Common Criteria Information Technology Security Evaluation

Site Security Target of Hua Hong Semiconductor Limited

Version 1.0

Revision history

Version history

Version	Date	Modification
1.0	July 31th，2025	Creation

Validation process

Process	Name	Function
Author	Fei Fengxin	Customer Quality Engineering
Approver	Changliang Wu	Customer Quality Engineering and Quality System

Distribution list

Name	Company
ANSSI certifier	ANSSI
Peter DE LINT	SERMA Safety & Security
To whom it may concern	Composition Laboratory
Developer Responsible Name	Hua Hong Semiconductor Limited

Table des matières

1. Introduction

The purpose of this document is to describe the site security target for the production of secure semiconductor devices.

This Site Security Target refers to the sites:

- Fab9 Hua Hong Semiconductor Manufacturing (Wuxi) Corporate Limited (HHWX Fab9),
- Fab7 Hua Hong Semiconductor (Wuxi) Limited (HHWX Fab7).

These sites are part of production flow of security IC modules for Smart Card and IT security products. More precisely, HHWX Fab7 is used for the data preparation and wafer fab. Then, HHWX Fab9 is a wafer fab.

1.1 – Site Security Target and Site Reference

1.1.1 – Site Security Target reference

Reference	
Title	Site Security Target of Hua Hong Semiconductor Limited
Reference	HHWX_SST_V1.0
Version	1.0
Date	July 31th, 2025
Company	Hua Hong Semiconductor Limited
Name of the sites	Fab 7 Hua Hong Semiconductor (Wuxi) Limited Fab 9 Hua Hong Semiconductor Manufacturing (Wuxi) Corporate Limited
Sites Location	No. 30 Xin Zhou Road, Xin Wu District, Wuxi, Jiangsu Province, P.R China No. 30-1 Xin Zhou Road, Xin Wu District, Wuxi, Jiangsu Province, P.R China
Product Type	Wafer fab & Data preparation
EAL level	EAL6
Evaluation Laboratory - ITSEF	SERMA Safety & Security
Certification body	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Tableau 1: Site Security Target Reference

1.2 – Site Description

The sites HHWX Fab7 and HHWX Fab9 are located in Jiangsu near Shanghai (P.R China). These sites are in charge of the data preparation, wafer manufacturing\scrap\delivery and mask reception/scrap activities. Different analyses are performed as well on products at the reliability and failure analysis

laboratory. The site relevant areas are listed Section. Access to these areas is only granted with personal badge.

1.2.1 – Physical Scope

The site HHWX is composed of multiple buildings fully occupied by HHWX. The overall security is under the responsibility of HHWX Information Security Management Committee. The information security management committee is composed of chairman, deputy chairman and member. This information security management committee is supported by the information security team with a team leader (head of QRA and head of IT) and team members (coordinator of each department). The areas in the scope of the SST are listed below:

- Fab 7 (including access control area (Security Room) , IT server room, Data preparation area (Security Product T/O Room) , security product warehouse, Cleanroom
- Fab 9 (including access control area (Security Room), IT server room (Not related to Data Preparation Flow) , Cleanroom

1.2.2 – Logical Scope

The site HHWX is in charge of the data preparation (Fab7 E1), wafer manufacturing (Fab7&Fab9 Clean room)\scrap (Fab7 warehouse) \ delivery(Fab7 warehouse) and mask reception/scrap(Fab7 warehouse) activities. The site supports also the failure analysis and the reliability assurance. In addition, HHWX site hosts an IT room related to the production IT infrastructure. The activities of the site cover as defined in “Eurosmart Security IC Platform Protection Profile with Augmentation Packages” [1] and “Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile”[2]:

- IC Manufacturing and testing (Phase 3).

Supporting services are provided by HHWX such as the physical site security, IT support, facilities management, etc.

2. Conformance Claims

The evaluation is based on Common Criteria 2022, release 1:

1. Common Criteria for Information Technology Security Evaluation, part 1: Introduction and General Model; CC:2022, Revision 1, CCMB-2022-11-001[3],
2. Common Criteria for Information Technology Security Evaluation, part 3: Security Assurance Requirements; CC:2022, Revision 1, CCMB-2022-11-003[4],
3. Common Criteria for Information Technology Security Evaluation, part 4: Framework for the Specification of Evaluation Methods and Activities; CC:2022, Revision 1, CCMB-2022-11-004, November 2022[5],
4. Common Criteria for Information Technology Security Evaluation, part 5: pre-defined packages of security requirements; CC:2022, Revision 1, CCMB-2022-11-005, November 2022[6].

For the evaluation the following methodology will be used:

1. Common Criteria for Information Technology Security Evaluation, part 3: Security Assurance Requirements; CC:2022, Revision 1, CCMB-2022-11-003, November 2022[4],
2. Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, CEM:2022, Revision 1, CCMB-2022-11-006, November 2022[7],
3. MINIMUM SITE SECURITY REQUIREMENTS V2, March 2025.

There is no extended component required for this SST.

The Assurance Component from the assurance level EAL6 in the evaluation of the site comprises the following assurance components:

- ALC_CMC.5: Advanced support,
- ALC_CMS.5: Development tools CM coverage,
- ALC_DVS.2: Sufficiency of security controls,
- ALC_LCD.1: Developer defined life-cycle processes,

The assurance level chooses for the SST is compliant to the Protection Profile (PP [1] and [2]) and therefore suitable for the evaluation of security ICs. This Site Security Target is conformant to Part 3 of the Common Criteria.

The chosen assurance components are derived from the assurance level EAL6 of the assurance class “Life-cycle support”. For the assessment of the security measures, attackers with high attack potential are assumed. Therefore, these sites support product evaluation up to EAL6.

The sites do not directly contribute to the development of the intended TOE in the sense of Common Criteria. The sites ensure a reproducible production process within the limits defined for the released wafer production process. This is subject of the configuration management.

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyze and implement the TOE. The assurance family “Tools and Techniques” is not applicable because there is no source code development performed by HHWX. There is no software compilation performed by HHWX.

