Table of Contents

1. SST Introduction ..... 3
1.1 SST Reference and Site Reference ..... 3
1.1.1 SST Reference ..... 3
1.1.2 Site Reference ..... 3
1.2 Site Description ..... 3
1.2.1 Physical Scope of the Site ..... 3
1.2.2 Logical Scope of the Site ..... 4
2. Conformance Claims ..... 5
3. Security Problem Definition ..... 6
3.1 Asset ..... 6
3.2 Threats ..... 6
3.3 Organizational Security Policies ..... 8
3.4 Assumptions ..... 10
4. Security Objectives ..... 12
4.1 Security Objective Definition ..... 12
4.2 Security Objectives Rationale ..... 15
5. Extended Components Definition ..... 18
6. Security Assurance Requirements ..... 18
6.1 Application Notes and Refinements ..... 19
6.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC) ..... 19
6.1.2 Overview and Refinements regarding CM Scope (ALC_CMS) ..... 19
6.1.3 Overview and Refinements regarding Development Security (ALC_DVS) ..... 20
6.1.4 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD) ..... 20
6.2 Security Assurance Rationale ..... 20
7. Site Summary Specification ..... 29
7.1 Preconditions Required by the Site ..... 29
7.2 Services of the Site ..... 29

7.3 Objectives Rationale ....30
7.4 Security Assurance Requirements Rationale ....35
7.4.1 ALC_CMC.5 ....35
7.4.2 ALC_CMS.5 ....37
7.4.3 ALC_DVS.2 ....37
7.4.4 ALC_LCD.1 ....37
7.5 Assurance Measure Rationale ....38
7.6 Mapping of the Evaluation Documentation ....42
8. Reference ....42
8.1 Literature ....42
8.2 Definitions ....43
8.3 Abbreviations ....43

List of Tables

Table 3.1 OSP addressed by the Site ....10
Table 3.2 Assumptions for the Client ....12
Table 4.1 Security Objectives for the Site ....14
Table 4.2 Mapping Security Objectives ....17
Table 6.1 Security Assurance Rationale ....25
Table 7.1 Mappings among the Security Objectives, and Threats / OSPs ....35
Table 8.1 Abbreviations Table ....43

# 1. SST Introduction

The SST describes security features of the site and defines the scope of the site. This chapter is divided into two sections “SST reference and Site reference” and “Site description”.

## 1.1 SST Reference and Site Reference

### 1.1.1 SST Reference

Title: Site Security Target Lite of Mask Operation of Semiconductor Manufacturing International (Shanghai) Corporation

Site: Mask Operation of Semiconductor Manufacturing International (Shanghai) Corporation

Product type: Mask Manufacturing

EAL-level: The site supports product assessment up to EAL6

Author: Yingying Han

Version: 0

Publication Date: 2024/06/06

### 1.1.2 Site Reference

Name of the site:

Mask Operation of Semiconductor Manufacturing International (Shanghai) Corporation

Location of SMIC Mask Operation:

NO.18 Zhangjiang Road, Pilot Free Trade Zone, Shanghai, People Republic of China

## 1.2 Site Description

### 1.2.1 Physical Scope of the Site

The site comprises of six buildings, including the block SO1, SO3, SO8, Fab-3B, 9B, CW4. The functionality of each building is described below:

- The building SO1 includes several areas in scope. The IT Server Room (room 01114), Security Control Center #1 (room 01017A) and Finished-Good Warehouse (FGWH) are located at the first floor. The IT critical operation room (room 06063) is located at the sixth floor.
- The building SO3 includes the Security Control Center #2 (room 04136) which is located at the first floor and the Mask Operation Office which is located at the sixth floor, the Mask Operation Server Room (room 337) which is located at the third floor.
- The building SO8 includes Security Control Center #3 (room 1034) which is on the first floor.

- The Fab-3B building includes the Mask Operation Fab facility, located at the first floor. This is the area mainly for mask production.
- The scrapping of masks takes place in the room F9117-B which is on the first floor of the building 9B.
- The Scrap Warehouse (room W4205) is located at the second floor of the CW4 building.

The access control, surveillance and active detectors (if applicable) are adopted to the plants and the buildings for physical protection.

