (sensitive assets are in locked/secure cage/cabinet/room),
  - Level 3 - High Security Zone; Sensitive assets can be directly accessed but they are under authorized person control or two-factor authentication.
  - Level 4 – Restricted Zone, Sensitive assets are in unmanned secure room.

9 The site allows supporting the Test of TOEs targeting an Evaluation Assurance Level up to: EAL6.

1.3.1 Physical scope of the site

10 The MPHIL site is composed of 2 buildings, namely: 1 and 2 buildings and are situated in 21063 square meters Lot. The total floor area of building 1 is 21344 square meters while building 2 is 21376 square meters. The total area occupied by

manufacturing and warehouse were around 13581 square meters. The Warehouse, Scan, Reliability Laboratory and Wafer Probe operation, Lobby 1 reception and Admin Office are located at the building 1. Employee entrance, Singulated Final Test, Strip Test, Back grind, Wafer probing expansion, Engineering office and FA lab are located at Building 2.

11 The whole site is subject to the site certification objective.

1.3.2 Logical scope of the site

12 The sensitive assets manipulated are the wafers and the finish products after assembly.

13 The activities part of the evaluation are:

- Incoming Materials,
- Wafer Cage and Subcon Store,
- Die Bank,
- Wafer Probe,
- Final Test,
- Strip Test,
- Tape & Reel,
- Destruction of secured scrap materials,
- Outbound (Finish products shipment and delivery).

14 They are detailed at section 9 -Site Description.

15 The TOE life cycle is part of the global product life cycle that goes from product development to its usage by the final user.

16 The product life cycle phases are those detailed in PP0084 [6] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software, OS and potentially Application Layer) and IC development;
- Phases 3 and 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalization steps may occur in Phase 3;
- Phase 5 concerns the product finishing (eg: within a Smartcard, Inlay, eCover…) called “Composite Integration”;
- Phase 6 is dedicated to the product personalization prior final use;
- Phase 7 is the product operational phase.

17 The manufacturing of MICROCHIP PHILIPPINES is only involved in Phase 4.

Conformance Claims

18 This SST is conformant with the Common Criteria for Information Technology Security Evaluation Version 3.1 revision 5:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001 Version 3.1 Revision 5 [1],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003 Version 3.1 Revision 5 [2].

19 For the evaluation, the following methodology will be used:

- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003 Version 3.1 Revision 5 [2].
- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017 [3],
- Supporting Document Guidance Site Certification, Version 1.0, Revision 1, CCDB-2007- 11-001, October 2007 [4],
- Minimum Site Security Requirement Version 3.0, February 2020 [5].

20 This SST is Common Criteria Part 3 [2] conformant.

21 There are no extended components required for this SST.

22 The Assurance Components which are in the scope of this site certification are:

- **ALC_CMC.5**: Advanced support,
- **ALC_CMS.5**: Development tools CM coverage,
- **ALC_DVS.2**: Sufficiency of security measures,
- **ALC_LCD.1**: Developer defined life-cycle model,
- **ALC_DEL.1** : Delivery procedures.

23 The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) (Ref: BSI-PP-0084) [6]. Therefore the scope of the evaluation is suitable to support product evaluations up to assurance EAL6 conformant to Part 3 of the Common Criteria.

24 Assurance components evaluated are based on the assurance level EAL6 of the Assurance class “Life- Cycle Support”. Assessment of the site security measures demonstrates resistance to penetration of attackers, with a high attack potential. This site supports product evaluations up to EAL6.

25 Note:

- ALC_DEL is a part of this certification for MICROCHIP PHILIPPINES because shipment process is done to customer.
- The MICROCHIP PHILIPPINES site does not provide services such as TOE design or development, but only Testing. Thence ALC_TAT class is not in the evaluation scope.

Security Problem Definition

26 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.

27 This SST is based on the life-cycle defined in the Security IC Platform Protection Profile (Ref: BSI-PP-0084) [6]. The Assets (Section **17**), Threats (Section 19) and Organizational Security Policies (OSP) (Section **22**) defined in this SST are derived from the life-cycle defined in that PP.

28 The Security Problem Definition comprises two major security problems. The first set of security problems comprises all kind of attacks regarding theft (e.g. samples) or disclosure (e.g. design data) or manipulation of assets. These security problems are described in terms of threats. The second set of security problems comprises the requirements for the configuration management (e.g. controlled modification) and the control of security measures. These security problems are described in terms of Organizational Security Policies (OSP).

29 The configuration management covers the integrity and confidentiality of the TOE and the security management of the site.

1.4. Assets

30 The following section describes the assets handled at the site regarding the product manufacturing process.

31 The site has internal documentation and processes relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security policies and measures which aims to protect the assets for the maintenance of appropriate controls

32 The integrity of any machine or tool used for development, production, testing and personalization is not considered as an asset. However, appropriate measures must be defined for the site to ensure the integrity. These items normally consist of standard hardware and software which are programmed or customize.

33 The assets handled by the site are:

Designation	Description
Secure wafers	The wafers received from the wafer fab and subject to Test process. Wafers have to be handle by the site for Integrity and Confidentiality objective.
Secure module/IC	The finish products after Test operations have to be handle by the site for Integrity and Confidentiality objective.
Scrap material	The rejected sensitive material (wafer, IC, document, data) issued from manufacturing operation. Temporary storage and destruction is under the responsibility of the site. It has to be securely managed for confidentiality objective.
Classified documentation	Any documents received or issued by the site which contains restricted and/or classified information. These documents have to be handle by the site for Confidentiality objective.
Test specification	The test specification document received or issued by the site necessary for processing the Test operation. Test specification has to be handle by the site for Integrity and Confidentiality objective.
Test program data	The test program, in its logical form, received or issued by the site, is used for verification of the functionality of the manufactured product (Test operation). This test program shall be maintained (and transfer when necessary) in a secure manner for maintaining its Integrity and Confidentiality.
Personalization data	The personalization data, received or issued by the site, is used for initialization of the manufactured product (Personalization operation). These personalization data shall be maintained (and transfer when necessary) in a secure manner for maintaining their Integrity and Confidentiality.

Table 2: Assets

1.5. Threats

34 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.

