Table of Contents

1.0 SST Reference

The purpose of this document is to describe the Security Target for the Assembly and Testing of Secure Wafers and ICs located in Singapore for the assembly and testing of Secure Wafers and ICs.

1.1 SST Overview

Title:	Public Site Security Target
Version Number:	6
Date:	15 Aug 2022
Site:	UTAC USG1
Site Location:	5 Serangoon North Avenue 5 Singapore 554916
Product Type:	Security Wafers/ ICs
EAL-Level:	EAL 6 **
Evaluation Body:	SERMA SAFETY & SECURITY
Certification Body: (ANSSI)	Agence National de la Securite des Systemes d'Information

** Note that Only Classes AST and ALC are applicable for Site Certification Objectives in this Security Target.

1.2 References

	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 Criteria Supporting Document Guidance Site Certification October 2007 Version 1.0 Revision 1 CCDB-2007-11-001
4	Joint Interpretation Library Minimum Site Security Requirements Version 3.0 February 2020
5	Bundesamt Für Sicherheit in der Information stechnik Guidance for Site Certification Version 1.0
6	Security IC Platform Protection Profile with Augmentation packages Version 1.0 Ref BSI-PP-0084

2.0 SST Introduction

2.1. Site Identification

The SST is referring to UTAC USG1, which provides assembly and test services for customers Security IC Platform Protection Profile with Augmentation packages Version 1.0 Ref BSI-PP-0084 and located at the following address:

United Test and Assembly Center Pte Ltd
5 Serangoon North Ave 5
Singapore 554916

The site is a 5 storey building, of which the first four levels are solely used for the assembly manufacturing and testing of secured and non-secured ICs. The 5th floor houses the administration offices. The whole facility consists of the production, engineering, research and development, warehousing, business administration and management activities.

Description of the site activities:

Incoming Material (Security IC wafers & other raw materials)

Secure Customers will send to UTAC (USG1) their secure wafers for probing, assembly and final testing. Customers will also provide their build instructions and test programs to the site in order to start the wafer probing, assembly and testing production.

Storage and Warehousing of Secure IC Wafers

Upon physical receipt of the Secure IC wafers (in boxes) at Receiving Area, the site will key in the Incoming material information into the system (SLRS – Stream Line Receiving System). After transaction in SLRS, the boxes are unpacked un-packed and placed inside a secure cabinet. A packing list is attached to each lot. The production material handler will do physical lot verification against the SLRS packing list. If okay, the receiving personnel will acknowledge the shipment in the UMS (UTAC Management System) and issue the GRN (Goods Received Notice). The production material handlers (2 personnel) will then move the received lot to the wafer bank/die bank area using a caged trolley with a combination lock.

Wafer Bank

Upon physical receipt of lot at wafer bank, the wafer bank personnel will transact the lot into the UMS. After which, it is unpacked and transferred to a FOUP and lot is sent for Wafer Incoming Quality Inspection. The Process Traveler is generated and attached to the lot prior to sending lot to Wafer Sort.

Wafer Sort

Once secure lot is received from Wafer Bank, the wafer sort operator will scan the barcode in the process traveler (PT). The barcode contains the lot ID which links to the UMS for system check of the lot information. System will download the correct test program if UMS information matched with the PTRD information and wafer sort production can now start. The secure device test program resides in the production program server in the isolated network. The BB Server containing the serialization of the device is controlled by the customer. UTAC (USG1) only provides the isolated network infrastructure and physical security for production.

Assembly

Before any mass production is conducted in assembly, the site will have already optimized the production process during the NPI (New Product Introduction) stage where the site will review the customer spec requirements, run qualification and pre-production lots. Data on the runs are sent to customer for their review and final

approval for full production. For every mass production launch, each job is assigned a unique production lot ID which will be traced from the start to finish through the UMS. The site also practices Zero Balancing where each die in the wafer or each packaged unit is traced and accounted for through-out the process. An assembly process traveler document is attached to each production lot.

Once production is launched, the wafers will undergo the following manufacturing processes in assembly:

Wafer Taping: This is the process where the active side is protected with a backgrind tape to protect it while the wafer undergoes back-grinding during the next process. Lot In/Out is transacted in the UMS.

Wafer Backgrind: The taped wafers are then back-grinded to the desired thickness as required by the customer in the Assembly Build Instruction. Back-grind process recipe is auto-download by scanning of the barcode in the process traveler. Lot In/Out is transacted in the UMS. Once completed back-grinding process the tape is then removed from the wafer.

Wafer Mount: The back-grinded wafers are then mounted on a wafer ring to prepare it for the laser groove & wafer dicing processes. Lot In/Out is transacted in the UMS.

Laser Groove / Wafer saw: For low K wafers (≤ 65 nano), laser groove is required prior to wafer saw. Wafer saw process will complete the isolation of the different ICs in a wafer. Both laser groove and wafer saw recipe are auto-downloaded through UTAC (USG1) RMS (Recipe Management System). Lot In/Out is transacted in the UMS.

Once the wafers are completely sawn, the lot goes through UV cure, Post saw inspection and Tape and Reel (for wLCSP devices) or through Flip Chip attach (for Flipchip devices). Lot In/out are transacted in the UMS for each process stage.

Tape and Reel: For wLCSP devices, Wafer map diagrams of the wafers are downloaded through the CIM Wafer Map Client System and the electrically good dies are picked and place into reels. Lot In/Out is transacted in the UMS. Once completed Tape & Reel, the secure lot in reels is sent to EOL-Packing area in caged trolleys with combination lock and under "4 eyes" supervision. Wafer skeletons are accounted for, packed and security sealed and sent to the Reject Control Center.

Flip Chip Attach: For Flip Chip devices, Wafer map diagrams of the wafers are downloaded through the CIM Wafer Map Client System and the electrically good dies are picked and place into PCB substrates and sent for reflow and flux clean. Lot In/Out is transacted in the UMS. Wafer skeletons are accounted for, packed and security sealed and sent to the Reject Control Center.

Mold/PM Cure: After flux clean, the flip chip attached substrates are baked in preparation for the molding process. During molding, the flipchip dies are encapsulated with thermo-setting molding compound and cured. Lot In/Out is transacted in the UMS.

Ballmount: After Post mold Cure, the molded substrates are sent for ball mounting where a solder ball alloy is attached on the ball pads of the substrates and reflowed. Lot In/Out is transacted in the UMS.

Saw Singulation: Ball-mounted substrates are mechanically sawn to isolate into individual units. Lot In/Out is transacted in the UMS.

Auto VM: After singulation, the lot is sent for 100% auto visual-mechanical inspection. Visual defect/reject units are separated from the good units. Lot In/Out are transacted in the UMS. The rejected units are placed inside a plastic bag and security sealed before sent to the Reject Control Center. (Note: Rejects are placed inside a caged trolley with combination lock when transporting to the Reject Control Center).

Final Test & Pre-personalization: In order to check if the connectivity of the secure modules are good or not, the modules/units undergo testing process via contact pin (USG1) isolated server. The key set for unit serialization is transferred by customer to their Black box server. During testing process, the test operator scans the barcode in the Process Traveler which links to the PTRD (Program Test Recipe Database). The system will then provide what test program revision to use. This information is automatically sent to the tester which does an auto-matching and retrieves the correct test program from the isolated server. Once test program is loaded into the tester, the system communicates with the BB box server to retrieve the keys for unit serialization.

In the event that UTAC (USG1) Product Engineers find abnormalities in the test program during program check-out, they will abort the check-out and feedback the abnormalities (with data) to the customer. The customers will then review and modify the program and send a new test program revision to UTAC (USG1).

The BB Server containing the serialization of the device is controlled by the customer. UTAC (USG1) only provides the isolated network infrastructure and physical security for production.

Use of SFTP Server and SFTP Client system is for transfer of confidential/sensitive data between UTAC and the Customer securely through data encryption. The SFTP Server is hosted in locked rack at secured UTAC Data Centre (with biometric access control). On request, SFTP user ID and password will be generated and issued to specific customer, to allow a secure access for each individual customer.