The assurance component ALC_DEL.1 is only applicable to external delivery to the internal client, the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS. Therefore, the component ALC_DEL.1 is not applicable.

3. Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site.

The Site Security Target is based on the life-cycle defined in Protection Profiles [1] and [2]. The assets (see Section 3.1 – Assets), threats (see Section 3.2 – Threats) and Organizational Security Policies (see Section 3.3 – Organizational Security Policies) defined in this SST are derived from the life-cycle defined in that PP.

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

3.1 – Assets

The following 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 an intended TOE. This comprises sites security concepts and the associated security measures as well as key and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the site of assets below.

The integrity of any machine or tool used for development, production, testing and personalization is not considered as an asset. However, appropriate measures are defined for the site to ensure this important condition.

3.1.1 – List of assets

- Company policy and procedures (DSS related company management policies and procedures)
- Physical Design data (topographic information/GDS file of security Product from Customer)
- Test and characterization related data
- Products (masks, wafers, scrap).

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

3.2 – Threats

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

The following threats are described in a general way. However, they are applicable to the site. These shall support the mapping to the Security Objectives of the site.

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

This attack includes already a variety of targets and aspects with respect to the various assets listed in the section above. It shall cover the range of individuals that try to get unregistered or defect devices that can be used to further investigate the functionality of the device and search for possible exploits. Such as attacker will have limited resources and a low financial budget to prepare the attacks. However, the time can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk.

It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control and surveillance. In general, an access control concept with two or three levels shall be implemented. If two levels are implemented, the more restrictive level of the access control shall prevent the simple access using a lost or stolen access token. Other restrictions may be need for parallel access by two employees. The technical measures shall include automated measures to support the surveillance.

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

Although this attack is applicable for the site where the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise devices at a specific testing for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential.

Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the splitting of sensitive data like keys provide additional support against such attacks. Also, the unique registration of the products can support the protection if they can be disabled or blocked.

T.Computer-Net: A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to development and/or production systems

with the intention to modify the development and/or production process thus violating integrity and possibility confidentiality.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow to attack a product or manipulate a product or retrieve information to allow or change the configuration or the personalization. In addition, a successful access to a company processing the product or the company that produces the product.

Such attackers are considered to have high attack potential because the attacker may have appropriate technical equipment to perform such an attack. Furthermore, the attacker may have the resource to develop or buy software or hardware which can exploit known vulnerabilities within the tools and software used by the company.

Therefore, a protective concept with more than one level is expected. This shall comprise a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users shall have individual accounts which require authentication. For specific tasks or processes standalone networks may be required. The protection must be supported by appropriate measures to update and maintain the computer and network system and analyze logs that may provide indications for attack attempts.

T.Accident-Change: An employee, contractor or student trainee may exchange products of different production lots / different internal clients during production or changes tool configuration that have an impact on the intended TOE by accident.

Employees, contractors or student trainee that are not trained may take products or influence production systems without considering possible impacts or problems. This threat includes accidental changes e.g. due to working tasks of intern engineers or maintenance tasks or contractors within the development and production area.

Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step. Further examples may be machine failure or misalignment between operators that are responsible for products of the same internal client are mixed during production. This also includes the disposal of sensitive products using the standard flow and not the controlled destruction.

T.Unauthorised-Staff: Unauthorized employees or subcontractors get access to assets or systems used for development, configuration management and/or production, so that the confidentiality and/or the integrity of the intended TOE is violated. This can apply to any development and/or production step and any asset related to the intended TOE or its configuration.

Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. tools which process the layout data e.g. in the design center as well as sensitive test and/or configuration data within the test center.

Also other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to start an attack. The disposal of defect equipment and/or sensitive configuration items must be considered.

The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to these different measures are required.

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

Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorized employees and the split of sensitive knowledge can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

T.Attack-Transport: An attacker might try to get hold of any assets during the internal shipment. The target is to compromise confidential information or violate the integrity of the assets during the shipment process to allow a modification, cloning or the direct / indirect retrieval of confidential information.

Confidential information comprises design data, internal client and/or consumer data like code and data or classified product documentation.

The protection of the internal shipment depends on the assets that are exchanged. The protection is related to the assets that must be considered during the site evaluation.

During production, testing and/or assembly, sensitive products and standard products may be handled in parallel. This aspect is addressed by the threats T.Accident-Change, T.Unauthorised-Staff and T.Staff-Collusion. Associated measures against these threats must be covered in the rationale of the SST.

3.3 – Organizational Security Policies

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

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

P.Config-Items: The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed or used at the site as well as the received and transferred and/or provided items.

The configuration management may rely completely on the naming and identification of the received configuration items. In this case at least the consistency with the expected values must be verified and the unique identification must be ensured. This holds also for test programs or other items that are provided to the site for local use. For configuration items that are created, generated or developed at

the site the naming and identification must be specified. For data like configuration or initialization the identification and handling must be described.

P.Config-Control: The procedures for setting up the production and development process for a new product as well as the procedure that allows changes of the initial setup for a product is only applied by authorized personnel. Automated systems support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial setup of a production and development process ensures that sufficient information is provided by the internal client.

The product setup may include the following information, but these shall be changed uniquely by authorized methods in production and development methods:

- Identification of the product,
- Properties of the product when received at the site,
- Properties of the product when internally shipped,
- Classification of the items (which are security relevant),
- Who (either name of the site or the internal client) is responsible for destruction of defect devices,
- Any configuration of the processed item as part of the services provided by the site,
- Which address is used for internal shipment.

P.Config-Process: The services and processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development and production of the product and optimizations of the process flow as well as the documentation that describes the services and processes provided by the site. A released production and development process is defined and under version control.

At least the documentation that includes the process descriptions and the security measures of the site must be under version control. Measures should be in place to ensure that the evaluated status is ensured. In most cases tools are used to support the production of the site. This may comprise e.g. scripts or batch routines developed by the site or a commercial data base system. This can also comprise service levels or quality parameters.