35 All threats are applicable to the whole site, and need to counter them sufficiently.

36 The Identified Threats related to the site are:

Designation	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. Concerned assets include good wafers and ICs, reject Wafers and ICs from manufacturing process intended for scrap and destruction, and special transport protection like security seals that support the security of the external shipment to client. This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It covers 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 attended that such an attacker can be defeated by state of the art physical, technical, and procedural security measures like access control and surveillance. The technical measures 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. Concerned assets include good wafers and ICs, reject Wafers and ICs from manufacturing process intended for scrap and destruction, and special transport protection like security seals that support the security of the external shipment to client. This attack is applicable for the location. 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 expertise & standard equipment, could remotely access sensitive network segments to get company proprietary data such as test results or other sensitive production data. They could also modify the testing or production process at the site. A logical attack against the network requires that the attacker first compromise an IT Asset via a phishing or malware attack on an end user. The target of such an attack is to gain access the company's assets and ultimately access to the network to harvest information that could be used to compromise a product or manipulating a product or retrieving information to allow or change the configuration or the personalization. Such attackers are considered to have high risk potential because attacks of this nature happen on a regular basis. Furthermore, the attacker may have the substantial nation state resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company. These attacks are mitigated via the regular monitoring of host assets using Carbon Black and the requirement for end users to take annual security training as well as we conduct regular phishing exercises.
T.Accident-Change	Employee, trainee, or contractor could have made exchange the products of different production lots or different clients during execution of their tasks at production and shipment collection by accident. Concerned assets include Wafers and Singulated ICs. Employee, trainee, or contractor 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 production or test area.
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. The concerned assets include wafers for probing and ICs for testing. 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. 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 defective 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. Only authorized personnel are allowed into the secure area incase there is a need to access need to request the department in-charge. Subcontractors, visitors, or non-employee of the site will be subjected to record their particulars and will be escorted by an employee during the duration of their stay and have restricted access to the site. The site has a guideline for the access of unauthorized employees when entering the site.
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. Concerned assets include good wafers and ICs, reject Wafers and ICs from manufacturing process intended for scrap and destruction, and special transport protection like security seals that support the security of the external shipment to client. While the site conducts security training and security talks for the employees, they have to also sign the confidentiality agreement during their term of employment with the site.

	Procedures are established about the limitation of access, and document control access on production and sensitive data.
T.Attack-Transport	An attacker might try to get data, specifications or products during the internal shipment and/or the external delivery. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment and/or the external delivery process to allow a modification, cloning or the retrieval of confidential information after further production steps. Confidential information comprises design data, customer and/or consumer data like code and data (including personalization data and/or keys) stored in the ROM and/or EEPROM or classified product documentation. Concerned assets include good wafers and ICs, reject Wafers and ICs from manufacturing process intended for scrap and destruction, and special transport protection like security seals that support the security of the external shipment to client. The protection of the internal shipment and/or the external delivery is based on the configuration items that are provided by MPHIL site. MICROCHIP assumes that the configuration items are protected according to assumption A.Product-Integrity

Table 3: Threats

1.6. Organisational Security Policies

37 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).

38 The documentation of the site under evaluation must be under configuration management. This comprises all procedures regarding the evaluated production flow and the security measures that are in the scope of the evaluation

Designation	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 may rely completely on the naming and identification of the received configuration items. In this case at least the consistency with the expected values must be verified and the unique identification must be ensured. This holds also for test programs or 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. For data like configuration, initialization or personalization data the identification and handling must be described. For configuration items that are created, generated or developed at the site the naming and identification is specified.
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 authorised personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for setup 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 or externally delivered, (iv) classification of the items (which are security relevant), (v) who (either Name of the site 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 external delivery and/or 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 development and production of the product, the management of flaws and optimisations of the process flow as wel as the documentation that describes the services and/or processes provided by a site. The documentation describing the processes and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is ensured. Tools and databases are used to support the production process of the site. This comprises e.g. lot traveler, Reporter 8 and MES database system. The configuration control also comprises data and parameters for testing and quality parameters.
P.Reception-Control	The inspection of incoming items done at the site ensures that the 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.
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 or externally delivered.
P.Zero-Balance	The site ensures that all sensitive items (security relevant parts of the TOEs of different clients) are separated and traced on a device basis. For each hand over, either an automated or an organizational "two-employees-acknowledgement" (four-eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are either destroyed at the site or sent back to the client or customer and/or consume (depending on the production-setup). A destruction process is mandatory and will be agreed between the client and the site that is responsible for the destruction of defect devices. All processes contributing to the destruction and/or Return Material Authorization (RMA) procedures are under internal quality management control.
P.Organise-Product	The configuration, pre-personalisation, initialization or personalization process is applied as specified by the client. If the data includes sensitive items like keys relevant for the life-cycle or configuration data that affect the security of the TOE appropriate measures must be in place. This includes the requirement that the knowledge of sensitive keys shall be split to at least two different persons. Furthermore, technical measures like crypto-boxes, separation of network, split access permission and secure storage shall be implemented for this kind of data. This policy is adapted to cover all kinds of data handled by the site in an appropriate way.
P.Product-Transport	Technical and organizational measures ensure the correct labeling of the product. A controlled internal shipment and/or the external delivery is applied. The transport supports traceability up to the acceptor. This policy can include measures for packing if required by the client to protect the product during transport. Controls are in place when the forwarder indicated by the client before the handover of the security products. Traceability of the outgoing materials and security products are monitored. Information of freight forwarders are also recorded to ensure traceability and accountability. All outgoing and internal shipments have a dedicated outgoing shipment channel for the transfers of goods (including configuration products) to ensure security.
P.Data-Transfer	Confidential/sensitive data transfers in electronic form must be sent in a signed, encrypted and secured manner. All sensitive configuration or information (include product specifications, test programs, test program specifications etc.) is also encrypted to ensure security before sending out to clients through email
P.Secure-Scrap	Storage of the functional or defective Scrap materials are securely maintained with authorized access. Secured scrap products must be destroyed securely with registered vendors or are returned to the clients (according to the production setup).