Outgoing Visual Inspection: Before the final packaging of the tested lots, the lots undergo visual inspection according to the visual criteria defined by the customer.

Packaging: Depending on the customer's packing requirements, the final packaging of the secure devices is packed in reel format or in trays. These are then packed into boxes with proper box identification labels as required by the customer.

Destruction of secured reject materials:
The good and bad dies in the wafers are all tracked using the Zero Balancing procedure from the start to end of the production of the secure lot and are also recorded electronically in the UMS. For customers who require their scrap dies and wafers to be shipped back to their facility, they will arrange the appropriate transportation for the shipping of the scrap materials to their site. UTAC (USG1) will store the scrap materials in proper containers with the relevant procedure before the scrap materials are collected and transported to customer's site.

Shipment to customers
Shipments are considered "internal shipment" as the packaged materials is routed back to UTAC (USG1) direct customer. Customer provides their own forwarders which UTAC (USG1) security performs the necessary security checks before they are allowed in to collect the materials. The site will inform the customer upon completion of the production order and the completed modules are ready for collection.

2.2 Site Description:

2.2.1 Physical scope

The physical scope of the evaluation process of the site consists of Level 1 (Receiving, shipping, Packing, Assembly-post mold, Security Command Center and Reject Control Center), Level 2 (Production Control Center, Final Test), Level 3 (Assembly-cleanroom, FA Lab, IT room), Level 4 (Diebank/wafer bank, Wafer probe, Reliability Lab).

The entire perimeter of the building premises is surrounded with a fence. The main entrance of the building is secured with a car barrier fitted with curtain for vehicle entry. Employees who are driving, riding or cycling issued with RFID Tag pasted on their ID badge. Flashing the RFID Tag at the transponder will render the barrier open. Pedestrian movement is through a double full height turnstile secure with card access In/Out readers. Audio/Video Intercom System at vehicle entry and double full height turnstile for communication with visitors. Full height fence secure both sides of the turnstile and the vehicle lanes to deter intrusion. CCTV cameras are installed on strategic locations along the perimeter and are house at the Security Command Center for surveillance monitoring. Access controls, restricted access and CCTV surveillance cameras are also located at various locations within UTAC (USG1) facility. CCTV footages in the identified secure areas within UTAC (USG1) facility are housed in the Security Command Center for surveillance. Security guards are stationed at Employee entrance, Loading Bay, Receiving and Shipping areas. Roving security checks are also conducted within working hours.

In general, the relevant physical sections that are target of the evaluation process are the areas that are directly involved in the services and/or processes of the site used for security products as well as areas that support these either from operational point of view (configuration control, operation control, location of IT-system, warehouse, etc.) or from organizational point of view (site security organization and control, maintenance of systems and tool, FA and Rel services, customer services etc.).

2.2.2. Logical scope

The logical boundary covers the following items:

- Receiving and storage of security wafers,
- Production/ manufacturing of the security IC modules,
- Pre-personalization of the security modules which includes the testing and operating system loading of completed modules,
- Logistics – Incoming wafers, outgoing wafers, outgoing finish goods, storage and warehousing,
- Handling of scrap materials from production process to destruction.

3.0 Conformance Claims (AST_CCL)

3.1 Version on Common Criteria

3.1.1 The SST evaluation is based on Common Criteria version 3.1, release 5.
3.1.2 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model version 3.1, revision 5, April 2017 (CCMB-2017-04-001)

3.1.3 Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance Components, April 2017 version 3.1 Rev 5 (CCMB-2017-04-003)

3.2 The methodology used for the evaluation:

3.2.1 Common Methodology for IT Security Evaluation, Evaluation Methodology, April 2017 version 3.1 rev 5 (CCMB-2017-04-004)

3.3 Evaluated Assurance Components are from the assurance level EAL6:

3.3.1	ALC_CMC.5	Production support, acceptance, procedures and automation
3.3.2	ALC_CMS.5	Development tools CM Coverage
3.3.3	ALC_DEL.1	Delivery Procedures
3.3.4	ALC_DVS.2	Sufficiency of Security Measures
3.3.5	ALC_LCD.1	Developer defined life-cycle model
3.3.6	ALC_TAT.3	Compliance with implementation standards, all parts

3.4 The list of Security Assurance Requirements (SAR) to form the scope of evaluation for USG1:

3.4.1	ALC_CMC.5	Production support, acceptance, procedures and automation
3.4.2	ALC_CMS.5	Development tools CM Coverage
3.4.3	ALC_DVS.2	Sufficiency of Security Measures
3.4.4	ALC_LCD.1	Developer defined life-cycle model

Assurance components evaluated are based on assurance level EAL6.

3.5 There is no extended Assurance Component Definition (AST_ECD) in this Site Security Target as USG1 site is solely managed and controlled by UTAC employees. Although there are customer's server residing in secured room or location provide by UTAC to the customer, these servers in the room or at the location are solely managed and under physical and logical controls of the customer.

3.6 USG1 implemented the controls and related security measures as defined in the Joint Interpretation Library Minimum Site Security Requirements Version 3.0 February 2020.

3.7 The Site Security Target is compliance to the Security IC Platform Protection Profile with Augmentation packages Version 1.0 Ref: BSI-PP-0084.

3.8 The Site Security Target is compliance to the Common Criteria For Information Technology Security Evaluation Part 3: Security Assurance Components April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.

4.0 Security Problem Definition (AST_SPD.1)

The security problems are derived from the potential threats based on the assets owned by the site and the Organizational Security Policies (OSP) are also defined in this section. The security problem definition comprises of mainly: Theft - Theft of information, Physical theft of assets AND lapses in Physical/Logical Security – in production process, handling of pre-personalization data. These threats are described generally in the SST to cover the aspect of potential attacks which the site has detail procedures, access matrix, lay-out blueprints that governs the security of the site.

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

4.1 Security Assets

This section describes the assets handled at the site. The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of the intended TOE. This comprises site security policies and measures which aims to protect the assets for the maintenance of appropriate controls.

Assets refer to the security elements which are received / consigned by the customers and owned by the site as follows (but not limited to):

- Customer's secure IC and Wafers
- Customer's finished products
- Customer's Test specs, Test programs and pre-personalization data
- Secure wafer / dies rejects
- Customer owned hardware for secure products
- Security seal
- IT network lay-out
- Physical security lay-out
- RCC Compactor Key (Reject Control Center Compactor Key)

The integrity of any machinery or tooling used for production is not considered as part of the definition of asset. However, the site has maintained procedures, measures and internal documentation to ensure the importance of this condition.

4.2 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the TOE. During the receiving of incoming materials (Secure wafer, ICs), production and test, the intended TOE and the representation of parts of the intended TOE are vulnerable to such attacks. These threats are described generally and are applicable to the site. The explanation below the threats will help to address the Security Objectives according to the site specific aspects:

T.Smart-Theft:
In a situation where the attacker plans to access the authorized area or restricted boundaries for the purpose of stealing secured items from the site. This attacker could use tools or equipment to break into the physical boundary of the company or building. Potential physical theft could also happen during incoming of raw material, during in process of manufacturing production till shipment of the finish goods. Concerned assets include Customer's Secured IC and wafers, Customer's Testing Specifications, test programs and pre-personalization data, Secure IC wafers /dies or tested units which are rejected in the manufacturing process or intended for scrap, special transport protection like security seals that support the security of the internal shipment to the customer.

This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get used or rejected devices that can be used to further investigate the functionality of the device and search for further exploits The time spent by an attacker to prepare the attack and the flexibility of such an attack will provide big risk.

Potential attackers could be either existing employee of the company or external attackers whom are not existing employees. It will cause the company financial loss and loss of reputation as the goods are entrusted to the site by the client.

T.Rugged-Theft:
In a situation where the attacker is experienced, plans to attack by accessing the permissible area or restricted boundaries for sensitive configuration items. Attacker could be paid for such stealing activities. Concerned assets include Customer's Secure IC / wafers, finished products, Testing Specifications, test programs and pre-personalization data, special transport protection like security seal that support the security of the internal shipment to the client.