1.2.2 Logical Scope of the Site

Mask Operation of Semiconductor Manufacturing International (Shanghai) Corp provides the services and/or processes covered in the scope of the site evaluation process as follows.

- Encrypted/Decrypted GDS data management
- Security mask manufacturing
- Security mask warehousing and dispatch
- Security mask service (mask remount/recheck, mask repair if be required by Fab)
- Mask scrap management/destruction

More specifically, the client transfers the encrypted GDS files to a FTP server located at SO1 and then the GDS files will be uploaded to a mask server located at SO1. The mask engineer retrieves the GDS files to optimize GDS data to manufacture mask. Based on the mask data in the mask server, the security masks are manufactured in the mask division located at Fab 3B. And the scrap masks will be stored in the building CW4 and destroyed in building 9B.

The site performs the secure shipment to the wafer foundry. It only refers to the internal shipments and/or shipments between sites and not to shipment to customers or end users. Therefore, ALC_DEL is not in the scope of the site.

A part of Life cycle phase 3: IC Manufacturer (according to the Protection Profile [6]) is subject of this SST.

## 2. Conformance Claims

This section describes how the Site Security Target conforms to the Common Criteria.

The evaluation is based on Common Criteria Version 3.1, revision 5

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 [1]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017 [2]

This SST is CC Part3 conformant.

The evaluation follows below methodology:

- Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017 [3]
- Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007 [4]
- JIL-Minimum Site Security Requirements v3.0, February 2020 [5]

The evaluation of the site comprises the following assurance components:

ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1

The assurance level chosen for the SST is compliant to the Protection Profile (PP) [6] and therefore suitable for Security ICs.

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

The site does not directly contribute to the development of the intended TOE and the shipment to the end user. Therefore, ALC_DEL.1 and ALC_TAT.3 are not applicable to the site.

## 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 intended TOE and the security management of the site. The goal is to achieve and hold a high security level to counter attacks with high attack potential at the site.

### 3.1 Asset

Security is concerned with the protection of assets. Internal documentation and data at this site are relevant to maintain the confidentiality and integrity of an intended TOE, including site security concepts and the associated security measures. These items are not explicitly listed in the list of assets below.

The integrity of any machine or tool used for production and testing is not considered as an asset. However, appropriate measures are defined for the site to ensure the correct operation of machines and tools based on regular maintenance and calibration.

The assets are related to the production of security masks as follows.

- Development and implementation data (GDS data, mask data include JDV data & process data)
- Masks
- Scrap masks
- Tamper-proof labels
- Site security documentation, specifications related to the product and the definition of the mask set as well as the detailed production process including optional processes and parameters
- Production relevant data of intended TOE

### 3.2 Threats

The threats at this site are considered as follows.

T.Accident-Change Defines that an employee or contractor may exchange products of different production lots or different clients during production by accident.

Employees or contractors 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 employee or maintenance tasks of contractors within the development, production or test area. Such accidental changes can include the modification of configurations for tools that may have an impact on the TOE, the wrong assignment of tools for a dedicated process step.

T.Attack-Transport defines that an attacker might try to get data, specifications or products during the internal shipment. The target is to compromise confidential information or violate the integrity of the products during the stated internal shipment to allow a modification, cloning or the retrieval of confidential information. Confidential information comprises design data, information on the functionality or client data.

T.Computer-Net defines that a hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as design data, test data or other sensitive production data or modify the testing or production process at the site.

A logical attack against the network of the site provides the lowest risk for an attacker. The target of such an attack is to access the company network to get information that may allow attacking a product or manipulating a product or retrieving information to allow or change the configuration or the personalization or may allow specific physical attack. In addition, a successful access to a company network leads to loss of reputation of the company processing the product or the company that produces the product.

T.Rugged-Theft defines that 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 each site 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 masks, written specifications and analysis reports that may compromise parts of the design or products that can be sold or misused in an application context. This can comprise devices at a specific testing or personalization state for cloning or introduction of forged devices. Those attackers are considered to have the highest attack potential. Such attackers may not be completely defeated by the physical, technical, and procedural security measures.

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

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 masks that can be used to further investigate the functionality of the device and search for possible vulnerabilities. Such an attacker will have limited resources and a low financial budget to prepare the attack. However, the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk. It is expected that such an attacker can be defeated by state of the art physical, technical, and procedural security measures like access control and surveillance.