Table 4: Organizational Security Policies

1.7. Assumptions

Designation	Description
A.Product-Specification	The product developer must provide appropriate specifications and guidance for the testing of the product. This comprises plans for an appropriate test requirements and parameters for the development of the functional and electrical test program appropriate for the final testing. The provided information includes the classification of the delivered item and data.
A.Item-Identification	Each configuration item received by the site (like specifications, definitions, process limits, process parameters, test requirements, test limits or guidance, scripts) is appropriately labeled to ensure the identification of the configuration item.
A.External-Delivery	The recipient (customer) of the product is identified by the address provided by the client. The address of the consumer is part of the product setup in the Baan system.
A.Internal-Shipment	The recipient (client) of the product is identified by the address of the client site. The address of the client is part of the product setup in the Baan system.
A.Init-Data	The scripts (test program or personalization data) for the configuration and initialization process are provided by the client of the product. The client verifies the configuration and/or initialization process during the product introduction and the release process of the site.
A.Product-Integrity	The self-protecting features of the products are fully operational and it is not possible to influence the configuration and behavior of the products based on insufficient operating conditions or command sequences generated by an attacker or by accident
A.Destruct-Scrap	Scrap configuration items are destructed at site so that they are useless for an attacker.

Table 5: Assumptions

Security Objectives

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

Designation	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the "need to know" principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces four levels (level 1 to level 4) of access control to sensitive areas of the site. The access control measures ensure that only registered employees and vendors can access restricted areas. Sensitive products are handled in restricted areas only. Access is granted by authentication thru access badge, biometrics, and passwords.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.
O.Alarm-Response	The technical and organisational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorised 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 every year. 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. Processes may be controlled within a shorter time frame to ensure a sufficient protection.
O.Maintain-Security	Technical security measures are maintained regularly to ensure correct operation. The logging of sensitive systems is checked regularly. This comprises the access control system to ensure that only authorised employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the networks and computer systems.
O.Logical-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 authorised 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. Every user of an IT system has its own user account and password. All computer systems with access to sensitive data require successful authentication either by user name and password or identification token (e.g. company badge) and password.

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.
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 authorised 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 development and production of the product, 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.Accept-Product	The site delivers configuration items that fulfill the specified properties. Specification checks, machine parameters checks, functional and/or 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.Organize-Product	For the configuration, pre-personalization, initialization or personalization process it is ensured that the specified process is applied. The data integrity is controlled. Keys and other sensitive data can only be constructed by at least two employees. The operation is applied in crypto-boxes or similar devices. After the release process changes are only applied based on the request of the client. The update is done according to a controlled process.
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 nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Zero-Balance	The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgment during hand over is applied for functional and defective devices. According to the agreed production flow the defect devices are either destroyed at the site or sent to the client or the consumer.
O.Reception-Control	Upon reception of product 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-Shipment	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.External-Delivery	The recipient of a physical configuration item is identified by the assigned consumer address. The external delivery procedure is applied to the sensitive configuration item. A delivery address is assigned to each product and subject of a controlled process. The packaging is also part of the defined process and applied as specified by the client. The forwarder supports the tracing of sensitive configuration items during external delivery. For every 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 authorised 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.

Table 6 – Security Objectives Description

Security Objectives Rationale

40 The SST 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 includes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives.

41 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 items. Therefore, they do not contribute to the security of the site under evaluation.

Threat / OSP	Security Objective	Justification
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat. **O.Physical-Access** ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. **O.Security-Control** ensures that an attacker will be detected when trying to reach the assets through a Secure Room **O.Alarm-Response** supports **O.Physical_Access** and **O.Security_Control** by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. **O.Internal-Monitor** and **O.Maintain-Security** ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Smart_Theft.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat **O.Physical-Access** ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. **O.Security-Control** ensures that an attacker will be detected when trying to reach the assets through a Secure Room **O.Alarm-Response** supports **O.Physical_Access** and **O.Security_Control** by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. **O.Internal-Monitor** and **O.Maintain-Security** ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Rugged_Theft.
T.Computer-Net	O.Internal-Monitor	The technical and organizational measures prevent unauthorized access to the internal network. The development network is not

	O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	connected to anything that an attacker could use to set up a remote connection. **O.Logical-Access** ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. **O.Logical-Operation** ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection). **O.Staff-Engagement** ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). **O.Internal-Monitor** and **O.Maintain-Security** ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Computer-Net.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Process O.Accept_Product O.Staff-Engagement O.Zero-Balance	The automated measures and the control and verification procedures avoid accidental changes of sensitive items. **O.Logical-Access** ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. **O.Logical-Operation** ensures that computer systems (as MES) used to manage the manufacturing processes are kept up to date and under controlled access. **O.Config-Items** ensures that all configuration items for secure products are identified. **O.Config-Process** ensures that configuration management is used and applied for sites services control. **O.Accept-Product** to ensure that the products to be returned to the clients are compliant with their specifications. **O.Staff-Engagement** ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). **O.Zero-Balance** ensures that all items are traced and accounted for. Together, these objectives will therefore counter T. Accident-Change
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	Physical and logical access control limits the access to sensitive product or data to authorized persons. In addition, organizational measures prevent uncontrolled access to products or product related items (including secure scrap). **O.Physical-Access** ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. **O.Security-Control** ensures that an attacker will be detected when trying to reach the assets through a Secure Room **O.Alarm-Response** supports **O.Physical-Access** and **O.Security-Control** by ensuring that a response will be given to the alarm

	O.Zero-Balance O.Control-Scrap	systems and that this response is quick enough to prevent access to the assets. **O.Logical-Access** ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. **O.Staff-Engagement** ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). **O.Zero-Balance** ensures that all items are traced and accounted for. **O.Control-Scrap** ensures that scrap material cannot be accessed by an authorized party. **O.Logical-Operation** ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection). **O.Internal-Monitor** and **O.Maintain-Security** ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Unauthorised Staff
T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O. Data-Transfer O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to assets. **O.Staff-Engagement** ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). **O.Zero-Balance** ensures that all items are traced and accounted for. **O.Data-Transfer**-ensures the integrity of the secure delivery of data. **O.Control-Scrap** ensures that scrap material cannot be accessed by an authorized party. **O.Internal-Monitor** and **O.Maintain-Security** ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Staff Collusion
T.Attack-Transport	O.Internal-Shipment O.External-Delivery O.Data-Transfer	The applied security measures on sensitive data during internal shipment and external delivery prevent modification or disclosure of any sensitive items during transport. The applied security measures on physical items during internal shipment and external delivery allow detection of attempted attacks. **O.Internal-Shipment** ensures the traceability and security of products during shipment. **O.External-Delivery** ensures the traceability and security of products during delivery to customer.