The risk for this attack could vary depending on the subject and the recognized value of the assets. These attackers could be prepared to take high risks for payment. They are considered to be sufficiently resourced to overcome the security measures. The target of the

attack could be devices that can be re-sold or misused in an application context. This can be devices installed at testing or personalization area for cloning or introduction of forged devices. These attackers are considered to have the highest attack potential.

These attackers could not completely be blocked by the physical, technical and procedural security measures. The site has special restricted location and access to highly secured area where such information are the most sensitive. Signed and Secured Keys are also used to transmit confidential or sensitive files with external parties to provide additional protection against such attacks.

T.Computer-Net:
Data theft could happen when the attacker tried to access the network without authorization. The attacker could try to download or intercept confidential documents of the company/clients' data (such as pre- personalization data) for manipulation. In such cases, data theft through access of the company network or data servers could lead to loss of reputation of the company as well as the leak of confidentiality of customer's knowhow and intellectual property. This could eventually lead to a financial loss, compensation or legal case for the company. Concerned assets include Customer's Testing Specifications, test programs and pre- personalization data.

These attackers are considered to have high attack potential because they might have vast technical knowledge to perform such attack whereby the in house system or software may not have sufficient capabilities to withstand such attacks.

Risk of Logical theft is reduced by the implementation of the security firewall to the external network. Limitations are set on websites, web applications and computer applications which are not essential for company use. Computer users also have individual accounts which require password authentication.

The site also houses dedicated servers and procedures in place handling Pre-personalization data which will enhance the security of the data received from the clients. The production network is also separated from the office network which the production network has no access to the internal network and has no access to internet to reduce the risk of any external attacks from hackers.

Sensitive and confidential information exchanges like the pre-personalization data that client send to the site for testing and OS loading are also encrypted when send to the site for decryption. Access of the encryption and decryption key are limited to only users who require access to clients' exchanges.

Use of SFTP Server and SFTP Client system is for transfer of confidential/sensitive data between UTAC and the Customer securely through data encryption. The SFTP Server is hosted in locked rack at secured UTAC Data Centre (with biometric access control). On request, SFTP user ID and password will be generated and issued to specific customer, to allow a secure access for each individual Customer.

T.Unauthorized Staff:
Unauthorized entry into prohibited area such as store, warehouse, production area and personalization is restricted. Concerned assets include Clients Secured IC and wafers, Client's Secured modules, Clients Testing Specifications, test programs and pre-personalization data, special transport protection like security seals that support the security of the internal shipment to the client. The site is segregated into different levels of restricted access and the access is only permitted to authorized personnel.

Only authorized personnel are allowed into the different sections of the company and are controlled by the card access matrix which is reviewed and approved by Management.

Subcontractors/ vendors, visitors or non-employee of the site will be subjected to record their particulars and escorted by an employee during the duration of their stay in the site and have restricted access to the site. The site has also internal procedure guiding the access of unauthorized employees entering the site.

T.Staff-Collusion:
Threats from external attacker might have collaborated with existing employee to extract data, confidential information or material from the site. Collaboration of such nature could have been motivated by personal interest or extortion. Concerned assets include Customer's Secured IC and wafers, finished products, Testing Specifications, test programs and pre-personalization data, Secure IC wafers or tested products which are rejected in the manufacturing process or intended for scrap.

While the site conducts yearly 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 such as key ceremony when handling clients' pre-personalization data, limited access and document controlled access on production data and clients' sensitive data are also available at site. Handling of material or product at site using the 4 eyes principal is also implemented to reduce the tendency of such attacks.

T.Accidental Change:
Employee, trainee, freight forwarder could have also make mistakes in executing their tasks and therefore resulting in the wrong mix of the different shipment at collection, mixing the wrong lot or batch of raw materials of products in production or even loading wrong personalization data by mistake. Concerned assets include Customer's Secured IC and wafers, Secured modules, Testing Specifications, test programs and pre-personalization data.

Site has measures in place to prevent accidental changes in high risk area prone to accidental change such as incoming shipment identification, outgoing shipment collection, in production process during issuing of materials and also loading of personalization data.

T..Attack-Transport:
Potential attacker might be planning to get products or confidential data during shipment of the product. Their aim on the attack is to get sensitive information for unauthorized activities, such as replicating any sensitive product devices or data, reselling of security devices or getting sensitive information. Concerned assets include Customer's Secured IC and wafers, finished products, Secure ICs / wafers or modules which are rejected in the manufacturing process or intended for scrap, specific assets like security seals, special transport protection or similar items that support the security of the internal shipment to the client. These specific assets are handled the same way as other assets to prevent misuse, disclosure or lost.

Incoming and outgoing shipment of raw material and finished goods/ products to clients are controlled via a restricted channel whereby access is dedicated to only logistics personnel and all transactions of materials are performed between the freight forwarders and logistics personnel are also recorded. Procedure and controls for Freight Forwarders (for incoming and outgoing shipments) are also in place. Collection for the finished goods is also identified with unique numbers whereby it's only made known to the freight forwarder who are collecting the goods.

Internal transportation of TOE is also monitored under the production process security element.

4.3 Organizational Security Policies (OSPs)

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

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the evaluated production flow and the security measures that are in the scope of the evaluation. Guidelines outlining the Security policy of the Site are mapped as follows:

P.Config-Items:

The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of the items that are created, generated, developed or used at the site.

All products and item codes are guided by the site's configuration system which uses unique item code for different client, Bill of material (BOM) and products. The site also uses a Work in Progress (WIP) and Zero balancing system for production and item traceability. Procedure of the customer's creation and new product introduction (NPI) are also in place to ensure that the information of the clients, material configuration and process specifications of the product are defined.

The documentation (Physical copy) of this customer's assembly build diagram and specifications are controlled documents released only for production. Limited access to these documentations (electronic copy) is also stored in the server, available only to authorized engineering personnel. Procedures on the creation of the Bill of Material guiding the unique item code for all raw materials (including security products) and clients codes. The entire production system is also guided by the UMS and SAP system which control information of the entire process from incoming to production and shipment. The naming and the identification of these configured items are specified during the entire production process.

P.Config Control:

The procedures governing setting up the production process for new product and the procedure that allows changes of the initial setup for a new product shall only be perform by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set-up and changes. The procedure for the initial set-up of a test and/or process flow ensures that sufficient information is provided to the client.

The test and/or process flow set-up may include the following information (a) identification of the product, (b) identification of the site, (c) classification of the items (which are security relevant), (d) reject and scrap management, (e) information of shipment address.

All these setup are also managed via the UMS and SAP system and governed by procedure on item master part creation. Configured items will be tied to the customer's approval documents before releasing it for mass production. Program name will be defined based on the clients name and configuration name. There are internal procedures and work instructions to ensure the traceability of clients' inventory and is further governed by the UMS and SAP system.

P.Config-Process:

Services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for assembly and testing of the product like the process control plan will govern how the process is run and what are the tools and assembly equipment used in the production of the module. This clearly explains in detail the manufacturing processes, quality and testing of the modules at the site.

The documentation with the process description and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status complies.

P.Reception Control:

Procedures on receiving of products, outgoing shipments to clients and internal material flow are followed to ensure that security is not compromise. Inspection of incoming materials is also done on site to ensure that the received configuration items comply with the properties stated by the client.

Traceability of the materials and products are monitored via UMS and SAP system. Information of freight forwarders are also recorded to ensure traceability and accountability. All incoming shipments have a dedicated incoming reception channel for the transfers of goods (including security material) to ensure security.

P.Accept-Product:

The testing and quality control of the site ensures that the released products comply with the specification agreed with the clients. The quality control plan depicts the process, control and measures in place for the acceptance process of the configuration items. Therefore, the properties of the product are ensured when shipped.

P.Zero-Balance:

Site ensures that all sensitive items (on the intended TOE from clients) are separated and traced by devices basis. Procedure on Zero balancing is practiced to ensure that all scrap materials are accounted for at each different manufacturing process. Security products are traced and recorded to ensure traceability. At the end of the production process where functional or defective assets are consolidated, they are ether destroyed or send back to the clients (dependent on the production setup).