T.Staff-Collusion defines that an attacker tries to get access to material processed at the site. The attacker tries to get support from one or more employees through an attempted extortion or an

attempt at bribery.

T.Unauthorized-Staff defines that employees or subcontractors who are not authorized to get access to assets or affect production or configuration systems to violate the confidentiality and/or the integrity of the product.This can apply to any production step and any configuration item of the final product as well as to the final product or its configuration.

## 3.3 Organizational Security Policies

This section describes the organizational security policies that are to be enforced by this site. The organizational security policies in Table 3.1 are introduced by the requirements of the assurance components of ALC for the assurance level EAL6. The chosen policies support the understanding of the production flow and the security measures of the site. In addition, they allow an appropriate mapping to the Security Assurance Requirements (SAR).

The documentation of the site is under configuration management. This comprises all procedures regarding the evaluated production flow and the security measures that are needed to ensure the security of the site.

Table 3.1 OSP addressed by the Site

| Policy | Description |
|---|---|
| P.Accept-Product | The quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the finished products. |
| P.Config-Control | The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client. |
| P.Config-Items | The configuration management system shall be able to uniquely identify assets. This includes the unique identification of items that are used for production as well as that are produced at the site.<br>The configuration management is applicable to the documentation of the site, the parameter and test software for the mask sets of different products and/or the products itself. For configuration items that are created, generated or developed at the site the naming and identification are specified. |
| P.Config-Process | The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items and tools used for the production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by a site.<br>The documentation that includes the process descriptions and the security measures of the site is under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases automated tools are used to support and control the production at the site. |
| P.Product-Transport | Technical and organizational measures shall ensure the correct labeling of the product. A controlled internal shipment shall be applied. The transport supports traceability up to the acceptor. If applicable or required, this policy shall include measures for packing if required to protect the product during transport. |
| P.Reception-Control | The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. Furthermore, it is verified that the items can be identified and assigned to a specific product.<br>The incoming inspection is mainly related to the masks which are produced from mask division in the site. They are considered as sensitive configuration items that must be tracked at the site. |

| | |
|---|---|
| P.Scrap-Mask | If the inspection of the mask failed, the mask is registered as a scrap. The mask scrap will be manual etched by mask operation regularly, and then be sent to waste warehouse for further destruction or scrap mask will be shipped to client for final destruction based on the requirement of the client. |
| P.Transfer-Data | Any data classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data. In addition, measures are used to control the integrity of the data after the transfer. |
| P.Zero-Balance | The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced until shipment or destroyed. For each hand over, either an automated or a double check is applied for functional and defect assets. |

## 3.4 Assumptions

This section describes the assumptions that are made on the operational environment to be able to provide security functionalities. Mask Operation is operating in a production flow and must rely on preconditions provided by the previous site. So, each site relies on the materials and information received by the previous site/client.

This is reflected by the assumptions which are to be fulfilled by the client. The assumptions for the client are described in Table 3.2.

Table 3.2 Assumptions for the Client

| Assumption | Description |
|---|---|
| A.Item-Identification | Each asset received by the site is appropriately labelled to ensure the identification of the asset. |
| A.Internal-Shipment | The finished mask is securely shipped to the wafer foundry. Mask Operation has a standard secure procedure for packing of finished masks and preparation of shipment. |
| A.Prod-Specification | The client must provide the design data and appropriate information (e.g. specifications) consistent to the released process technology in order to ensure an appropriate data processing and photomask production process. The provided information includes the classification of the documents and product. |

The assumptions are outside the range of Mask Operation and provides 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.

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

## 4. Security Objectives

This section describes the security objectives that are a concise and abstract statement of the intended solution to the problem defined by the security problem definition in Section 3.

### 4.1 Security Objective Definition

The Security Objectives describes the physical, technical, and organizational security measures, the configuration management as well as the internal shipment at this site in order to provide the developed TOE assurance will work correctly. The security objectives for the site are described in Table 4.1.