		O. Data-Transfer ensures the integrity of the secure delivery of data. Together, these objectives will therefore counter T. Attack-Transport.
P.Config-Items	O.Reception-Control O.Config-Items	The Security Objective directly enforces the OSP O.Config-Item. **O.Reception-Control** ensure an immediate identification of the product upon reception and confirm the received quantity **O.Config-Item** ensures that all configuration items for secure products are identified. Together, these objectives will therefore counter P. Config-Items
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	Network and Logical protection (O. Logical – Access) and the usage of configuration management tools by authorized people ensure the OSP. **O.Config-Items** ensures that all configuration items for secure products are identified. **O.Config_Control** ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. **O.Logical-Access** ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. Together, these objectives will therefore counter P. Config-Control.
P.Config-Process	O.Config-Process	The Security Objective directly enforces the OSP
P.Reception-Control	O.Reception-Control	The Security Objective directly enforces the OSP
P.Accept-Product	O.Config-Control O.Config-Process O.Accept-Product	Application of a configuration management plan and change management monitored by authorized people ensure that the intended TOE is conformant to the accepted on by the customer. **O.Config_Control** ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. **O.Config-Process** ensures that configuration management is used and applied for sites services control. **O.Accept-Product** to ensure that the products to be returned to the clients are compliant with their specifications. Together, these objectives will therefore counter P. Accept-Product.
P.Zero-Balance	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance O.Control-Scrap	All assets are traced internally until their possible destruction (O. Zero-Balance, O. Control-Scrap) by trained and authorized people (O. Staff-Engagement) to enforce the OSP **O.Staff-Engagement** ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). **O.Zero-Balance** ensures that all items are traced and accounted for.

		O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party. **O.Internal-Monitor** ensures that the above is managed and maintained. Together, these objectives will therefore counter P. Zero-Balance
P.Organise-Product	O.Logical-Operation O.Logical-Access O.Config-Control O.Config-Process O.Organise-Product	**O.Logical-Operation** ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus and spyware protection). **O.Logical-Access** ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. **O.Config_Control** ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. **O.Config-Process** ensures that configuration management is used and applied for sites services control. **O.Organise-Product** ensures the correctness of test and/or personalisation data in accordance with client specification. Together, these objectives will therefore counter P. Organise-Product.
P.Product-Transport	O.Config-Process O.Internal-Shipment O.External-Delivery O.Data-Transfer	Appropriate procedures for internal and external shipment ensure correct labelling and traceability until the recipient. **O.Config-Process** ensures that configuration management is used and applied for sites services control. **O.Internal-Shipment** ensures the traceability and security of products during shipment. **O.External-Delivery** ensures the traceability and security of products during delivery to customer. **O.Data-Transfer** ensures the integrity of the secure delivery of data. Together, these objectives will therefore counter P. Product-Transport.
P.Data-Transfer	O. Data-Transfer	The Security Objective directly enforces the OSP.
P.Secure-Scrap	O. Security-Control O. Control-Scrap O. Zero-Balance	Appropriate procedures for zero balance to ensure that no secure product is lost or theft. **O.Security-Control** ensures that an attacker will be detected when trying to reach the assets through a Secure Room **O.Control-Scrap** ensures that scrap material cannot be accessed by an authorized party. **O.Zero-Balance** ensures that all items are traced and accounted

		for. Together, these objectives will therefore counter P. Secure Scrap.

Table 7: Mapping of Security Objectives

Extended Assurance Components Definition

42 There are no extended components required for this SST.

Security Assurance Requirements

43 The security assurance requirements for this Site Security Target shall support an evaluation according to the assurance level EAL6.

44 Therefore, this security assurance requirement is applied in this Site Security Target instead of ALC_DVS.1, ALC_CMC.4, ALC_CMS.4 as defined for the package EAL4 as requested by (PP-0084, [6]), because ALC_DVS.2 and ALC_CMC.5 are the hierarchically higher components. This Site Security Target is then suitable for EAL4 and EAL6 evaluations.

45 The Security Assurance Requirements (SAR) are from the class ALC (Life cycle support):

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

46 Since the site MPHIL does not provide services that are covered by ALC_TAT.3, the component ALC_TAT.3 is not applicable for this site.

47 Because hierarchically higher components are used in this SST, the Security Assurance Requirements listed above fulfill the requirements of:

- [4] ‘Common Criteria Supporting Document Guidance Site Certification’
- [6] ‘Security IC Platform Protection Profile - Eurosmart’
- [5] ‘Minimum Site Security Requirements’

1.8. Application Notes and Refinements

48 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, the associated processes for the handling of products are in the focus and described in this SST. These processes are subject of the evaluation of the site.

1.8.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

49 Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.1 ‘Application Notes for ALC_CMC’.
- Refinements of the TOE Assurance Requirements’ in [6] §6.2.1.4 ‘Refinements regarding (ALC_CMC)’.

50 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/ICs) 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.

51 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.

52 The configuration control and a defined change process for the procedures and descriptions of the site under evaluation is 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.

53 The life cycle described includes complex production processes that cannot be controlled at each state within the production process. In such a case the control of the product after 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 are under configuration management for these cases.

54 The configuration items for the considered product type are listed at section 17. 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.

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

1.8.2 Overview and Refinements regarding CM Scope (ALC_CMS)

56 Refer to subsections:

- 'Application Notes for Site Certification' in [4] §5.2 'Application Notes for ALC_CMS'.
- 'Refinements of the TOE Assurance Requirements' in [6] §6.2.1.3 'Refinements regarding (ALC_CMS)'.

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

58 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 at section 17 that are considered as "TOE implementation representation", includes:

- Secure wafers,
- Secure module/IC,
- Scrap material,
- Classified documentation,
- Test specification,
- Test program data,
- Personalization data.

59 Final physical design data in addition process control data, test data and related procedures and programs can be in the scope of the configuration management.

1.8.3 Overview and Refinements regarding Delivery (ALC_DEL)

60 Refer to subsections:

- 'Application Notes for Site Certification' in [4] §5.3 'Application Notes for ALC_DEL'.
- 'Refinements of the TOE Assurance Requirements' in [4] §6.2.1.1 'Refinements regarding (ALC_DEL)'.