P.Reception-Control: The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the internal client. Furthermore, it is verified that the intended TOE can be identified and a released production process is defined for the intended TOE. If applicable this aspect includes the check that all required information and data is available to handle the incoming items.

P.Accept-Product: The testing and quality control of the site ensures that the released intended TOE comply with the specification agreed with the internal client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the assets. Thereby, it is ensured that the properties of the intended TOE are ensured when internally shipped.

P.Zero-Balance: The site ensures that all sensitive items (security relevant parts of the intended TOEs of different internal clients) are separated and traced on a device basis. For each handover, either an automated or an organizational “two employees-acknowledgement” (four-eyes principle) is applied for functional and defect assets. As per the released production process the defect assets are either collected at the site or sent back to the internal client.

The following policy covers the packing and handover of products at the site after the applied production flow. A destruction process is mandatory and it must be agreed between the internal client and the site who is responsible for the destruction of defect devices. If the destruction is performed by the internal client, the zero-balancing must be appropriately extended.

P.Product-Transport: Technical and organizational measures ensure the correct labeling of the intended TOE. A controlled internal shipment is applied. The transport supports traceability up to the recipient. If applicable or required, this policy includes measures for packing to protect the product during transport.

The following policy supports the electronic transfer of sensitive assets as specified in Section 3.1.

P.Secure-Scrap: Controls are in place when the forwarder indicated by the internal 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: Any data in electronic form (e.g. product specification, release information etc.) that is classified as sensitive or higher security level by the internal client is encrypted to ensure confidentiality of the data.

Confidential / sensitive data transfers in electronic form must be sent in a signed, encrypted and secure manner. All sensitive configuration or information (include product specification, test programs, test program specification, etc.) is also encrypted to ensure security before sending out to internal clients through email.

3.4 – Assumptions

The site operating in a production flow, it must rely on preconditions provided by the previous site. This is reflected by the assumptions that must be defined for the interface.

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

A.Prod-Specification: The internal client must provide appropriate information (e.g. specification, definitions, process limits, process parameters, test requirements, test limits, bond plans) to ensure an appropriate development or production process. The provided information includes the classification of the documents and product.

Depending of the site activities, further assumptions may be required (e.g. if the site ships the product to the consumer the related information must be transferred or if the site receives data from the internal client for the configuration the integrity if the data must be ensured. Furthermore, depending on the status of the assets an assumption on the already operational self-protection of the product may be added to the rationale of the required security measures.

A.Item-Identification: Each configuration item received by the site is appropriately labelled to ensure the identification of the configuration item.

A.Internal-Shipment: The recipient (internal client) of the product is identified by the address of the internal client site. The address of the internal client is part of the product setup. The internal client provides the address and shipping information via secure channel to HHWX.

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

A.Destruct-Scrap: Scrap assets are also transferred and they are destructed at on site so that they are useless for an attacker.

4. Security Objectives

4.1 – Security Objectives definition

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

O.Physical-Access: The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows enough separation of employees to enforce the “need-to-know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. The site enforces two or three levels of access control to sensitive areas of the site. The access control measures ensure that only registered employees and registered visitors can access restricted areas. Sensitive products and data are handled in restricted areas only. Network cabling is protected according to classification of the transferred data by avoiding routes through public areas or by usage of appropriate cryptographic measures.

Special access control measure with a high efficiency is implemented, which is allowed only two access control levels. Special measures mean checking of PIN, fingerprint or similar authentication mechanisms in addition to a badge.

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

O.Alarm-Response: The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still must overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack. The areas which are not permanently manned by employees or guards are under permanent alarms.

O.Internal-Monitor: The site performs weekly security management meetings. The security management meetings are used to review security incidents, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. In addition, quarterly meetings are organized to discuss about security metrics and events. Furthermore, an internal audit is performed annually to control the application of the security measures. Sensitive processes may be controlled within a shorter time frame to ensure enough protection.

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

O.Logical-Access: The site implements a firewall system to enforce a logical separation between the internal network and the internet. The firewall system ensures that only defined services and defined connections are accepted. Furthermore, the internal network is separated into production, office and administration networks. Specific networks for production and administration are further logically separated from other internal network to enforce access control. Access to the production network and related system is restricted to authorized employees involved in the configuration tasks of the production systems. Every user of an IT system has its own user account and password. An authentication using a unique user account and password is enforced by all computer systems. The implementation is defined on the protection needs of the data related to the provided processes. For the different networks, different coordinated protection levels are available. User accounts and associated user authentication are defined for network segments transferring sensitive data.

O.Logical-Operation: All network segments and the computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection, etc.). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data. The backup handles the same or equivalent logical and physical protection as the data used for processing.

O.Config-Items: The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify configuration items and allow an assignment to the internal client. Also, the internal procedures and guidance are covered by the configuration management.

O.Config-Control: The site applies a release procedure for the setup of the production and development process for each new product. In addition, the site has a process to classify and introduce changes for services and processes of released products. Minor changes are handled by the site; major changes must be acknowledged by the internal client. A designated team is responsible for the release of new products and for the classification and release changes. This team comprises specialists for all aspects of the services and processes. The services and processes can be change by authorized personnel only. Automated systems support configuration management and production control.

O.Config-Process: The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the production of the product and optimizations of the process flow as well as for the documentation that describes the services and processes provided by a site.

O.Acceptance-Test: The site delivers assets that fulfill the specified properties. Parameter checks, functional and visual check and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.

O.Staff-Engagement: All employees who have access to sensitive assets and who can move parts of the products out of the defined production and development flow are checked regarding security concerns and have to sign a contract confidentiality clause. The security controls operated on employees include among others a criminal background check. Furthermore, all employees are trained and qualified for their job.

O.Zero-Balance: The site ensures that all sensitive products (intended TOE of different internal clients) are separated and traced on a device basis. Automated control and/or two employees' acknowledgment

during hand-over is applied for functional and defective devices. According to the agreed production or development flow the defect devices are either destroyed at the site or sent to the internal client or the consumer.