The policy on Zero balancing covers the handling of products at each production flow of the site. All finished products are returned to the clients that has provided the site with the products. This is considered as internal shipment routing back to the clients.

P.Prod-Transport:

Procedures and measures are ensured for the correct labeling of the product. Products are labeled according to the specification determine by the clients and are verified before shipment to the clients. Products are packed per specification indicated by the customers. 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.

Use of SFTP Server and SFTP Client system is for transfer of confidential/sensitive data between UTAC and the Customer securely through data encryption. The SFTP Server is hosted in locked rack at secured UTAC Data Centre (with biometric access control). On request, SFTP user ID and password will be generated and issued to specific customer, to allow a secure access for each individual Customer.

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).

4.4 Assumptions:

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected in the assumptions defined below for the interface between the client and the site.

A.Item-Identification:

Each Configuration item received by the site is appropriately labeled to ensure the identification of the configuration item.

A.Product-Spec:

The product developer (customer) must provide appropriate specifications and guidance for the assembly and testing of the product. This comprises bond plans for an appropriate assembly process as well as test requirements and test parameters for the development of the functional tests or a finished test program appropriate for the final testing. The provided information includes the classification of the delivered item and data.

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. The client defined the requirements for packing of the security products in case the standard procedure of UTAC (USG1) is not applicable.

A.Testdata-Support:
The client must provide test programs via secure connection to the site in correct data format. The client is responsible for the secure transfer of data into the UTAC (USG1) security network for the secure behavior of the provided programs and for the secure configuration of the equipment that is under client's control.

The assumptions are outside the sphere of influence of UTAC (USG1). They are needed to provide the basis for an appropriate production process, to assign the product and destruction of all configuration items related to the intended TOE.

5 0 Security Objectives (AST_OBJ)

The security objectives are related to physical, technical and organizational security measures, the configuration management as well as the internal shipment and s shall conform to the EAL 6. These measures defined the physical, data, organizational security measures, and logistical security of the site.

O. Physical-Access: Different Security access supports the different level of access control level of different authorized staff entering the facility. The area of access of the authorized staff is subjected to the basis of each individual's job scope and enforcing the "need to know" principle. The access control supports the limitation for the access to sensitive area including the identification and rejection of unauthorized entry. The site enforces up to three levels (level 0 to level 2) of access control depending on the area of access. The access control measures and mapping ensures that only authorized staff and accompanied visitors can access restricted areas. Any visitors who are accompanied must also be authorized to visit the restricted area by a formal security application, approved by authorized personnel. All Security products are handled in restricted areas only.

O. Security-Control: The site has defined the responsibilities of each different personnel responsible for the security of the site. Measures, response and controls on the operation of the system for access control and surveillance are also defined. Technical security equipment such as video control, CCTV, sensors will also support the enforcement of the access control. All staff is responsible for registering the visitors, get authorized approval for entry to each area and should ensure to escort the visitors.

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

O. Internal- Monitor: The site performs security management meeting once every year. The security management meetings are used to review security incidences, to verify that the maintenance measures are applied and to reconsider the assessment of risks and security measures. An internal audit is also conducted yearly to control the application and seek further improvement of the security measures defined.

O. Maintain- Security: Technical security measures are maintained regularly to ensure correct and accurate operations. Access control system to ensure that only authorized employee have access to sensitive area as well as computer/ network system to ensure the protection of the networks and computer systems based on the appropriate configuration.

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. The internal network is also separated into the production network and the administration 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 internal network is also restricted to authorized employees that are working in the related area or that are involved in the configuration tasks or the production system. Every authorized user of an IT system has its own user account and password managed by the authorized IT administrator. An authentication user account and password is enforced by all computer systems.

O. Logical- Operations: The network segments and computer systems are kept up to date software updates, security patches, virus protection, and spyware protection). The backup of sensitive data and security relevant logs is applied accordingly 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 is assigned to each different client.

O. Config-Control: The site has a procedure for the setup of the production process for each new product- From the release of a new configuration of the product to the production of the product. The site has also integrated a process of change management whereby process to introduce changes to the product or processes is enforced. Only authorized personnel can access the changes in the system. The configuration management system which is automated supports the entire production control.

O. Config- Process: The site controls its services and processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development of test programs and the assembly of the products, for the management of optimizing the documentation and process flow managed by the site.

O. Acceptance-Test: The site delivers configuration items that fulfill the specified properties. Specification checks, Machine Parameters, Functional and visual control checks and tests are performed to ensure that the products are compliant to the specifications defined. Tests logs are stored and maintained in the database to support the tracing and identification in case of any systematic failures.

O. Staff engagement: All employees have to sign a non-disclosure agreement upon their employment with the site. Authorized staffs who are engaged to move, transfer and have contact with the security configuration items have to be trained and qualified based on the security procedures, on handling of the products. Briefing session with employees on basic security procedures of the company is done for every new employee joining the site and yearly sessions are also conducted to facilitate and enforce the importance of security within the site.

O. Zero-Balance: Tracing of the security product is essential and the site has to ensure that each device of the client are tracked separately and are accounted for each functional and defective device at every production step. Devices are tracked until when they are shipped or destructed as determined by clients.

O. Reception-Control: Upon receipt of products an incoming inspection is performed. The inspection comprises the received amount of products and the identification and assignment of the product to a related internal production process.

O. Internal Transport: The internal shipment procedure is applied to the configuration item. The recipient of a physical configuration item is identified by the assigned clients address. The internal shipment procedure is applied to the configuration site. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during the internal shipment.

O. Data Transfer: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms (PGP Keys) to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secured measures and they are sufficiently protected.

Use of SFTP Server and SFTP Client system is for transfer of confidential/sensitive data between UTAC and the Customer securely through data encryption. The SFTP Server is hosted in locked rack at secured UTAC Data Centre (with biometric access control). On request, SFTP user ID and password will be generated and issued to specific customer, to allow a secure access for each individual Customer.

O. Control Scrap: The site has measures to destruct sensitive configuration items. Rejected or defective devices are either destructed by authorized vendors or are returned to the clients.

5.1 Security Objectives Rationale

The SST includes a Security Objectives Rationale with two parts. The first part includes the tracing which shows how the threats and OSP's 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.
The OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

.

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

5.1.1 Mapping of the Security Objectives

Threats and OSP	**Security Objectives**
T. Smart Theft	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security
T. Rugged-Theft	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security
T. Computer-Net	O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Staff-Engagement
T. Accidental-Change	O. Logical-Access O. Config-Process O. Acceptance-Test O. Staff-Engagement O. Zero-Balance
T. Unauthorized Staff	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Config-Control O. Staff-Engagement O. Zero-Balance O. Control Scrap

Threats and OSP	Security Objectives
T. Staff Collusion	O. Internal Monitor O. Maintain- Security O. Staff-Engagement O. Zero-Balance O. Data-Transfer O. Control-Scrap
T. Attack-Transport	O. Internal-Transport O. Data-Transfer
P. Config-Items	O.Config-Items O.Reception-Control
P. Config-Control	O. Logical-Access O. Config-Control
P. Config-Process	O. Config-Process
P. Reception-Control	O. Reception-Control
P. Accept-Product	O. Config-Items O. Config-Control O. Config-Process O. Acceptance-Test
P. Zero-Balance	O. Internal-Monitor O. Staff-Engagement O. Zero-Balance O. Control-Scrap
P. Prod-Transport	O. Internal-Transport O. Data-Transfer
P. Data-Transfer	O. Data-Transfer
P. Secure Scrap	O. Zero Balance O. Control-Scrap

6.0 Extended Assurance Components Definition (AST_ECD)

No extended components are currently defined in this Site Security Target.

7.0 Security Assurance Requirement (AST_REQ)

Clients using this site Security Target require an evaluation against evaluation assurance level EAL 6. This Security Assurance Requirement (SAR) is often requested in the Security IC Platform Protection Profile.

The Security Assurance Requirements (SAR) are from the class ALC (LIFE-CYCLE SUPPORT) as defined:

- CM Capabilities (ALC_CMC.5)
- CM SCOPE(ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-Cycle Definition (ALC_LCD.1)

Note 1: The assurance component ALC_DEL.1 is only applicable to the external delivery to the consumer the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS. The component ALC_DEL.1 is not in the scope of audit.