61 The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE for parts of it (ii) to the consumer or consumer's site (Composite TOE Manufacturer), The CC assurance components 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 initialization Data and/ or Configuration Data may include supplements of the Security IC Embedded Software.

62 In the particular case of a security IC more “material and information” then the TOE itself (which by definition includes the necessary guidance) is exchanged with clients. Since the TOE can be externally delivered after different life cycle phases, 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.

63 Since the assurance component ALC_DEL.1 is applicable to the external delivery to the consumer, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS, external delivery is covered by the component ALC_DEL.1.

1.8.4 Overview and Refinements regarding Development Security (ALC_DVS)

64 Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.4 ‘Application Notes for ALC_DVS’.
- ‘Refinements of the TOE Assurance Requirements’ in [4] §6.2.1.2 ‘Refinements regarding (ALC_DVS)’.

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

66 The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorized persons only, and scrap must be destroyed.

67 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.

1.8.5 Overview and Refinements regarding Development Security (ALC_LCD)

68 Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.6 ‘Application Notes for ALC_LCD’.

69 The site does 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 Protection Profile (BSI-PP-0084) [6] provides a life-cycle description there specify life-cycle steps can be assigned to the tasks at site. This may comprise a change of life-cycle state if e.g. initialization is performed at the site or not.

70 The Protection Profile (BSI-PP-0084) 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 returned to the clients. The defective devices are scrapped at MPHIL site.

1.8.6 Overview and Refinements regarding Development Security (ALC_TAT)

71 Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.7 ‘Application Notes for ALC_TAT’.

72 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”, requires evidence for the suitability of the tools and technique used for the development process of the TOE.

73 Neither source code of the intended TOE is handled nor is any task performed at the site that must be considered accordingly to ALC_TAT.

1.9. Security Assurance Rationale

74 The Security Assurance Rationale maps the content elements of the selected assurance components of [2] to the Security Objectives defined in this SST. The refinements described above are considered.

1.9.1 Security Requirements Rationale – Dependencies

75 The dependencies for the assurance requirements are as follows:

- ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- ALC_CMS.5: None
- ALC_DVS.2: None
- ALC_DEL.1: None

76 One of the dependencies is not (completely) fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [4] at §5.1 'Application Notes for ALC_CMC'.

1.9.2 Security Requirements Rationale – Mapping

SARs	Security Objective	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	Wafers are labeled by a unique part ID. Automatic tools are used to set-up the wafers in a new production item. The products get a unique client part ID automatically generated by the system tools based as defined by **O. Config-Items.**
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Config-Items O.Config-Control O.Config-Process	Incoming inspection according to **O.Reception-Control** ensures product identification and the associated labeling. This labeling is mapped to the internal identification as defined by **O.Config-Items**. This ensures the unique identification of security products. **O.Config-Control** ensures that each client part ID is setup and released 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	O.Config-items O.Config-control	**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.

SARs	Security Objective	Rationale
and appropriate review of changes to all configuration 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 labeling 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.5.5C: 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.Organize-Product	**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** support the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. **O.Organize-Product** ensures that the specified process is applied and is under control of dedicated authorized staff.
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config-Process O.Config-Control O.Zero-Balance O.Accept-Product O.Organize-Product	**O.Config-Process** comprises the automated management of the production processes. **O.Config-Control** assigns the setup including processes and items for the production of each client part ID. **O.Zero-Balance** ensures the accountability of all security products during production. **O.Accept-Product** provides an automated mechanical testing of the product quality and supports the tracing. **O.Organize-Product** ensures that the specified process is applied and is under control of dedicated authorized staff.
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.Logical-Operation	**O.Reception-Control** different roles are assigned to difference teams. The members of each team are response to released differences step of the production and final good (Secure rejects) are differences. **O.Logical-Access** and **O.Logical-Operation** support the control by limiting the access and ensuring the correct operation for all tasks to authorised staffs difference access assignment.
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. 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	O.Config-Items O.Accept-Product O.Config-Control	**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

SARs	Security Objective	Rationale
product by automated means, including the originator, date and time in the audit trail.	O.Config-Process	IDs at the site the production control comprises steps and there by includes the required audit trail including the originator. According to **O.Config-Process** the CM plans describe the services provided by the site. **O.Accept-Product** provides an automated mechanical testing 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. **O.Config-Process** also ensures that only controlled changes are applied.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the delivered configurations item.	O.Reception-Control O.Logical-Access O.Config-Control O.Config-Process O.Logical-Operation	**O.Reception-Control** comprises the incoming labelling and the mapping to internal identifications. **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. **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	**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.5.13C: The CM plan shall describe how the CM system is used for the development of the TOE.	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. **O.Config-Items** ensure the unique identification of each product produces 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	O.Reception-Control	The objectives: **O.Reception-Control**, **O.Config-Control**, **O. Config-Process** ensure that only released client part IDs are

SARs	Security Objective	Rationale
demonstrate that all configuration items are being maintained under the CM system.	O.Config-Control O.Config-Process O.Zero-Balance O.Internal-Shipment O.External - Delivery	produced. This is supported by **O.Zero-Balance** ensuring the tracing of all security products. **O.Internal-Shipment** and **O.External-Delivery** include the packing requirements, the reports, logs and notifications including the required evidence.
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config-Control O.Config-Process	**O.Config-Control** comprises a release procedure as evidence. **O.Config-Process** ensures the compliance of the process.

Table 8: Security Assurance Rationale for ALC_CMC.5

SARs	Security Objective	Rationale
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information. The CM documentation shall include a CM plan	O.Config-Items O.Config-Control O.Config-Process	Since the process is subject of the evaluation no products are part of the configuration list. **O.Config-Items** ensure 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 ID's 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-Shipment O.External-Delivery	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-Shipment** and **O.External-Delivery.**

SARs	Security Objective	Rationale
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	MPHIL does not involve subcontractors for the production of IC product. According to **O.Config-Items** all configuration items for secure products are identified.