Table 4.1 Security Objectives for the Site

| Objective | Description |
|---|---|
| O.Acceptance-Test | The site delivers masks that fulfil the properties guaranteed by the mask foundry. Optical checks are performed to ensure the compliance with the specification. The inspection results are logged to support tracing and the identification of systematic failures. |
| O.Alarm-Response | The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to sensitive asset. After the alarm is triggered, the unauthorized person still has to overcome further security measures. The reaction time of the staff or guards is short enough to prevent a successful attack. |
| O.Config-Control | The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a change management for changes requested by the client as well as internal changes within the production process for released products. Internal changes are classified, and minor ones are handled by the site, major changes must be acknowledged by the client. A designated team is responsible for the release of new products and for the management of changes and their release. This team comprises specialists for all aspects of the services and/or processes. The services and/or processes can be introduced or changed by authorized personnel only. Automated systems support configuration management and production control. |
| O.Config-Items | The site has a configuration management system that manages different mask sets for different products and clients. A unique internal identification is assigned to each product to uniquely identify assets and allow an assignment to a client. Also the internal procedures and guidance are covered by the configuration management. |
| 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 to produce masks, for the management of flaws and optimizations of the process flow as well as for the documentation that describes the services and/or processes provided by a site. |
| O.Control-Scrap | The site has measures in place to destroy sensitive documentation, erase electronic media and destroy sensitive assets so that they do not support an attacker.<br>Conditionally, scrap masks during production and inspection fail will be destroyed at the site. |

| | |
|---|---|
| O.Internal-Shipment | For finished masks are identified by the assigned Fab address which maintained by CE in RTR tooling and are delivered by qualified forwarder. An appropriate internal shipment procedure is applied for both assets. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of assets during internal shipment. For every sensitive asset, the protection measures against manipulation are defined. |
| O.Internal-Monitor | The site performs security management meetings at least once a year. The security management meetings are used to review security incidences, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes are controlled within a shorter time frame to ensure the sufficient control and appropriate protection. |
| O.Logical-Access | The site enforces a logical separation between the internal network and the internet including a firewall. The security measures ensure that only defined services and defined connections are accepted on the internal network. The internal network is appropriately separated to prevent interference between the production and the office environment.<br>Additional specific networks for production and configuration are separated from any internal network to enforce access control. Access to the production network and associated systems is restricted to authorized employees working in the related area or involved in the configuration tasks of the production systems. Every user of an IT system has his/her own user account and password. An authentication using user account and password is enforced by all computer systems. |
| O.Logical-Operation | Network segments and computer systems are kept up-to-date (software updates, security patches, virus protection, spyware protection), especially those with an external interface. The backup of security relevant logs is applied according to the classification of the stored data. Access to the backup is also restricted to authorized person only. |
| 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.Physical-Access | The combination of physical partitioning of the different access control levels together with technical and organizational security measures allow a sufficient separation of employees to enforce the “need to know” principle. The access control supports the limitation of access to these areas including the identification and rejection of unauthorized people. The access control measures ensure that only registered employee or vendor can access restricted areas. Sensitive products are handled in restricted areas only. |
| O.Reception-Control | Upon reception of encrypted GDS file from clients though FTP server, Mask Operation authorized Data Engineer decrypt the database after it download from FTP server, then check the database and inform CE or Customer if have any problem. Upon reception of the returned masks, an incoming inspection is performed to register the mask in the tracking system. |
| O.Security-Control | Assigned personnel of the site or guards operate the security systems like 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.Staff-Engagement | All employees who have access to sensitive assets and who can move parts of the product out of the defined production flow are checked regarding security concerns and must sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job. |
| O.Transfer-Data | Sensitive electronic assets (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to ex-tract the sensitive electronic asset. The keys are ex-changed based on secure measures, and they are sufficiently protected. |
| O.Zero-Balance | The site ensures that all masks (intended TOE of different clients) are separated and traced by respectively. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective masks. According to the agreed production flow the defect masks are either destroyed at the site or sent to the client. |

## 4.2 Security Objectives Rationale

Security Objectives Rationale contains two divisions. The first division describes a tracing which shows how the threats and OSPs are covered by the Security Objectives. The second division describes a justification that shows that all threats and OSPs are effectively addressed by the Security Objectives, and the rationale is also contained in chapter 7.3.

The mapping of security objectives is described in Table 4.2.