O.Reception-Control: Upon reception of any intended TOE and immediate incoming inspection is performed. The inspection comprises the received amount, their identification and the assignment of the items to a related internal process.

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

O.Transfer-Data: Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure the confidentiality and the integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected. The O.Transfer-Data is applicable for internal shipment of such data as well.

O.Control-Scrap: The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive assets so that they do not support an attacker. The measures in place includes also that the site returns the assets to be scrapped to the stakeholder, according to the secure shipment procedure of the stakeholder. Sensitive assets can be transferred with the functional devices to be destructed at another site. In such case, this is addressed within assumptions for the other site.

4.2 – Security Objectives Rationale

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

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

Threats & OSP	Security Objective	Justification
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The justification of structural technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. O.Physical-Access ensures that the sensitive areas are physically portioned and access restricted, so an unauthorized person cannot just walk-in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a sensitive area. O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response will be given to the alarm systems and that the response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Smart-Theft.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. O.Physical-Access ensures that the sensitive areas are physically partitioned and access restricted, so an unauthorized person cannot just walk-in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a sensitive area. O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response will be given to the alarm systems and that the response is quick enough to prevent access to the assets. O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Rugged-Theft.

T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are secured (such as login and password) to restrict access to. O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up to date (software updates, security patches, virus, spyware protection, etc.). O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Computer-Net.
T.Accident-Change	O.Logical-Access O.Logical-Operation O.Config-Items O.Config-Control O.Zero-Balance O.Staff-Engagement O.Acceptance-Test	Automated measures and control procedures allow preventing accidental changes on sensitive items. O.Logical-Access ensures that the networks are protected with firewall to prevent external or internal unauthorized access and that machines are secured (such as login and password) to restrict access to. O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up to date (security patches, virus, spyware protection, etc.). O.Config-Items ensures that all configuration items for secure products are identified. O.Config-Control ensures that sites procedures for manufacturing are known and followed for the operations. O.Zero-Balance ensures that all items are traced and accounted for. O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Acceptance-Test to ensure that the products to be returned to the internal clients are compliant with their specifications. Together, these objectives will therefore counter T.Accident-Change.

T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Config-Control O.Zero-Balance O.Control-Scrap	Physical and logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets. O.Physical-Access ensures that the sensitive areas are physically partitioned and access restricted, so an unauthorized person cannot just walk-in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a sensitive area. O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response will be given to the alarm systems and that the response is quick enough to prevent access to the assets. O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are secured (such as login and password) to restrict access to. O.Logical-Operation ensures that all computer systems used to manage the overall network are kept-up to date (software updates, security patches, virus, spyware protection, etc.). O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party. O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the operations. O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Unauthorised-Staff.

T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Zero-Balance O.Control-Scrap O.Transfer-Data	The application of internal security measures combined with the hiring policies that restrict to trust-worthy employees limits unauthorized access to assets. O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party. O.Transfer-Data ensures the integrity of the secure shipment of the data. O.Internal-Monitor and O.Maintain-Security ensure that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Staff-Collusion.
T.Attack-Transport	O.Internal-Shipment O.Transfer-Data O.Staff-Engagement O.Internal-Monitor	The application of internal shipment policy ensures that the zero-balance principle is correctly applied. O.Internal-Shipment ensures the traceability and security of products during internal transport. O.Transfer-Data ensures the integrity of the secure delivery of data. O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Internal-Monitor ensures that the above security objectives are managed and maintained. Together, these objectives will therefore counter T.Attack-Transport.
P.Config-Items	O.Reception-Control O.Config-Items	O.Reception-Control ensures an immediate identification of the product. The Security Objective O.Config-Items directly enforces the OSP. O.Config-Items ensures that all configuration items for secure products are identified. Together, these objectives will therefore covers P.Config-Items.

P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	Network and Logical (O.Logical-Access) protection and the usage of configuration management tools by authorized people ensure the OSP. O.Config-Items ensures that all configuration items for secure products are identified. O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the development and manufacturing operations. Together, these objectives will therefore cover P.Config-Control.
P.Config-Process	O.Config-Process	The security objective enforces directly this OSP.
P.Reception-Control	O.Reception-Control	The security objective enforces directly this OSP.
P.Accept-Product	O.Config-Control O.Acceptance-Test O.Config-Process	Application of a configuration management plan and change management monitored by authorized people ensure that the intended TOE is conformant to the accepted one by the internal client. O.Config-Control ensures that sites procedures for development and manufacturing are known and followed for the development and manufacturing operations. O.Acceptance-Test to ensure that the products to be returned to the internal clients are compliant with their specifications. O.Config-Process ensures that configuration management is used and applied for sites services control.
P.Zero-Balance	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance O.Control-Scrap	All assets are traced internally until their possible destruction (O.Zero-Balance, O.Control-Scrap) by trained and authorized person (O.Staff-Engagement) to enforce the OSP. O.Staff-Engagement ensures that all staff is aware of its responsibilities. O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party. O.Internal-Monitor ensures that the above security objectives are managed and maintained. Together, these objectives will therefore counter P.Zero-Balance.

P.Product-Transport	O.Config-Process O.Internal-Shipment O.Transfer-Data	Appropriate procedures for internal and external shipment ensure correct labeling and traceability until the recipient. O.Config-Process ensures that configuration management is used and applied for sites services control. O.Internal-Shipment ensures the traceability and security of products during internal transport. O.Transfer-Data ensures the integrity of the secure shipment of the data. Together, these objectives will therefore counter P.Product-Transport.
P.Secure-Scrap	O.Security-Control O.Zero-Balance O.Control-Scrap	Appropriate procedures for zero balance to ensure that no secure product is lost or theft. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a secure room. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorised party. O.Zero-Balance ensures that all items are traced and accounted for. Together, these objectives will therefore counter P.Secure-Scrap.
P.Data-Transfer	O.Transfer-Data	The security objective enforces directly the OSP.

Tableau 2: Mapping of Security Objectives

5. Extended Assurance Components Definition

No extended components are currently defined in this SST.