Note 2: The assurance component ALC_TAT.3 is not in the scope of evaluation because neither source code nor is any task performed at the site that must be considered accordingly to ALC_TAT.

7.1 Application Notes and Refinements

The description of the site certification process includes specific application notes. The main item is that a product that is considered as intended TOE is not available during the evaluation. Since the terms "TOE" is not applicable in the SST the associated process for the handling of products (or "intended TOEs") are in the focus and described in this Site Security Target. These processes are subject of the evaluation of the site.

7.1.1 Overview and Refinements regarding CM Capabilities (ALC _CMC)

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

According to the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes are defined for ALC_CMC.5.

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

The life cycle described is a complex production process which sufficient verification steps to ensure the specified and expected results are used during the control of the product. Test procedures, verification procedures and associated expected results must be under configuration management.

The configuration items for the considered product type are listed in section 4.1. The CM documentation of the site is able to maintain the items listed for the relevant life cycle step and the CM system is able to track the configuration items.

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

7.1.2 Overview and refinement regarding CM Scope (ALC_CMS)

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

In the particular case of a security IC, the scope of the configuration management can include a number of configuration items. The configuration items already

defined in section 4.1 that are considered as TOE implementation representation, include:

- Wafers with Security ICs (untested and tested)
- Dies after wafer level chip scale packaging
- Assembled flipchip devices
- Test programs which may include authentication data for testing
- Test results data generated by chip probe and final test
- Pre-personalization data
- Client specific instructions that support the security of internal shipment to the client

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

7.1.3 Overview and refinements regarding Development Security (ALC_DVS)

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

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

Based on these requirements the physical security as well as the logical security of the site is in the focus of the evaluation. Beside the pure implementation of the security measures also the control and the maintenance of the security measures must be considered.

If the transfer of configuration items between two sites involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation), this is considered as internal shipment. In general, the security requirements for confidentiality and integrity are the same but it must be clearly distinguished to ensure the correct subject of the evaluation.

7.1.4 Overview and refinements regarding life Cycle Definition (ALC_LCD)

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 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. testing or initialization is performed at the site or not.

The Protection Profile does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products are assembled and the functional devices are delivered to the clients. The defective devices are scrapped or also returned to the client.

7.2 Security Assurance Rationale (SAR)

The Security Assurance rationale maps the content elements of the selected assurance components to the security objectives defined in this Site Security Target. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, the process is based on the assumption that the received configuration items are appropriately labeled and identified. O. Config-Process ensures that only authorized staff can apply changes. This comprises changes related to process flows, procedures, and items of clients. Teams are defined to assess and release changes

Table 7.2a: Dependency Table for Class ALC – Life-cycle Support

ALC Component	Dependencies	Applied Dependencies
ALC_CMC.5	ALC_CMS.1 ALC_DVS.2 ALC_LCD.1	ALC_CMS.1 ALC_DVS.2 ALC_LCD.1
ALC_CMS.5	No dependencies	Not Applicable
ALC_DEL.1	No dependencies	Not Applicable
ALC_DVS.2	No dependencies	Not Applicable

Note: The dependencies are fulfilled with the required level of assurance components or with superior level.
The ADV_IMP.1 is not fulfilled since ALC_TAT.3 is not in the scope of evaluation (refer to note 2 in part 7.0 of the SST). Thus, all dependencies introduced by this EAL6 package are satisfied.

Table 7.2b: Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling.	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 is assigned to each different client defined by O.Config-Items. Wafer lots come with unique part ID automatically generated by the system tools. . Lot number & wafer ID are the data to be process identified. The process of the data is conducted according to the configuration information of the product owner. Generated files are identified by unique file names and version numbers. The usage (reported in A-UTAC-MF-090623) and the labeling system described in A-UTAC-PC-080101 appears convenient for unique items identification recording and traceability.
ALC_CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control	Incoming inspection according ensures product identification and associated labeling. The labeling is checked against internal identification as defined by O. Config-Items. O. Config-Control ensures that each client part ID is setup and release based on a defined process. This also includes changes related to a customer part ID. Configurations can only be done by authorized staff. O. Config-Process provides a configured and controlled assembly and test processes. O. Reception-Control comprises the incoming labelling and the mapping to internal identifications.
ALC_CMC.5.3C: The CM documentation shall justify that acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control	O. Config-Process ensures that only authorised staff can apply changes. This comprises changes related to process flows, procedures and items of clients. Teams are defined to assess and release changes. O. Reception-Control comprises the incoming labelling and the mapping to internal identifications. O. Config-Items comprise the internal unique identification of all items that belong to a customer part ID. Each product is setup according to O. Config-Control comprising all necessary items.

SAR	Security Objective	Rationale
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O. Config-Items O. Config-Control O. Reception-Control	O. Config-Items comprise the internal unique identification of all items that belong to a customer part ID. Each product is setup according to O. Config-Control comprising all necessary items. O. Reception-Control comprises the incoming labeling and the mapping to internal identifications.
ALC_CMC.5.5C: The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O. Logical-Access O. Logical-Operation O. Config-Control O. Config-Process O. Acceptance-Test	O. Config-Control assigns the setup including processes and items for the production of each customer part ID. O. Config-Process comprises the control of the production processes. O. Logical-Access and O. Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff. O. Acceptance-Test provides an automated testing of the functionality and supports the tracing
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O. Config-Control O. Config-Process	O. Config-Control assigns the setup including processes and items for the production of each customer part ID. O. Config-Process comprises the automated management of the assembly and test flow processes.
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. Config-Control O. Config-Process	Different roles are assigned to different teams. Members of the teams are responsible to release different steps of the production and the final product. The management of the production environment and the different steps is assigned to different teams as described by O. Config-Process. O. Config-Control assigns the setup including processes and items for the production of each customer part ID.
ALC_CMC.5.8C: The CM system shall identify the configuration items that comprise the TSF.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control	O. Config-Items comprise the internal unique identification of all items that belong to a customer part ID. The management of the production environment and the different steps is assigned to different teams as described by O. Config-Process. O. Config-Control assigns the setup including processes and items for the production of each customer part ID. O. Reception-Control comprises the incoming labeling and the mapping to internal identifications.
ALC_CMC.5.9C: The CM system shall support the audit of all changes to the product by automated means, including the originator, date, and time in the audit trail.	O. Config-Control O. Config-Process O. Zero-Balance O. Reception – Control O. Internal-Transport	The automated production control covered by O. Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator. The processes used for the identification and manufacturing are covered by O. Config-Control O. Config-Process ensures that only authorised staff can apply changes. This comprises changes related to process flows, procedures and items of clients. Teams are defined to assess and release changes. O. Reception-Control comprises the incoming labeling and the mapping to internal identifications. The reception and incoming inspection supports the detection of attacks during the transport of the secure products to UTAC (USG1) according to O.Reception-Control. O. Zero-Balance ensures the accountability of all security products during production. All devices including functional and non-functional are tracked according to O. Zero-Balance. O. Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence. The internal shipment to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport supported

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. Acceptance-Test O. Internal-Transport	O. Config-Control describes the management of the configuration items received from the client and delivered to the client. According to O. Config-Process the CM plans covers the general dependencies of the production process O. Acceptance-Test provides an automated testing of the functionality and supports the tracing. O. Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence.