Table 4.2 Mapping Security Objectives

| Threat and OSP | Security Objective | Justification |
|---|---|---|
| T.Accident-Change | O.Logical-Access<br>O.Logical-Operation<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Acceptance-Test | The logical access control and configuration management together with organizational measures detect the accident change to the intended TOE and allow for appropriate response on the threat. |
| T.Attack-Transport | O.Transfer-Data<br>O.Internal-Shipment | The shipment method and the organizational measures ensure that integrity changes of shipped objects are detected and appropriately responded upon. |
| T.Computer-Net | O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement | The technical and organizational measures prevent unauthorized access to internal network. |
| T.Rugged-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. |
| T.Smart-Theft | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security | The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. |

| | | |
|---|---|---|
| T.Staff-Collusion | O.Internal-Monitor<br>O.Maintain-Security<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Control-Scrap<br>O.Transfer-Data | The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees limits unauthorized access to assets. |
| T.Unauthorized-Staff | O.Physical-Access<br>O.Security-Control<br>O.Alarm-Response<br>O.Internal-Monitor<br>O.Maintain-Security<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Control-Scrap | Physical and logical access control prohibits access to assets. Both scraps and normal products are under control. |
| P.Accept-Product | O.Config-Control<br>O.Config-Process<br>O.Acceptance-Test | The process control and quality control of the site ensures that the released products comply with the specification agreed with the client. |
| P.Config-Control | O.Config-Items<br>O.Config-Control<br>O.Logical-Access | The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify assets and allow an assignment to the client. |
| P.Config-Items | O.Config-Items<br>O.Reception-Control | The site has a configuration management system that assigns a unique internal identification to each product to uniquely identify assets and allow an assignment to the client. |
| P.Config-Process | 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 protection of mask. |

| | | |
|---|---|---|
| P.Product-Transport | O.Config-Items<br>O.Config-Process<br>O.Internal-Shipment | The internal shipment procedure is applied to the asset.<br>The forwarder supports the tracing of assets during internal shipment. For every sensitive asset, the protection measures against manipulation are defined. |
| P.Reception-Control | O.Reception-Control | The inspection of incoming items done at the site ensures that the received assets comply with the properties stated by the client. |
| P.Scrap-Mask | O.Control-Scrap | Both scraps and normal products are under control. |
| P.Transfer-Data | O.Transfer-Data | Sensitive electronic assets (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. |
| P.Zero-Balance | O.Internal-Monitor<br>O.Staff-Engagement<br>O.Zero-Balance<br>O.Control-Scrap | The site ensures that all security products (intended TOE of different clients) are separated and traced on a device basis. |

## 5. Extended Components Definition

No extended components are currently defined in this SST.

## 6. Security Assurance Requirements

This section describes a set of Security Assurance Requirements to be adopted to evaluate the intended TOE. Clients using this Site Security Target require an evaluation against evaluation assurance level EAL6, potentially claiming conformance with the Eurosmart Protection Profile [6].

The SARs are chosen from the class ALC (Lifecycle support) as defined in [2]:

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

The Security Assurance Requirements listed above fulfil the requirements of [4] because hierarchically higher components than the defined minimum site requirements (ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, see section 3.2.3 of [4]) are used in this SST.

## 6.1 Application Notes and Refinements

The description of the site certification process [4] includes specific application notes. The main item is that a product that is considered as intended TOE (e.g., any TOE type) is not available during the evaluation. Since the term “TOE” is not applicable in the SST the associated processes for the handling of products, or “intended TOE” are in the focus and described in this SST. These processes are subject of the evaluation of the site.

### 6.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

A Manufacturing Execution System is used to assure the traceability and completeness of different production lots. The number of masks is tracked by this system. Appropriate administration procedures are implemented for managing masks. It is ensured, that masks removed from the production stage and returned to the production stage are identified in the production control system.

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

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

The configuration items for the considered product type are listed in section 3.1. The CM documentation of the site can maintain the items listed for the relevant lifecycle step and the CM system is able to track the configuration items. A CM system must be employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures must be provided in order to maintain the integrity and confidentiality of the configuration items.

### 6.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

The scope of the configuration list for a site certification process is limited to the documentation relevant for the SAR claimed in the Site Security Target and the configuration items handled at the site.