6. Security Assurance Requirements

Internal clients using this Site Security Target require a TOE evaluation up to evaluation assurance level EAL6, potentially claiming conformance with the Protection Profiles [1] and [2].

The Security Assurance Requirements (SAR) are chosen from the class ALC (Life-cycle support) as defined in [4]:

- CM Capabilities (ALC_CMC.5),
- CM Scope (ALC_CMS.5),
- Developer Environment Security (ALC_DVS.2),
- Development Life-cycle Definition (ALC_LCD.1),

The Security Assurance Requirements listed above fulfill the requirements of [9] because hierarchically higher components are used in this Site Security Target.

6.1 – Application Notes and Refinements

The description of the sites certification process in [9] 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 term “TOE” is not applicable in the SST the associated processes 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:

- CM Capabilities
  - Section 5.1 in [9], “Application Notes for ALC_CMC”, for the relevant application notes.
- CM Scope
  - Section 5.2 in [9], “Application Notes for ALC_CMS”, for the relevant application notes.
- Development Security
  - Section 5.4 in [9], “Application Notes for ALC_DVS”, for the relevant application notes.
- Life-cycle Definition
  - Section 5.6 in [9], “Application Notes for ALC_LCD”, for the relevant application notes.

6.2 - Security Assurance Rationale

Since this SST references the PP [1] and [2], the life-cycle module used in this PP includes also the processes provided by these sites. Therefore, the life-cycle module described in the PP [1] and [2] is considered to be applicable for this site.

The Security Assurance Rationale maps the content elements of the selected assurance components to the Security Objectives defined in this SST. The refinements described Section Extended Assurance Components Definition.

Tableau 3: Mapping and Rationale for ALC_CMC

SAR	Security Objective	Rational	Reference
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 O.Config-Control O.Reception-Control O.Config-Process	The TOE is labeled with its unique reference by the configuration management system as defined by O.Config-Items and O.Config-Control. O.Reception-Control ensures the product identification and the associated labeling. O.Config-Process provides a configured and controlled production process. The method used to uniquely identify the configuration items is described in the configuration management documentation. Each item is assigned a unique identifier (O.Config-Items). The configuration items are tracked throughout the life-cycle (O.Config-Control). Incoming inspection according O.Reception-Control ensures product identification and the associated labeling. O.Config-Process provides a configured and controlled production process.	WIMR-QRA-1107 HSM-1000 WGM-TDDS-0003
ALC.CMC.5.2C: The CM documentation shall describe the method used to uniquely identify the configuration items.	O.Config-Control O.Config-Items O.Reception-Control O.Config-Process	The method used to uniquely identify the configuration items is described in the configuration management documentation. Each item is assigned a unique identifier (O.Config-Items). The configuration items are tracked throughout the life-cycle (O.Config-Control). Incoming inspection according O.Reception-Control ensures product identification and the associated labeling. O.Config-Process provides a configured and controlled production process.	WIMR-QRA-1107 HSM-1000 WGM-TDDS-0003

ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-Items O.Config-Control O.Reception-Control O.Config-Process	O.Config-Items comprises the internal unique identification of all items. 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. O.Config-Process ensures that only authorized staff can apply changes. This comprises changes related to process flows, procedures and items of internal clients. Teams are defined to assess and release changes.	WISQ-0035 WGM-TDDS-0003 HSM-1000 WIEM-0004
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 comprises the internal unique identification of all items. Each item is setup according to O.Config-Control comprising all necessary items. O.Reception-Control comprises the incoming labeling and the mapping to internal identification.	WISQ-0035 WGM-TDDS-0003
ALC_CMC.5.5C: The CM system shall provide automated controls such that only authorized changes are made to the configuration items.	O.Config-Control O.Config-Process O.Logical-Access O.Logical-Operation	The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures such that only authorized change are made to the configuration items (O.Config-Control). Access is controlled such that only authorized users may make changes (O.Logical-Access). An authentication is necessary to get access to the system (O.Logical-Access). The configuration management system manages all relevant assets (O.Config-Items).	WISQ-0035 WGM-TDDS-0003 HSM-1000 WIEM-0004
ALC_CMC.5.6C: The CM system shall support the production of the TOE by automated means.	O.Config-Process O.Zero-Balance O.Acceptance-Test	O.Config-Process comprises the automated management of the production processes. O.Zero-Balance ensures the control of all security products during production. The site provides automated tools for the development activities and procedures for their uses regarding O.Acceptance-Test.	WISQ-0035 HSM-1000 WGM-TDDS-0003

ALC_CMC.5.7C: The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O.Reception-Control O.Logical-Access	O.Reception-Control ensures the reception procedure of the logical assets from the internal client. The person responsible for accepting the logical assets cannot be the developer. O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorized staff.	WGM-TDDS-0003 WHSM-2004 HSM-2013 WISQ-0035
ALC_CMC.5.8C The CM system shall *clearly* identify the configuration items that comprise the TSF.	O.Config-Items O.Config-Control O.Config-Process	The CM System identified the configuration items part of the TOE. It is labelled with its unique reference by the configuration management system as defined by O.Config-Items and O.Config-Control. According to O.Config-Process the CM plan describes the services provided by the site.	WISQ-0035 WGM-TDDS-0003
ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.	O.Config-Items O.Config-Control O.Config-Process O.Acceptance-Test	The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures such that change are properly recorded to the configuration items (O.Config-Items and O.Config-Control). O.Config-Process ensures that only authorized staff can apply changes. This comprises changes related to process flows, procedures and items of internal clients. Teams are defined to assess and release changes. The site provides automated tools for the development activities and procedures for their uses regarding O.Acceptance-Test.	WGM-TDDS-0003 WHSM-2004 WISQ-0014 HSM-1000 WISQ-0035