SAR	Security Objective	Rationale
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the delivered configuration items are generated.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control	O. Reception-Control comprises the control of the incoming configuration items. O. Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. O. Config-Process ensures that only controlled changes are applied.
ALC_CMC.5.12C: The CM documentation shall include a CM plan.	O. Config-Control O. Config-Process	According to O. Config-Control the setup of each customer part ID includes an associated CM plan including the release. O. Config-Process ensures the reliability of the processes and tools based on dedicated CM plans.
ALC_CMC.5.13C: The CM plan shall describe how the CM system is used for the development of the product.	O. Config-Control O. Config-Process	O. Config-Control describes the management of the customer 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. Config-Items O. Config-Control O. Config-Process O. Reception-Control	O. Reception-Control supports the identification of configuration items. O. Config-Items ensure the unique identification of each product produces at USG by the customer part ID. O. Config-Control ensures a release for each new or changed customer part ID. O. Config-Process ensures the automated control of released products
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O. Config-Control O. Config-Process O. Zero-Balance O. Reception-Control O. Internal-Transport	The objectives O. Reception-Control, O. Config-Control, O. Config-Process ensure that only released customer part IDs are produced. This is supported by O. Zero-Balance ensuring the tracing of all security products. O. Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O. Config-Control O. Config-Process O. Acceptance-Test O. Internal Transport	In this work unit, the processes rather than the TOE are in the focus. The several procedures in place at USG1 to support the CM system demonstrate that all the configuration item are being maintained. O. Config-Control ensures a release for each new or changed customer part ID O. Config-Process the CM plans describe the services provided by the site. O. Acceptance-Test provides an automated testing of the functionality and supports the tracing. O. Internal-Transport include the packing requirements, the reports, logs and notifications including the required evidence

Table 7.2c: Rationale for ALC_CMS.5

SAR	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 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 the 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 ensures a release for each new or changed customer part ID O. Config-Process defines the configuration control including part IDs, procedures and processes. In the frame of this site certification objective, the TOE here shall be understood as the Customer Product (for which USG1 performs manufacturing operations). These are clearly stated in the provided procedures & instructions. USG1 has the capability (demonstrated through documentation) to record & trace the configuration items part of the TOE.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control O. Internal-Transport	Items, products and processes are uniquely identified by the database system according to O.Config-Items. With the production flow, 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 labeling and preparation for the transport is defined by O.Internal-Transport supported by O.Config-Items.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/subcontractor of the item.	O. Config-Items	UTAC (USG1) does not involve subcontractors for the assembly of security products. According to O.Config-Items, all configuration items for secure products are identified.

Table 7.2d: Rationale for ALC_DVS.2

SAR	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. Control-Scrap	The physical protection is provided by: O. Physical-access and supported by O. Security-Control, O. Alarm-response, 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. Any scrap that may support an attacker is controlled according to O. Control-Scrap.

SAR	Security Objective	Rationale
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.	O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Acceptance-Test O. Zero-Balance O. Reception-Control O. Internal-Transport O. Data-Transfer	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives: The associated control and continuous justification is subject of the objectives:O. Internal-Monitor O. Maintain- Security .The logical protection of data and the configuration management is provided by The personnel security measures. O. Logical-Access and O support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff. O. Logical-Operation including functional and non-functional are tracked accordingly. O. Acceptance-Test provides an automated testing of the functionality and supports the tracing. All devices including functional and non-functional are tracked according to O. Zero-Balance. The reception and incoming inspection supports the detection of attacks during the transport of the secure products to UTAC (USG1) according to O.Reception-Control. The reception and incoming inspection supports the detection of attacks during the transport of the secure products to UTAC (USG1) The internal shipment to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport] O.Data-Transfer to ensure access by authorized recipients only.
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 product during internal shipment.	O. Reception-Control O. Internal-Transport O. Data-Transfer	The reception and incoming inspection supports the detection of attacks during the transport of the secure products to UTAC (USG1) according to O.Reception-Control. The internal shipment to the client is protected by similar measures according to the requirements of the client based on O.Internal-Transport supported by O.Config-Items. Sensitive data received by UTAC (USG1) is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.

Table 7.2e: Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C: The life-cycle definition documentation shall describe the model used to develop and maintain the TOE..	O. Config-Control O. Config-Process	The processes used for the identification and manufacturing are covered by O. Config-Control and O. Config-Process.
ALC_LCD.1.2C: The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.	O. Config-Process O. Acceptance-Test O. Zero-Balance	The site does not perform development tasks. The applied test flow process is controlled according to O. Config-Process, the finished customer parts are tested according to O. Acceptance-Test and all security products are traced according to O. Zero-Balance.

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

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

8.0 Site Summary Specification (AST_SSS)

8.1 Preconditions required by the Site

The site provides a released Wafer probe / package testing and wLCSP /flipchip assembly flow process. In order to perform this service, the client must fulfill requirements and provide sufficient information to setup and control the wafer probe / package test and wLCSP/Flipchip assembly flow.

This includes information about the classification of the documents and the product (see A.Prod-Specification). Also included are the test programs with authentication data and test vectors for the verification of the client trim code, pre-personalization data as well as consumer code and manufacturer code (see A. Testdata-Support).

The client must ensure secured transfer of appropriate testing related data to the site with appropriate labeling ensuring pairing to the physically handled untested wafers received by the client. Related testing data must be in a state that can be used by UTAC (USG1) testers directly with no need for transformation (see A.Testdata_Support). The security classification of items received must allow the handling according to the specific roles for this security classification.

For each product the client must provide the destination for the shipment of the tested wafers / dies and or packaged units. In addition, the client must define the packing requirements neede to support the confidentiality and integrity of the TOE. (see A.Internal-Shipment).

Regarding a destruction rejected dies /wafers /packaged units (untested or tested), the client must specify whether the scrap material needs to be destroyed by UTAC (USG1) or to be sent back to the client (see A.Scrap). Rejected wafers / dies /packaged units will be destroyed by UTAC (USG1) or sent back to the customer upon request.

8.2 Services of the Site

USG1 Site covers part of the life cycle of the client's secure device related to the testing of wafer /ICs. In detail, the following service and related management procedures are provided by the site:

- Incoming Material (Security IC wafers & other raw materials)
  Secure wafers for probing, assembly and final testing. Customers will also provide their build instructions and test programs to the site in order to start the wafer probing, assembly and testing production.

- Storage and Warehousing of Secure IC Wafers
  Secure IC wafers (in boxes) at Receiving Area, the site will key in the Incoming material information into the system (SLRS – Stream Line Receiving System). After

transaction in SLRS, the boxes are unpacked un-packed and placed inside a secure cabinet. A packing list is attached to each lot. The production material handler will do physical lot verification against the SLRS packing list. Receiving personnel will acknowledge the shipment in the UMS (UTAC Management System) and issue the GRN (Goods Received Notice). Production material handlers (2 personnel) will move the received lot to the wafer bank/die bank area using a caged trolley with a combination lock.

- Wafer Bank
  Wafer bank personnel will transact the lot into the UMS. After which, it is unpacked and transferred to a FOUP and lot is sent for Wafer Incoming Quality Inspection. The Process Traveler is generated and attached to the lot prior to sending lot to Wafer Sort.
  Once secure lot is received from Wafer Bank, the wafer sort operator will scan the barcode in the process traveler (PT). The barcode contains the lot ID which links to the UMS for system check of the lot information. System will download the correct test program if UMS information matched with the PTRD information and wafer sort production can now start. The secure device test program resides in the production program server in the isolated network. The BB Server containing the serialization of the device is controlled by the customer. UTAC (USG1 Site) only provides the isolated network infrastructure and physical security for production.

- Assembly
  Before any mass production is conducted in assembly, the site will have already optimized the production process during the NPI (New Product Introduction) stage where the site will review the customer spec requirements, run qualification and pre-production lots. Data on the runs are sent to customer for their review and final approval for full production. For every mass production launch, each job is assigned a unique production lot ID which will be traced from the start to finish through the UMS. The site also practices Zero Balancing where each die in the wafer or each packaged unit is traced and accounted for through-out the process. An assembly process traveler document is attached to each production lot.

  Once production is launched, the wafers will undergo the following manufacturing processes in assembly:

  Wafer Taping: This is the process where the active side is protected with a backgrind tape to protect it while the wafer undergoes back-grinding during the next process. Lot In/Out is transacted in the UMS.

  Wafer Backgrind: The taped wafers are then back-grinded to the desired thickness as required by the customer in the Assembly Build Instruction. Back-grind process recipe is auto-download by scanning of the barcode in the process traveler. Lot In/Out is transacted in the UMS. Once completed back-grinding process the tape is then removed from the wafer.

  Wafer Mount: The back-grinded wafers are then mounted on a wafer ring to prepare it for the laser groove & wafer dicing processes. Lot In/Out is transacted in the UMS.