In the particular case for the production of the security masks, the scope of the configuration management includes a number of configuration items. The configuration items already defined in section 3.1 are considered as “TOE implementation representation”

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

### 6.1.3 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, inspection data, configuration data and pre-personalization data must be guaranteed, access to any kind of samples (client specific samples or open samples) development tools and other material must be restricted to authorized persons only, and 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.

### 6.1.4 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

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

The PP [6] does not include any refinements for ALC_LCD. Mask Operation does not initiate a life cycle change of the intended TOE. The secure masks are produced and delivered to the wafer foundry required by the client. And the scrap masks are destructed in the site. After destructing the scrap masks, the destructed result will be checked again by conducted staff. If there is any suspicious remain, the destruct process will be conducted again till it fulfils the destruct requirements.

## 6.2 Security Assurance Rationale

The dependencies of the assurance requirements are as followed:

- CM capabilities (ALC_CMC.5): ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
- CM scope (ALC_CMS.5): None
- Development security (ALC_DVS.2): None
- Life-cycle definition (ALC_LCD.1): None

Some of the dependencies are not (completely) fulfilled:

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

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

Table 6.1 Security Assurance Rationale

| SARs | Objectives | Rationale |
|---|---|---|
| ALC_CMC.5.1C<br>ALC_CMC.5.1C: The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling. | O.Reception-Control<br>O.Config-Control<br>O.Config-Items<br>O.Config-Process | O.Reception-Control ensures product identification and the associated labeling. This labeling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products.<br>O.Config-Control ensures that each client product ID is setup and release based on a defined process. This comprises also changes related to a client product ID. The configurations can only be done by authorized staff.<br>O.Config-Process provides a configured and controlled production process. |
| ALC_CMC.5.2C<br>The CM documentation shall describe the method used to uniquely identify the configuration items. | O.Reception-Control<br>O.Config-Control<br>O.Config-Items<br>O.Config-Process | Incoming inspection according O.Reception-Control ensures product identification and the associated labeling. This labeling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products.<br>O.Config-Control ensures that each client part ID is setup and released based on a defined process. This comprises also changes related to a client part ID. The configurations can only be done by authorised staff.<br>O.Config-Process provides a configured and controlled production process. |

| | | |
|---|---|---|
| ALC_CMC.5.3C<br>The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | O.Reception-Control comprises the incoming labeling and the mapping to internal identifications.<br>O.Config-Items and O.Config-Control ensures the changes to both the internal and external configuration items are recorded and reviewed.<br>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. |
| ALC_CMC.5.4C<br>The CM system shall uniquely identify all configuration items. | O.Config-Items<br>O.Config-Control<br>O.Reception-Control | O.Reception-Control comprises the incoming labeling and the mapping to internal identifications.<br>O.Config-Items comprise the internal unique identification of all items that belong to a client part ID. Each product is setup according to O.Config-Control comprising all necessary items. |
| ALC_CMC.5.5C<br>The CM system shall provide automated measures such that only authorized changes are made to the configuration items. | O.Config-Control<br>O.Config-Process<br>O.Logical-Access<br>O.Logical-Operation | O.Config-Control assigns the setup including processes and items for the production of each client part ID.<br>O.Config-Process comprises the control of the production processes.<br>O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. |
| ALC_CMC.5.6C<br>The CM system shall support the production of the product by automated means. | O.Config-Process<br>O.Zero-Balance<br>O.Acceptance-Test | O.Config-Process comprises the automated management of the production processes O.Zero-Balance ensures the control of masks during production.<br>O.Acceptance-Test provides an optical check of the mask quality and supports the tracing. |

| | | |
|---|---|---|
| ALC_CMC.5.7C<br>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<br>O.Logical-Access<br>O.Config-Process | O.Reception-Control ensures the reception procedure of the logical assets from the client. The person responsible for accepting the logical assets cannot be the developer.<br>O.Logical-Access ensures the configuration item developer cannot accept the configuration items in the CM system.<br>O.Config-Process ensures the procedure of the CM plan. It is required in the procedure that the CM manager is not the CM developer. |
| ALC_CMC.5.8C<br>The CM system shall clearly identify the configuration items that comprise the TSF. | N/A | The site is for mask manufacturing and only receives the complete GDS file from the client. Therefore, it is not allowed to separate or to identify any parts that comprise the TSF. |
| ALC_CMC.5.9C<br>The CM system shall support the audit of all changes to the CM items by automated means, including the originator, date, and time in the audit trail. | O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Acceptance-Test | 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, date and time.<br>O.Config-items ensures the changes of the configuration items are recorded.<br>O.Config-Process ensures that the changes from the production steps are recorded automatically by the CM system.<br>O.Acceptance-Test provides an optical check of the mask quality and supports the tracing. |
| ALC_CMC.5.10C<br>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<br>O.Config-Process | O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site. |