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-Items O.Config-Control O.Config-Process	The configuration management system is used in accordance with the documented processes. The configuration management system provides automated measures such that change are properly recorded to the configuration items (O.Config-Items and O.Config-Control). O.Config-Process ensures that changes related to process flows, procedures and items of internal clients are properly recorded through the process.	WISQ-0035 WISQ-0014 WGM-TDDS-0003
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated.	O.Reception-Control O.Config-Items O.Logical-Access O.Config-Control O.Config-Process	O.Reception-Control comprises the incoming labeling and the mapping to internal identification. The configuration management system provides automated measures such that change are properly recorded to the configuration items (O.Config-Items and O.Config-Control). O.Logical-Access supports the control by limiting the access and ensuring the correct operation for all asks to authorized staff. O.Config-Process ensures that the versions are properly recorded through the process.	WISQ-0035 HSM-1000 WGM-TDDS-0003
ALC_CMC.5.12C : The CM documentation shall include a CM plan.	O.Config-Control O.Config-Process	The configuration management plan is described in the life-cycle documentation (O.Config-Process). The configuration management system is supported by O.Config-Control.	WISQ-0035
ALC_CMC.5.13C : The CM plan shall describe how the CM system is used for the development of the TOE.	O.Config-Control O.Config-Process	The configuration management plan is described in the life-cycle documentation (O.Config-Process). The configuration management system is supported by O.Config-Control.	WISQ-0035

ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.	O.Config-Control O.Config-Process O.Reception-Control O.Config-Items	O.Reception-Control supports the identification of configuration items. The configuration management system provides automated measures such that the identification and the acceptance process (O.Config-Items and O.Config-Control). O.Config-Process ensures the automated controls of released items.	WGM-TDDS-0003 WHSM-2004 HSM-2013 WISQ-0035
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Reception-Control O.Config-Control O.Config-Process O.Zero-Balance O.Internal-Shipment	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that items are maintained under the CM systems. O.Zero-Balance ensures the control of all security products during production. O.Internal-Shipment includes the packing requirements, the reports and notifications including the required evidences.	WISQ-0035 HSM-1000 WGM-TDDS-0003
ALC_CMC.5.16C: *The evidence shall demonstrate that all the configuration items have been and are being maintained under the CM system.*	O.Config-Control O.Config-Process O.Internal-Shipment	O.Config-Control comprises a release procedure as evidence. O.Config-Process ensures the compliance of the process. O.Internal-Shipment ensures the security shipment requirements are covered.	WISQ-0035 HSM-1000 WGM-TDDS-0003

The security assurance requirements of the assurance requirements of the assurance class “CM capabilities” listed above are suitable to support the development of complex products 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 supports the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

The scope of the evaluation according to the assurance class ALC_CMS comprises the security products, the complete documentation of the site provided for the evaluation and the configuration as well as associated tools. The specifications and descriptions provided by the internal client are not part of the configuration management at HHWX.

Tableau 4: Mapping and Rationale for ALC_CMS

SAR	Security Objective	Rational	Reference
ALC_CMS.5.1C: *The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.*	O.Config-Items O.Config-Control O.Config-Processs	The method used to uniquely identify the configuration items is described in the configuration management documentation.	WIMR-QRA-1107
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control O.Config-Process O.Reception-Control O.Internal-Shipment	Items are uniquely identified by the configuration management system according to O.Config-Items. The configuration items are tracked throughout the life-cycle (O.Config-Control). O.Config-Process ensures the compliance of the process. The identification of received products is defined by O.Reception-Control. The identification and preparation of items for shipment is defined by O.Internal-Shipment.	WIMR-QRA-1107
ALC_CMS.5.3C: For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	HHWX does not involve contractor for the TOE development. According to O.Config-Items all configuration items for secure products are identified.	WISQ-0035

The security assurance requirements of the assurance class “CM Scope” listed above support the control of the production and test environment. This includes product related documentation and data as well as the documentation of the configuration management and the security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these assurance requirements are suitable.

Tableau 5: Mapping and Rationale for ALC_DVS

SAR	Security Objective	Rational	Reference
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.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap O.Reception-Control O.Internal-Shipment O.Transfer-Data	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation. The reception and incoming inspection supports the detection of attacks during the transport of the security products HHWX according to O.Reception-Control. The shipment to internal client is protected by similar measures according to the requirements of the internal client based on O.Internal-Shipment. Sensitive data received by HHWX is encrypted according O.Transfer-Data to ensure access by authorized recipients only.	WHSM-2004 HSM-1000 HSM-1001 HSM-2013 HSM-2014
ALC_DVS.2.2C: The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Zero-Balance	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitoring, O.Logical-Operation and O.Maintain-Security. All devices including functional and non-functional are traced according to O.Zero-Balance.	WIEM-0004 WIEM-0038 HSM-2001 HSM-2010

ALC_DVS.2.3C : The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Reception-Control O.Internal-Transport O.Transfer-Data	The reception and incoming inspection supports the detection of attacks during the transport of the security products to the sites according to O.Reception-Control. The shipment to the internal client is protected by similar measures according to the requirements of the internal client based on O.Internal-Shipment. Sensitive data received and send by the sites are encrypted according to O.Transfer-Data to ensure access by authorized recipients only.	WIEM-0004 WIEM-0038 HSM-2001

The security assurance requirements of the assurance class “Development Security” listed above are required since a high attack potential is assumed for potential attackers. The assets and information handled at the site during production and testing of the product can be used by potential attacker for the development of attacks. Further on the Protection Profile [1] and [2] requires this protection for sites involved the life-cycle of Security ICs production.

Tableau 6: Mapping and Rationale for ALC_LCD

SAR	Security Objective	Rational	Reference
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 identification and manufacturing are covered by O.Config-Control and O.Config-Process.	WISQ-0035 WGM-TDDS-0003
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.Zero-Balance	The life-cycle documentation describes the governance that provides for the necessary control over the development and maintenance of the TOE through O.Config-Process and O.Zero-Balance	HSM-2014 WGM-TDDS-0003 WHSM-2004

The security assurance requirements of the assurance class “Life-cycle definition“ listed above are suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. One site provides only a limited support of the described life-cycle for the development and production of Security ICs. However,

the assurance requirements are suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

6.3 – Dependencies

The dependencies of the assurance requirements are as followed:

Tableau 7: Dependencies mapping

	ADV_FSP.2	ADV_FSP.4	ADV_IMP.1	ADV_TDS.1	ADV_TDS.3	ALC_CMS.1	ALC_DVS.1	ALC_LCD.1	ALC_TAT.1
ALC_CMC.5						x	x	x	
ALC_CMS.5									
ALC_DVS.2									
ALC_LCD.1									

Regarding the Assurance Life-Cycle are as followed (as detailed in the table above):

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

Some of the dependencies are not completely fulfilled which is described below. ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1 are only partially fulfilled as the site does not represent the entire development process.