Table 9: Security Assurance Rationale for ALC_CMS.5

SARs	Security Objective	Rationale
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.	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Data-Transfer O.Control-Scrap O.Organize-Product	The physical protection is provided by: **O.Physical-Access**, supported by **O. Security-Control**, **O.Alarm-Response.** The associated control and continuous justification is subject of the objectives **O.Logical-Operation** and **O.Maintain-Security**. The logical protection of data and the configuration management is provided by **O.Logical-Access** and **O.Logical-Operation**. The personnel security measures are provided by **O.Staff-Engagement**. Sensitive data received and send by the site is encrypted according to **O.Data-Transfer** to ensure access by authorized recipients only. Any scrap that may support an attacker is controlled according to **O.Control-Scrap**. **O.Organize-Product** ensures that the specified process is applied and is under control of dedicated authorized staff.
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.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance O.Accept-Product O.Data-Transfer O.Internal-Shipment	The associated control and continuous justification is subject of the objectives **O.Internal-Monitor**, **O.Logical-Operation** and **O.Maintain-Security**. All devices including functional and non -functional are traced according to **O.Zero-Balance**. **O.Accept-Product** supports the integrity control by mechanical testing of the finished products. Sensitive data received and send by the site is encrypted according to **O.Data-Transfer** to ensure access by authorized

		recipients only. The delivery to the client Is protected by similar measures according to the requirements of the client based on **O.Internal-Shipment.**
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 TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance O.Accept-Product O.Data-Transfer O.Internal-Shipment	The associated control and continuous justification is subject of the objectives **O.Internal-Monitor**, **O.Logical- Operation** and **O.Maintain-Security**. All devices including functional and non -functional are traced according to **O.Zero-Balance**. **O.Accept-Product** supports the integrity control by mechanical testing of the finished products. Sensitive data received and send by the site is encrypted according to **O.Data-Transfer** to ensure access by authorized recipients only. The delivery to the client Is protected by similar measures according to the requirements of the client based on **O. internal-Shipment.**

Table 10: Security Assurance Rationale for ALC_DVS.2

SARs	Security Objective	Rationale
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. Accept-Product 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.Accept-Product.** All security products are traced according **O.Zero-Balance**.

Table 11 Security Assurance Rationale for ALC_LCD.1

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

78 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.

SARs	Security Objective	Rationale
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.	O.External-Delivery	The applied delivery process is controlled according to **O.External-Delivery .**

Table 12 Security Assurance Rationale for ALC_DEL.1

Site Summary Specifications

79 The Site Summary Specification describes how the site meets the SARs.

1.10. Preconditions Required by the Site

80 MPHIL provides Test services for Wafers and ICs. Wafers and assembled ICs. are expected as input for the Test process. Defective dies in wafer are marked by inking or by electronic wafer map files. Defective ICs are identified throughout the process. The packaging and the wafers must be labelled to allow for production product identification.

81 The production is released after the client accepts the initial samples lot produced. Therefore, each client is responsible for the verification of his products based on the samples lot provided by the site.

82 The devices delivered to the site are tested based on the test parameters provided by MICROCHIP Business Units.

83 Security related products such as packaged Security ICs come with clearly defined and fitting interfaces for the production at MPHIL, these products are uniquely identifiable.

84 The information required for the testing of the ICs such as specification, testing guidance, and production requirements shall be provided by MICROCHIP Business Units.

85 Transport process, including the shipping address and the packing requirements for the shipment, needs to be specified by MICROCHIP or the client. This also includes the procedure for selecting the forwarder.

1.11. Services of the Site

86 Each product setup at the site gets a unique client part ID (Client consigned parts). This part ID is linked with the secure device that is tested in the site.

87 The processes for Testing and product acceptance are setup at the site according to the specifications (e.g. Testing specification and packaging requirements, if applicable) provided by the client. For the release, a samples lot is produced at the site.

88 The site has a standard procedure for packing of finished products and preparation of shipment. If special packaging requirements are requested by the client, they are included in the process setup. The client is alerted if products are ready for transport because the transport will be arranged by the customer. Base on the alert, the client provides the pickup information on the forwarder that is used for the verification of the forwarder before the handover of the products.

89 Defective or rejected products are destructed according to the defined secure destruction process.

90 The MPHIL, Manufacturing services can be detailed as follow:

- Incoming Materials,
- Wafer Cage and Subcon Store,
- Die Bank,
- Wafer Probe,
- Final Test,
- Strip Test,
- Tape & Reel,
- Destruction of secured scrap materials,
- Outbound (Finish products shipment and delivery).

91 They are detailed at section 9 - Site Description.

1.12. Rationale

92 The objectives rationale is provided at Security Objectives Rationale section. The following rationale gives more justification on how all threats and organizational security policies are effectively addressed by the security objectives.

1.12.1 Objectives mapping

93 The tables below demonstrate that all threats and OSP are mapped to at least one security objective.

	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
T.Smart-Theft	X	X	X	X	X				
T.Rugged-Theft	X	X	X	X	X				
T.Computer-Net				X	X	X	X		
T.Accident-Change						X	X	X	
T.Unauthorized-Staff	X	X	X	X	X	X	X		
T.Staff-Collusion				X	X				
T.Attack-Transport									
P.Config-Items								X	
P.Config-Control						X		X	X
P.Config-Process									
P.Reception-Control									
P.Accept-Product									X
P.Zero-Balance				X					
P.Organize-Product						X	X		X
P.Product-Transport									
P.Data-Transfer									
P.Secure-Scrap		X							

Table 13 - Objectives mapping

	O.Config-Process	O.Accept-Product	O.Organize-Product	O.Staff-Engagement	O.Zero-Balance	O.Reception-Control	O.Internal-Shipment	O.External-Delivery	O.Data-Transfer	O.Control-Scrap
T.Smart-Theft										
T.Rugged-Theft										
T.Computer-Net				X						
T.Accident-Change	X	X		X	X					
T.Unauthorized-Staff				X	X					X
T.Staff-Collusion				X	X				X	X
T.Attack-Transport							X	X	X	
P.Config-Items						X				
P.Config-Control										
P.Config-Process	X									
P.Reception-Control						X				
P.Accept-Product	X	X								
P.Zero-Balance				X	X					X
P.Organize-Product	X		X							
P.Product-Transport	X									
P.Data-Transfer									X	
P.Secure-Scrap					X					X

Table 13 - Objectives mapping (continued)

1.12.2 Objectives Rationale

94 The following rationale provides a justification that shows that all threats and OSP are effectively address by the security objectives.

O.Physical- Access

95 The plant is surrounded by a fence and controlled by CCTV. The access to the site is only possible via access controlled doors. The enabling of the alarm system and the additional external controls are managed according to the running operation at the site. This considers the manpower per shift as well as the operational needs regarding the receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into four security levels. The access control ensures that only registered and authorized persons can access sensitive areas.