| | | |
|---|---|---|
| ALC_CMC.5.11C<br>The CM system shall be able to identify the version of the implementation representation from which the the TOE is generated. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | O.Reception-Control comprises the incoming labeling and the mapping to internal identifications.<br>O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items.<br>O.Config-Process ensures that only controlled changes are applied. |
| ALC_CMC.5.12C<br>The CM documentation shall include a CM plan. | O.Config-Control<br>O.Config-Process | O.Config-Control describes the management of the client part ID sat the site. According to O.Config-Process the CM plans describe the services provided by the site. |
| ALC_CMC.5.13C<br>The CM plan shall describe How the CM system is used for the development of the TOE. | O.Config-Control<br>O.Config-Process | O.Config-Control describes the management of the client part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site. |
| ALC_CMC.5.14C<br>The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product. | O.Reception-Control<br>O.Config-Items<br>O.Config-Control<br>O.Config-Process | O.Reception-Control supports the identification of configuration items at Mask Operation.<br>O.Config-Items ensure the unique identification of each product produces at Mask Operation by the client part ID.<br>O.Config-Control ensures a release for each new or changed client part ID.<br>O.Config-Process ensures the automated control of released products. |
| ALC_CMC.5.15C<br>The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system. | O.Reception-Control<br>O.Config-Control<br>O.Config-Process<br>O.Zero-Balance<br>O.Internal-Shipment | The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced.<br>This is supported by O.Zero-Balance ensuring the tracing of all security products.<br>O.Internal-Shipment includes the packing requirements, the reports, and notifications including the required evidence. |

| | | |
|---|---|---|
| ALC_CMC.5.16C<br>The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. | O.Config-Control<br>O.Config-Process | O.Config-Control comprises a release procedure as evidence.<br>O.Config-Process ensures the compliance of the process. |
| ALC_CMS.5.1C<br>The configuration list includes the following: clear instructions how to consider these items in the list; the evaluation evidence required by the SARs of the life-cycle; development and production tools; security flaw; and development tools and related information. | O.Config-Items<br>O.Config-Control<br>O.Config-Process | Since the process is subject of the evaluation no products are part of the configuration list.<br>O.Config-Items ensure unique part IDs including a list of all items and processes for this part.<br>O.Config-Control describes the release process for each client part ID.<br>O.Config-Process defined the configuration control including part IDs procedures and processes. |
| ALC_CMS.5.2C<br>The configuration list shall Uniquely identify the configuration items. | O.Config-Items<br>O.Config-Control<br>O.Config-Process<br>O.Reception-Control<br>O.Internal-Shipment | Items, products and processes are uniquely identified by the database system according to O.Config-Items.<br>Within the production process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process. The identification of received products is defined by O.Reception-Control. The labeling and preparation for the transport is defined by O.Internal-Shipment. |
| ALC_CMS.5.3C<br>For each ][ configuration item, the configuration list shall indicate the developer/subcontractor of the item.<br>][ is indicated that “TSF relevant” has been deleted. | O.Config-Items | According to O.Config-Items all configuration items for secure products are identified. |