7. Site Summary Specification

7.1 – Preconditions Required by the Sites

The sites perform the data preparation and the wafer manufacturing including the failure analysis and reliability assurance. In order to perform these services in a secure way, the internal client of the site needs to support the security processes of the site. The following paragraphs describe preconditions of the client to perform the aforementioned services.

For the setup and control of the production process, the appropriate specification and relative production information is provided by the client. Specific requirements for classified design data must also be defined and uniquely identified including the identification of encrypted files.

The released production process includes the tool configuration and set-up for the wafer manufacturing. The released production process further includes the parameters and limits that must be fulfilled by the wafers.

For the shipment of security product, the recipient of the masks is identified by the address of the respective sites. The packing of wafers and preparation of the shipment adhere to the standard procedure of the sites, unless the specific requirement form the client. The client is responsible for delivery and transfer of the masks including the selection of the forwarder and the provision of data for the verification of the transport order.

Details of the preconditions and requirements required by the client are summarized in the corporate documentation. The documents shall be handed out to the client in order to provide information about the secure incorporation of HHWX site into the client’s production process.

Tableau 8: Preconditions of assumptions

7.2 – Services of the Site

Services	Details
Data preparation	• GDS file reception and preparation • Shipment GDS file to Mask-shop/customer
Wafer Manufacturing	• Mask reception • Wafer production • Wafer Storage & delivery • Mask & Wafer Scrap
Failure analysis and reliability assurance	• Verification and validation processes through failure analyses test
Supporting services	• Human resources local management, • Physical security, • Facilities management.

7.3 – Objectives Rationale

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

O.Physical-Access: The site implements a “need-to-know” principle by separation measures using a combination of physical partitioning together with technical and organizational security measures. The access control measures support the enforcement of the separation and the “need-to-know” principle. The handling of assets is restricted to separates security areas. By the combination of these measures the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Security-Control: The site is using dedicated personnel for guard services. These personnel are responsible for operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incidents and the hosting of visitors. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorised-Staff and it addresses P.Secure-Scrap.

O.Alarm-Response: In case of an access attempt to an asset by an unauthorized person the site has an alarm system in place. After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees and/or guards is short enough to prevent a successful attack. By the combination of these measures, the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorised-Staff can be prevented.

O.Internal-Monitor: The established security measures of the site are regularly reviewed by security management meetings and internal audits. This helps to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion, T.Attack-Transport and it addresses P.Zero-Balance.

O.Maintain-Security: Technical security measures are maintained regularly. This ensures that the systems are working correctly and are configured as required to ensure the protection of the networks and computer systems. In addition, all employees are trained regularly. Hence, this helps to prevent the threats: T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorised-Staff, T.Staff-Collusion.

O.Logical-Access: The development network is strictly separated from the other internal networks and the internet by using firewalls. The different projects inside the developer network are separated by logical directory structure. The access to the different project information is protected by personal credentials. By considering the “need-to-know” principle, only authorized person has access to the project relating information. Each user has her/his own user account. Based on their classification assets are in addition only processed in the according logical security area with regard to the implemented access security measures. It prevents the threats T.Computer-Net, T.Unauthorised-Staff, T.Accident-Change and it addresses P.Config-Control.

O.Logical-Operations: The used workstations for development purposes are using authentication measures for the users of these systems. Authentication may include multi-factor authentication depending on the type of the development workstation. It prevents the threats T.Computer-Net, T.Unauthorised-Staff and T.Accident-Change.

O.Config-Items: A configuration management system is in use which manages all TOE relating hardware, software and information. Each item gets an internal unique identification. The threats T.Accident-Change is prevented and the security policy P.Config-Items and P.Config-Control are fulfilled.

O.Config-Control: Procedures arrange for a formal release of configuration documents and specifications for set-up of wafer production. The information is also stored in the configuration database. Engineering Change Procedures are in place to classify and introduce changes. The system tool requires personalized access controlled. Each user has access-rights limited to the needs of her/his function. Thereby only authorized changes are possible. It addresses the threats T.Unauthorised-Staff and T.Accident-Change. It supports P.Config-Control, P.Accept-Product.

O.Acceptance-Test: Items quality and acceptance tests are introduced and released based on the related specifications. The tools, specifications and procedures for these test are controlled. It supports P.Accept-Product and it covers T.Accident-Change.

O.Staff-Engagement: The site has established personnel security measures: all employees who have access to assets are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. This helps to prevent the threats T.Computer-Net, T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion, T.Attack-Transport. It addresses P.Zero-Balance.

O.Config-Process: The configuration items are tracked throughout the life-cycle of the TOE. The procedures may be detailed in the CM plan. It prevents the security policies P.Config-Process, P.Accept-Product, P.Product-Transport.

O.Zero-Balance: The site execute zero balancing to monitor that no secure object gets lost onsite or during transport. Therefore, the amount of incoming and outgoing objects is managed and monitored by

the CM system. This helps to prevent the threat T.Unauthorised-Staff, T.Staff-Collusion, T.Accident-Change. It prevents the security policy P.Zero-Balance and P.Secure-Scrap.

O.Transfer-Data: For secure data transfer, transport are handled over to the internal client. All secure information is transferred encrypted form. The internal client gets informed if a new release is available. Furthermore, technical measures like cryptography, separation network, split access permission and secure storage shall be implemented for this kind of data. This helps to prevent threats T.Staff-Collusion and T.Attack-Transport. It prevents the security policy P.Product-Transport and P.Data-Transfer.