96 This is supported by O. Security- Control that includes the maintenance of the

access control and the control of visitors. The physical security measured is supported by O. Alarm-Response providing an alarm system.

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

O.Security-Control

98 During working and off hours the security officer will monitor the site and surveillance system. The CCTV systems support these measures because it is always enabled.

99 Further on the security control is supported by O. Physical Access requiring different level of access control for the access to security product during operation as well as during off hours.

100 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 and the OSP P. Secure Scrap is addressed.

O.Alarm-Response

101 During working hours the security officer will monitor the alarm system. The alarm system is connected to a control center that is running 24 hours. O. Physical-Access requires certain time to overcome the different level of access control. The response time of the security officer and security response team (who is on duty) are needed to provide an effective alarm response

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

O.Internal-Monitor

103 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 success control. Major changes of security systems and security procedures are reviewed in general management security review meetings (min. 1 per year). Upon introduction of a new process, a formal review and release for mass production is made before being generally introduced.

104 This addresses T. Smart-Theft, T.Rugged-Theft, T. Computer-Net, T.Unauthorised-staff, T.staff-Collusion and OSP. P. Zero Balance.

O.Maintain Security

105 The security relevant systems enforcing or supporting O. Physical-Access, O. security-Control and O. Logical Access are checked regularly by the security officer. In case of maintenance, it is done by the suppliers. In addition, the configuration is updated as required by authorized security officer (for the access control system). Log files are also checked for technical problems and specific maintenance requests.

106 This addresses T. Smart-Theft, T.Rugged-Theft, T. Computer-Net, T.Unauthorised-staff and T.staff-Collusion

O.Logical-Access

107 The internal network is separated from the internet with a firewall. The internal network is further separated into sub networks by internal firewalls. These firewalls allow only authorized information exchange between the internal sub networks. Each user is logging into the system with his personalized user ID and password. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events.

108 The individual accounts are addressing T. Computer-Net.

109 All configurations are stored in the database of the ERP system. Supported by O. Config-Items.

110 This addresses the threats T. Accident-Change and T. Unauthorized –Staff and the OSP P. Config-Control and P.Organise-Product.

O.Logical-Operation

111 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.

112 This addresses the threats T. Computer-Net, T.Accident-Change, T. Unauthorized-Staff, and the OSP P.Organize-Product.

O.Config-Items

113 The configuration management system is in place and assigns a unique internal identification to each product to uniquely identify configuration items and is assigned to each different client. Items, products and processes are uniquely identified by the database/ERP system

114 This addresses the threat T.Accident-Change and the OSP P. Config-Items and P. Config-Control.

O.Config-Control

115 Procedures arrange for a formal release of specifications and test programs based in 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 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

116 This addresses the OSP P. Config-Control, P.Accept-Product and P.Organize-Product.

O.Config-Process

117 The release configuration information including production and acceptance specifications is automatically copied to every work order. The test program is automatically loading to the test machine accordingly to the configuration information of the work order.

118 This addresses the threat T.Accident-Change and the OSP P. Config-process, P. Accept Product, P.Organize-Product and P. Product--Transport.

O.Accept-Product

119 Product acceptance is introduced and released based on the client approval. The tools, specifications and procedures for product compliance and/or tests specification are controlled by the means of O. Config items and O. Config-Control. Acceptance results are logged and linked to a work order in the ERP system.

120 This addresses the Threat T.Accidental-Change and the OSP P. Accept-Product.

O.Organise-Product

121 When receiving test script, pre-personalisation or initialisation data, team in charge of these activities are trained to decipher the received package, to verify the origin of these data, to transfer data to test's server and to verify the integrity of received package.

122 This security objective is supported by O.Config-Items, O.Config-Control and O.Accept-Product.

123 This addresses the OSP P.Organise_Product.

O. Staff-Engagement

124 All employees are interviewed before hiring. They must sign and NDA and the staff compliance agreement on Security matters before they start to work in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products.

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

126 This addresses the threats T. Computer-Net, T.Accident-Change, T. Unauthorized-Staff, T. Staff-Collusion and the OSP P. Zero Balance.

O. Zero Balance

127 Products are uniquely identified throughout the whole process. The amount of functional and non-functional dies on a wafer and for a production order is known. Scrap and rejects are following the good products thru the whole production process. At every process step the registration of good and rejected products is recorded and updated via the ERP system.

128 This security objective is supported by O. Physical-Access, O. Config-Items and O.Staff-Engagement.

129 This addresses the threats T. Accident-change, T. Unauthorized-Staff, T.Staff-Collusion, OSP P. Zero-Balance and P. Secure Scrap.

O.Reception-Control

130 At reception, each configuration item including security products are identified by the shipping documents, packaging label and information in the ERP system based on shipments alerts from the client and supported by O. Config-Items. If a product cannot be identified, it is put on hold in a storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seal of these boxes if applicable.

131 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-Shipment

132 The recipient of a production lot is linked to the work order in the ERP 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.

133 This addresses the Threat T.Attack-Transport and the OSP P. Product-Transport.

O.External-Delivery

134 The recipient of a production lot is linked to the work order in the ERP system whose customer address is specified by the client. Packing procedures are documented in the product configuration, based on the client and/or customer requirements. This security objective is supported by O. Staff Engagement and O. Config-Items.

135 This addresses the Threat T.Attack-Transport and the OSP P. Product-Transport.

O.Data-transfer

136 Sensitive electronic information is stored and transferred encrypted using PGP procedures. Supported by O. Logical Access and O. Staff-engagement

137 This addresses the threats T. Staff Collusion and T. Attack-Transport as well as the OSP P. Product-Transport and P. Data-transfer.

O.Control-Scrap

138 Scrap is identified and handled in the same way as functional devices. They are stored internally in a secured location. The scrap is destructed form 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.

139 Supported by O. Physical-Access and O. Staff-engagement,

140 This addresses the threats T. Unauthorized-Staff and T-Staff-Collusion, the OSP P. Zero balance and P. Secure Scrap.

1.13. Security Assurance Requirements Rationale

141 The Security Assurance rationale is provided at section 41 - Security Assurance Rationale. The following rationale gives more justification for the selected Security Assurance Requirements.