  Laser Groove / Wafer saw: For low K wafers (≤ 65 nano), laser groove is required prior to wafer saw. Wafer saw process will complete the isolation of the different ICs in a wafer. Both laser groove and wafer saw recipe are auto-downloaded through UTAC (USG1) RMS (Recipe Management System). Lot In/Out is transacted in the UMS.

Once the wafers are completely sawn, the lot goes through UV cure, Post saw inspection and Tape and Reel (for wLCSP devices) or through FlipChip attach (for Flipchip devices). Lot In/out are transacted in the UMS for each process stage.

Tape and Reel: For wLCSP devices, Wafer map diagrams of the wafers are downloaded through the CIM Wafer Map Client System and the electrically good dies are picked and place into reels. Lot In/Out is transacted in the UMS. Once completed Tape & Reel, the secure lot in reels is sent to EOL-Packing area in caged trolleys with combination lock and under "4 eyes" supervision. Wafer skeletons are accounted for, packed and security sealed and sent to the Reject Control Center.

Flip Chip Attach: For Flip Chip devices, Wafer map diagrams of the wafers are downloaded through the CIM Wafer Map Client System and the electrically good dies are picked and place into PCB substrates and sent for reflow and flux clean. Lot In/Out is transacted in the UMS. Wafer skeletons are accounted for, packed and security sealed and sent to the Reject Control Center.

Mold/PM Cure: After flux clean, the flip chip attached substrates are baked in preparation for the molding process. During molding, the flipchip dies are encapsulated with thermo-setting molding compound and cured. Lot In/Out is transacted in the UMS.

Ballmount: After Post mold Cure, the molded substrates are sent for ball mounting where a solder ball alloy is attached on the ball pads of the substrates and reflowed. Lot In/Out is transacted in the UMS.

Saw Singulation: Ball-mounted substrates are mechanically sawn to isolate into individual units. Lot In/Out is transacted in the UMS.

Auto VM: After singulation, the lot is sent for 100% auto visual-mechanical inspection. Visual defect/reject units are separated from the good units. Lot In/Out are transacted in the UMS. The rejected units are placed inside a plastic bag and security sealed before sent to the Reject Control Center. (Note: Rejects are placed inside a caged trolley with combination lock when transporting to the Reject Control Center).

- Final Test & Pre-personalization: In order to check if the connectivity of the secure modules are good or not, the modules/units undergo testing process via contact pin (USG1) isolated server. The key set for unit serialization is transferred by customer to their Black box server. During testing process, the test operator scans the barcode in the Process Traveler which links to the PTRD (Program Test Recipe Database). The system will then provide what test program revision to use. This information is automatically sent to the tester which does an auto-matching and retrieves the correct test program from the isolated server. Once test program is loaded into the tester, the system communicates with the BB box server to retrieve the keys for unit serialization.

- In the event that UTAC (USG1 Site) Product Engineers find abnormalities in the test program during program check-out, they will abort the check-out and feedback the abnormalities (with data) to the customer. The customers will then review and modify the program and send a new test program revision to UTAC (USG1 Site).

- The BB Server containing the serialization of the device is controlled by the customer. UTAC (USG1 Site) only provides the isolated network infrastructure and physical security for production.

- Use of SFTP Server and SFTP Client system is for transfer of confidential/sensitive data between UTAC and the Customer securely through data encryption. The SFTP

Server is hosted in locked rack at secured UTAC Data Centre (with biometric access control). On request, SFTP user ID and password will be generated and issued to specific customer, to allow a secure access for each individual customer.

- Outgoing Visual Inspection: Before the final packaging of the tested lots, the lots undergo visual inspection according to the visual criteria defined by the customer.

- Packaging: Depending on the customer's packing requirements, the final packaging of the secure devices is packed in reel format or in trays. These are then packed into boxes with proper box identification labels as required by the customer.

- Destruction of secured reject materials:

  The good and bad dies in the wafers are all tracked using the Zero Balancing procedure from the start to end of the production of the secure lot and are also recorded electronically in the UMS. For customers who require their scrap dies and wafers to be shipped back to their facility, they will arrange the appropriate transportation for the shipping of the scrap materials to their site. UTAC (USG1 Site) will store the scrap materials in proper containers with the relevant procedure before the scrap materials are collected and transported to customer's site.

- Shipment to customers
  Shipments are considered "internal shipment" as the packaged materials is routed back to UTAC (USG1 Site) direct customer. Customer provides their own forwarders which UTAC (USG1 Site) security performs the necessary security checks before they are allowed in to collect the materials. The site will inform the customer upon completion of the production order and the completed modules are ready for collection.

UTAC (USG1 Site) maintains a certified Quality Management System as a basis for all security process, rules and policies. Each product gets a unique part ID. This part ID is linked with the wafers and dies with security ICs and processed dies. The site does conduct wafer probe also considering pre-personalization and wafer level chip scale packaging. Furthermore, the site provides secure storage and destruction operations according to the request of the client, or returns the scrap wafers to the client.

The processes for assembly, testing and acceptance are setup at the site according to the client's specifications (E.g. Bonding diagrams, Build Instruction, test specification and packaging requirements, if applicable) as provided by the client. For the release, a samples lot is produced at the site.

The complete product specific production flow includes a functional test of each device as part of the acceptance process. The functional tests are either developed by UTAC (USG1 Site) based on the test specifications and electrical parameters/ limits provided and determined by the client or the test program provided by the client. The test program are provided by the client and integrated in the test environment of the site. Test program provided by the client must be dedicated for the test tools used at the site.

The site has a standard procedure for packing of finished products and preparation of shipment. If special packaging requirements are provided by the client, they are included in the process setup. The client is alerted if products are ready for transport because the transport will be arranged by the client. 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.

Defective or rejected products are either returned to the client or they are destructed according to the defined secure destruction process. The client must decide during the product setup whether the rejects and defective devices on the wafer are also returned or if they shall be destructed by UTAC (USG1 Site).

The site ships the packaged wafers / dies / ICs to the destination defined by the client using a packing procedure that is defined by the client to ensure a secure handling of the secure wafers / dies /ICs. Before executing the packing operation, the security seal will be checked and confirmed by the system.

8.3 Objectives Rationale

The following rationale provides a justification that shows that all threats and OSP are effectively addressed by the security objectives:

O. Physical-Access

The plant is surrounded by a fence and controlled by CCTV. The access into 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. This 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.

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

During working hours the security officer will monitor the site and surveillance system. During off-hours, the alarm system is used to monitor the site. The CCTV systems support these measures because it is always enabled. Further on the security control is supported by O.Physical-Access requiring different level of access control for the access to security product during operation as well as during off hours.

This addresses the threats T. Smart-Theft and Rugged-Theft. Supported by O. Maintain-Security and O.Physical-Access also an internal attacker triggers the security measures implemented by O.Security-Control. Therefore also the Threat T.Unauthorized-staff is addressed.

O. Alarm-Response

During working hours the security officer will monitor the alarm system. The alarm system is connected to a control center that is running 24/7. 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

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

O. Internal-Monitor

Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like firewall, Virus protection and 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. The required security methods and measures are implemented and maintained. Effectiveness of all measures is verified regularly through internal audits which is conducted at least once / year. These audits, security meetings and the reviews of results and changes are suitable to check the implemented security measures. This will address the T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-staff, T.Staff-Collusion and the OSP P.Zero-Balance.

O. Maintain Security

The security relevant systems enforcing or supporting O. Physical-Access, O. security-Control and O. Logical Access are checked 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.

This addresses T. Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-staff and T.Staff-Collusion.

O.Logical-Access

The internal network is separated from the internet with a firewall. The internal network is further separated into 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. Access to the corresponding networks is restricted to authorized users working on the related area. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events.

The individual accounts are addressing T.Computer-Net. All configurations are stored in the database of the ERP system. Supported by O. Config-Items this addresses the threats T.Accidental-Change and T.Unauthorized-staff and the OSP P.Config-Control.

O. Logical-Operation

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

This addresses the threats T.Computer-Net and T.Unauthorized-staff.