O.Internal-Shipment: All necessary information regarding the transport has to be shared during the project setup with the internal client. All received objects are entered in the configuration management system for traceability. This helps to prevent threat T.Attack-Transport and it addresses the OSP P.Product-Transport.

O.Reception-Control: At reception each configuration item including security products are identified by the shipping documents, labels and information in the system. Inspection at reception is counting the amount of items and checking the shipping list if applicable. Thereby only correctly identified items are accepted. The OSP P.Config-Items and P.Reception-Control are addressed.

O.Control-Scrap: Scraps are stored internally in a secure location. They are destructed in a controlled and documented way. The destruction of items is done under supervision of qualified employees. It addresses the threats T.Unauthorised-Staff and T.Staff-Collusion. This addresses OSP P.Zero-Balance and P.Secure-Scrap.

7.4 – Assurance Measures Rationale

O.Physical-Access:

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.

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.

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.

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.

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 and implementation in its development and production environment.
- 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-Access:

- ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development and production environment.
- ALC_CMC.5.5C requires that the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.7C requires that the CM system support the production of the TOE by automated means. Thereby this objective contributes to meet the Security Assurance Requirement.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.

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 and implementation in its development and production environment.
- ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.
- ALC_CMC.5.5C requires that the CM system provide automated measures such that only authorized changes are made to the configuration items.

O.Config-Items:

- ALC_CMC.5.1C requires that the TOE is labeled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.

- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.14C requires the CM plan to describe 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 item is indicated in the configuration list.

O.Config-Control:

- ALC_CMC.5.1C requires that the TOE is labeled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.
- ALC_CMC.5.5C requires the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.

- ALC_CMC.5.12C requires that the CM documentation provide a CM plan.
- ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the 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 documentation describes the model used to develop and maintain the products.

O.Config-Process:

- ALC_CMC.5.1C requires that the TOE is labeled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.5C requires the CM system provide automated measures such that only authorized changes are made to the configuration items.
- ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means.
- ALC_CMC.5.8C requires the CM system to identify the configuration items that comprise the TSF.
- ALC_CMC.5.9C requires the CM system to support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail.
- ALC_CMC.5.10C requires the CM system to provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.12C requires that the CM documentation provide a CM plan.

- ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.
- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- 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.

O.Acceptance-Test:

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

O.Staff-Engagement:

- 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.

O.Zero-Balance:

- ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.
- ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

O.Reception-Control:

- ALC_CMC.5.1C requires that the TOE is labeled with its unique reference.
- ALC_CMC.5.2C requires that the CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.5.3C requires that the CM documentation justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
- ALC_CMC.5.4C requires that the CM system provides a uniquely identification to all configuration items.
- ALC_CMC.5.7C requires that the CM system support the production of the TOE by automated means. Thereby this objective contributes to meet the Security Assurance Requirement.
- ALC_CMC.5.11C requires that the CM system identifies the versions of the implementation representation from which the TOE is generated.
- ALC_CMC.5.14C requires the CM plan to describe the procedures used to accept modified or newly created configuration items as part of the TOE.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.3C.
- 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. This includes also the protection during the transport between production sides
- ALC_DVS.2.3C: requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and the integrity of the product.

O.Internal-Shipment:

- ALC_DVS.2.1C requires that the developer shall describe all physical security measures, 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. This includes also the protection during the transport between production sides.
- ALC_CMC.5.15C requires an evidence, which demonstrate that all configuration items are being maintained under the CM system.
- ALC_CMC.5.16C requires an evidence, which demonstrate that the CM system is being operated in accordance with the CM plan.
- ALC_CMS.5.2C according the unique identification of the packing as configuration item.
- ALC_DVS.2.3C: requires that the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and the integrity of the product.

O.Control-Scrap:

- 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. This includes also the protection during the transport between production sides.

O.Transfer-Data:

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

8. Documentation references

Reference	Definition
[1]	Eurosmart Security IC Platform Protection Profile with Augmentation Packages, version 1.0, BSI-CC-PP-0084-2014
[2]	Secure Sub System in System-on-Chip (3S in SoC) Protection Profile, version 1.5, BSI-CC-PP-0117
[3]	Common Criteria for Information Technology Security Evaluation, part 1: Introduction and General Model; CC:2022, Revision 1, CCMB-2022-11-001, November 2022
[4]	Common Criteria for Information Technology Security Evaluation, part 3: Security Assurance Requirements; CC:2022, Revision 1, CCMB-2022-11-003, November 2022
[5]	Common Criteria for Information Technology Security Evaluation, part 4: Framework for the Specficiation of Evaluation Methods and Activities; CC:2022, Revision 1, CCMB-2022-11-004, November 2022
[6]	Common Criteria for Information Technology Security Evaluation, part 5: Pre-Defined Packages of Security Requirements; CC:2022, Revision 1, CCMB-2022-11-005, November 2022
[7]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology; CEM:2022, Revision 1, CCMB-2022-11-006, November 2022
[8]	Minimum Site Security Requirements, V2, March 2025
[9]	Supporting Document, Site Certification, October 2007, Version 1.0, Revision
[10]	Site Security Target Template, Eurosmart, version 2.0, April 2021

Tableau 9: References

9. Deliverable references

Reference	Name
WISQ-0035	Secure Product Management
WHSM-2004	HHWX Physical Access Regulation
HSM-1000	Information Security Management System Manual
HSM-1001	Information Security Statement of Applicability (SOA)
WIEM-0004	Internal System Audit Regulation
WIEM-0038	Nonconformity Corrective Action Management Regulation
HSM-2001	Information Security Risk Assessment Management Regulations
WGM-TDDS-0003	The internal handling guideline for HHWX Security Products of Design Support Division
HSM-2013	User Access Control Procedure
HSM-2014	Encryption Control Management Regulation
HSM-2010	Information Security Incidents Management Regulation
WISQ-0014	Production Identification and Traceability Management Procedure
WIMR-QRA-1107	Site_HHWX_2025_Configuration List