- ALC_CMC.5: Advanced support,
- ALC_CMS.5: Development tools CM coverage,
- ALC_DVS.2: Sufficiency of security measures,
- ALC_LCD.1: Developer defined life-cycle model,
- ALC_DEL.1: Delivery procedures.

ALC_CMC.5

142 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 industrialized production process. The requirement for authorized changes and ability to identify the changes and version of the implementation will support the integrity and confidentiality required for the products. Responsibility of different departmental teams is also clearely identified for accepting or authorizing any change on the configuration items. Therefore these assurance requirements stated will meet the requirements for the configuration management.

ALC_CMS.5

143 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.

ALC_DVS.2

144 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 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 requires this protection for sites involved in the life-cycle of Security ICs development and production.

ALC_LCD.1

145 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.

ALC_DEL.1

146 The chosen assurance level ALC_DEL.1 of the assurance family “Delivery” is applicable because the finish products can be delivered to the customer.

1.14. Assurance Measure Rationale

O.Physical-Access

147 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. Thereby this objective contributes to meet the Security Assurance Requirement.

148 Thereby this objective contributes to meet the security Assurance Requirement.

O.Security-Control

149 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 this objective contributes to meet the Security Assurance Requirement.

150 Thereby this objective contributes to meet the security Assurance Requirement.

O.Alarm-Response

151 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 this objective contributes to meet the Security Assurance Requirement.

152 Thereby this objective contributes to meet the security Assurance Requirement.

O.Internal-Monitor

153 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. Thereby this objective contributes to meet the security Assurance Requirement. ALC_DVS.2.3C: 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.

154 Thereby this objective contributes to meet the security Assurance Requirement.

O.Maintain-Security

155 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 this objective contributes to meet the security Assurance Requirement. 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 and ALC_DVS.2.3C: 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.

156 Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

157 ALC_CMC.5.5C: Requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the security Assurance Requirement. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified.

158 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 this objective contributes to meet the security Assurance Requirement.

159 Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Operation

160 ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified.

161 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 this objective contributes to meet the security Assurance Requirement. 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. ALC_DVS.2.3C: 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.

162 Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Config-Items

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

ALC_CMC.5.3C. 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 identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. 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.

164 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. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration items is indicated in the configuration list.

165 The objective meets the set of Security Assurance Requirements.

O.Config-Control

166 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. A method used to uniquely identify the configuration items is required by ALC_CMC.5.3C. 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 authorized changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. 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 (production) 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 to demonstrate that all configuration items are maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

167 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.

168 In addition ALC_LCD.1.1C requires that the life cycle definition describes the model used to develop and maintain the products.

169 The objective meets the set of Security Assurance Requirements.

O.Config-Process

170 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 authorized changes are 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 identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan 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 to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

171 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.

172 ALC_LCD.1.1C requires that the lifecycle 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.

173 The objective meets the set of Security Assurance Requirements.

O.Accept-Product

174 Product acceptance is introduced and released based on the client approval with the tools, specification and procedure for these tests. They 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 MES.

175 ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means. ALC_CMC.5.9C requires that the CM system supports the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.

176 ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during production. ALC_DVS.2.3C requires that evidence

justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

177 ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

178 Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Organise-Product

179 ALC_CMC.5.5C requires that only authorised changes are made to the configuration items. In addition ALC_CMC.5.6C requires that the CM system shall support the production of the TOE by automated means.

180 In addition ALC_DVS.2.1C requires security measures that are necessary to protect the confidentiality and integrity of the TOE.

181 Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Staff-Engagement

182 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.

183 Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Zero-Balance

184 ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means. ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system.

185 ALC DVS.2.2C and ALC_DVS.2.3C require security measures that are necessary to protect the confidentiality and integrity of the TOE.

186 ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

187 Thereby this objective is suitable to meet the security Assurance Requirement.

O.Reception-Control

188 ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the 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 person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of design data used to generate the test scripts can be identified. ALC_CMC.5.14C requires the the version of test programs and the production processes used for production can be identified. ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system.

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

190 Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Internal-Shipment

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

192 ALC_CMS.5.2C requires that configuration list uniquely identify the configuration items.

193 ALC_DVS.2.2C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE. ALC.DVS.2.3C requires confidentiality and integrity of the product during internal shipment.

194 Thereby this objective contributes to meet the Security Assurance Requirement.

O.External-Delivery

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

196 ALC_CMS.5.2C requires that configuration list uniquely identify the configuration items.

197 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 customer.

198 Thereby this objective is suitable to meet the Security Assurance Requirement.

O.Data-Transfer

199 ALC_DVS.2.1C requires security measures that are necessary to protect the confidentiality and integrity of the TOE

200 ALC_DVS.2.2C: 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.2.3C requires confidentiality and integrity of the product during internal shipment.

201 This objective will meet the Security Assurance Requirement.

O.Control-Scrap

202 ALC_DVS.2.1C requires physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation.

203 Thereby this objective is suitable to meet the Security Assurance Requirement.

Definition, Abbreviations & References

1.15. Definition

Client	The term “client” is used indifferently with “customer”, which identify the entity for which the finish product is delivered.

1.16. List of abbreviations

CC	Common Criteria
CM	Configuration Management system
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
ESD	Earliest Ship Date
IC	Integrated Circuit
IMPEX	Import & Export
IT	Information Technology
MES	Manufacturing Execution System
OSP	Organizational Security Policy
PDD	Plan Delivery Date
PP	Protection Profile
RMA	Return Material Authorization
SAR	Security Assurance Requirements
SST	Site Security Target
TOE	Target Of Evaluation
TSF	TOE Security Function
WIP	Work In Process control system

1.17. References

[1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 CCMB-2017-04-001.
[2]	Common Criteria For information Technology Security Evaluation Part 3: Security Assurance Components April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.
[3]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology April 2017 Version 3.1 Revision 5, CCMB-2017-04-004.
[4]	Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.
[5]	Joint Interpretation Library, Minimum site security requirements, version 3.0, February 2020.
[6]	Security IC Platform Protection Profile with Augmentation Package BSI-CC-PP-0084-2014; Version 1 ; Issued 13-01-2014.

Version History

Version	Author / Date	Approver / Date	Comments
1.0	MICROCHIP / April 4th, 2022	MaJanice BAGSIT	