O. Config-Items

Each configuration item including security products are identified by the shipping documents, packaging label and information in the system based on shipments alerts from the client. If a product cannot be identified, it is put on hold in a secured storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seal of these boxes, if applicable. The CM documentation shall show that a process is in place to ensure an appropriate and consistent labeling and only correctly identified products are released for production. This addresses the OSP P. Accept-Product.and OSP P Config-Items

O. Config-Control

Procedures arrange for a formal release of configuration documents, specifications and test programs for the setup of test and/or assembly process flow. The information is also stored in the configuration database. The Engineering Change Notice (ECN) and Process Change Notice (PCN) procedures are in place to classify and introduce changes. The procedures also define the separation between minor and major changes and the relevant interactions and releases with clients if required. Each user has access rights limited to the needs of his function, thus, only authorized changes are possible.

Supported by O. Config-items this addresses the threat T.Unauthorized-staff and the OSP P. Config- Control, P.Accept-Product

O. Config-Process

The release configuration information including production and acceptance specifications is automatically linked to every work order. The test program is automatically loaded to the tester through barcode scanning of the secure lot process traveler according to the configuration information of the work order.

This addresses the threat T.Accidental-Change and the OSP P. Config-process, P. Accept Product.

O. Acceptance-test

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

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

O. Staff-Engagement

All employees are interviewed before hiring. They must sign NDA and a code of conduct for the use of computers 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. The security objectives O. Physical-Access, O. Logical-Access and O. Config-Items support the engagement of the staff.

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

O. Zero Balance

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

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

O. Reception-Control

At reception, each configuration item including security products are identified by the shipping documents, packaging label and information in the 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 secured storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seal of these boxes, if applicable. Thereby only correctly identified products are released for production.
The OSPs P.Config-Items and P.Reception-Control are addressed by the reception control.

O. Internal-Transport

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

The Threat T.Attack-Transport and the OSP P.Prod-Transport are addressed by the Internal Transport.

O. Data-transfer

The confidential data transfer from / to the site occurs only in encrypted (using PGP key). The cryptography keys are stored on a well-protected server. SFTP Server and Client is also use for confidential data transfer and SFTP transfer path is encrypted. The server is located inside the company data center secured with biometric access.

Supported by O.Logical-Access and O.Staff-Engagement, this addresses the threats T.Staff-Collusion and T.Attack-Transport as well as the OSP P.Prod-Transport and P.Data-Transfer.

O. Control-Scrap

Scrap is identified and handled in the same way as functional devices. They are stored internally in a secured location. The scrap is either returned to the client using the same packaging requirements as for functional products or its destructed in a controlled and documented way. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor.

Sensitive information and information storage media are collected internally in a safe location and destructed in a supervised and documented process.

Supported by O. Physical-Access and O. Staff-engagement, this addresses the threats T.Unauthorized-staff and T.Staff-Collusion and the OSP P.Zero-Balance, P.Secure-Scrap.

8.4 Security Assurance Requirements Rationale

The Security Assurance Rationale is given in section 7.2. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in Common Criteria for information Technology Security Evaluation Part 3: Security Assurance Components **April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.** Therefore the following Security Assurance rationale provides the justification for the selected Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. In general the selected Security Assurance Requirements fulfill the needs derived from the Protection Profile. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled.

ALC_CMC.5

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 support the integrity and confidentiality required for the products. Therefore these assurance requirements stated will meet the requirements for the configuration management.

ALC_CMS.5

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

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

ALC_LCD.1

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

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

ALC_TAT.3

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

8.5 Assurance Measure Rationale

O. Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Alarm-Response

ALC_DVS.2.1C: Requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Internal-Monitor

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.

O. Maintain-Security

ALC_DVS.2.1C: Requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby 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. Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

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_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.

O. logical-Operation

ALC_DVS.2.1C: Requires that the developer shall describe all personnel, Procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby 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. Thereby this objective is suitable to meet the Security Assurance Requirement.

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.

O.Config-Items

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

In addition ALC_CMC.5.3C requires that the CM system uniquely identifies all configuration items.

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

ALC_CMC.5.8C addresses the same requirement as 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 fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration items is indicated in the configuration list. The objective meets the set of Security Assurance Requirements.

ALC_CMC.5.11C requires the CM system be able to identify the version of the implementation representation from which the delivered configuration items are generated.

O. Config-Control

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

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

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

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.

ALC_CMC.5.6C addresses the same requirement as ALC_CMC.5.12C requires a CM documentation that includes a CM plan.

ALC_CMC.5.7C requires that the CM plan describes how the CM system used for the development (production) of the TOE.

ALC_CMC.5.8C addresses the same requirement as ALC_CMC.5.13C and 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.5.9C addresses the same requirement as ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are maintained under the CM system.

ALC_CMC.5.10C addresses the same requirement as ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMC.5.11C requires the CM system be able to identify the version of the implementation representation from which the delivered configuration items are generated.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
In addition ALC_LCD.1.1C requires that the life cycle definition describes the model used to develop and maintain the products.

The objective meets the set of Security Assurance Requirements.

O. Config-Process

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

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.

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.5.5C requires that the CM system supports the production by automated means.

ALC_CMC.5.6C addresses the same requirement as ALC_CMC.5.12C requires that the CM documentation includes a CM plan.

ALC_CMC.5.7C requires that the CM plan describe how the CM system is used for the development of the TOE.

ALC_CMC.5.8C addresses the same requirement as ALC_CMC.5.13C and 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.5.9C addresses the same requirement as ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.10C addresses the same requirement as ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMC.5.11C requires the CM system be able to identify the version of the implementation representation from which the delivered configuration items are generated.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

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

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

The objective meets the set of Security Assurance Requirements.

O. Acceptance-Test

The testing of the products is considered as automated procedure as required by ALC_CMC.5.5C.

ALC_CMC.5.10C addresses the same requirement as ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated with the CM plan.

.

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

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

Thereby the objective fulfills this combination of Security Assurance Requirements.

O. Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. Thereby the objective fulfills this combination of Security Assurance Requirements.

O. Zero –Balance

ALC_CMC.5.9C addresses the same requirement as ALC_CMC.5.15C requires evidence that all configuration items are being maintained under the CM system.

ALC DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the TOE.

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

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

O. Reception – Control

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

ALC_CMC.5.3C requires for each configuration item, the configuration list shall indicate the developer/subcontractor of the item

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

ALC_CMC.5.8C addresses the same requirement as 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.5.9C addresses the same requirement as ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.11C requires the CM system be able to identify the version of the implementation representation from which the delivered configuration items are generated.

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.
ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during the transfer between sites.

ALC_DVS.2-3 requires the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product during internal shipment.

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

O. Internal-Transport

ALC_CMC.5.9C addresses the same requirement as ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.5.10C addresses the same requirement as ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated with the CM plan.

ALC_CMS.5.2C goes according to the unique identification of the packaging as configuration item. Thereby this objective contributes to meet the Security Assurance Requirement.

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.2-3 requires the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product during internal shipment.

O. Data-Transfer

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.2-3 requires the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product during internal shipment.

This objective will meet the security Assurance Requirement.

O. Control-Scrap

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

8.6 Mapping of the Evaluation Documentation

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

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

9.0 Definitions

9.1 Client

UTAC (USG1) operates as a subcontractor of the IC manufacturer. The word "client" is used here instead of customer since the words 'customer" and "consumer" are reserved in CC.

9.2 Customer wafer map

The wafer map defined and coming from the client.

9.3 Wafer map

The electrical map data generated by the tester after chip probe.

10.0 List of Abbreviations

CC -	Common Criteria
CM -	Configuration Management
EAL -	Evaluation Assurance Level
IC -	Integrated Circuit
IT -	Information Technology
UMS	UTAC Management System
SAP -	Name of software used for enterprise resource planning
OSP -	Organization Security Policy
PP -	Protection Profile
SAR -	Security Assurance Requirement
SST -	Site Security Target
ST -	Security Target
TOE -	Target of Evaluation
wLCSP	Wafer Level Chip Scale Package
SOI	Standard Operating Instruction