| | | |
|---|---|---|
| ALC_DVS.2.1C<br>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<br>O.Security-Control<br>O.Alarm-Response<br>O.Logical-Access<br>O.Logical-Operation<br>O.Staff-Engagement<br>O.Maintain-Security<br>O.Control-Scrap<br>O.Zero-Balance | 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 personnel security measures. Are provided by O.Staff-Engagement. Any scrap that may support an attacker is controlled according to O.Control-Scrap.<br>All devices including functional And nonfunctional are traced according to O.Zero-Balance. |
| ALC_DVS.2.2C<br>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. | O.Internal-Monitor<br>O.Logical-Operation<br>O.Maintain-Security<br>O.Zero-Balance<br>O.Reception-Control<br>O.Internal-Shipment<br>O.Transfer-Data | The security measures descry-bed 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<br>O.Internal-Monitor, O.Logical-Operation and O.Maintain-Security. All devices including functional And nonfunctional are traced according to O.Zero-Balance.<br>The reception and incoming inspection supports the detection of attacks during the transport of the security products to Mask Operation according to O.Reception-Control.<br>The delivery to the client is protected by Similar measures according to the requirements of the client based on O.Internal-Shipment.<br>Sensitive data received and send by Mask Operation plants are both encrypted according O.Transfer-Data to ensure access by authorized recipients only. |
| ALC_LCD.1.1C<br>The life-cycle definition documentation shall describe the model used to develop and maintain the TOE. | O.Config-Control<br>O.Config-Process | The processes used for identification and manufacturing are covered by O.Config-Control and O.Config-Process. |

| | | |
|---|---|---|
| ALC_LCD.1.2C<br>The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE. | O.Config-Process<br>O.Zero-Balance<br>O.Acceptance-Test | The site does not perform development tasks. The applied production process is controlled according to O.Config-Process.<br>The finished products are check and traced according to O.Acceptance-Test.<br>All security products are traced according O.Zero-Balance. |

Since this SST references the PP [6], the life-cycle module used in this PP includes also the processes provided by this site. Therefore, the life-cycle module described in the PP [6] is 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, ALC_TAT is not applicable for the site. In addition, there is no delivery of security products directly to the consumer regarding the next life cycle step. Therefore, the transport of security products is always considered as internal shipment and ALC_DEL is not applicable for the site.

## 7. Site Summary Specification

### 7.1 Preconditions Required by the Site

Mask Operation provide mask services to manufacture masks based on the client requirements. In order to perform the services, the client of the site is required to fulfil the preconditions as descried in the chapter 3.4 “Assumptions”. The following paragraphs describe preconditions of the client.

For the setup and control of the production process, the client requires provide the appropriate specification, specific requirements for classified design data must also be defined and uniquely identified including the identification of encrypted GDS files.

The released production process includes the tool configuration and set-up for the GDS file optimization using the received GDS file. The released production process further includes the parameters and limits that must be fulfilled by the mask that are used by the wafer Fab.

For the shipment of security product, the recipient of the finished masks is identified by the address of the respective site. The packing of finished masks and preparation of the shipment adhere to the standard procedure of the site, unless the specific requirement from the client.

SMIC Customer Service (CS) is responsible for choosing qualitied forwards to delivery and transfer of the finished masks, comprising the selection of the forwarder and the provision of data for the verification of the transport order.

### 7.2 Services of the Site

The Mask Operation can perform the following secure production activities related in accordance with client instructions:

- GDS data conversion

The GDS file from the client is converted into the mask data according to the production specification. Customer provides encrypt GDS data by PGP, transfer the data to Mask Operation by FTP server. Mask Operation Data engineer decrypt the database after it download from FTP server, then check the database and inform CE if any problem occurs. Two Data engineer do data entry and compare the result, if no problem, prepare the JDV and inform Customer check via remote e-view or on-site JDV. Data will be released to Mask Operation production line after JDV data confirmed ok by Customer. Customer original data don’t do backup and it unencrypted and stored on Mask Operation Data server for temporarily. Customer data will be deleted from server by program after Mask shipping 6 months.

- Mask production

The mask is generated from the mask data based on the production specification. After production, the mask is inspected based on the specification.

- Security mask warehousing and dispatch

  The qualified mask is stored in the mask stocker. The finished mask is securely shipped to the wafer foundry. Mask Operation has a standard secure procedure for packing of finished masks and preparation of shipment.

- Mask service

  The Mask Operation provides the mask remount/recheck and mask repair service if it is required by the wafer foundry.

- Scrap management/destruction

  The mask scrap is stored in a secure scrap warehouse. The scrap is destroyed regularly based on the requirement from the client. The destruction report is sent to the client afterward.

## 7.3 Objectives Rationale

Table 7.1 provides an overview for the correspondence between Security objectives of the TOE / environment listed in section 4.1 and 4.2 to the threats and OSPs identified in section 3.2 and 3.3 and demonstrating that all threats and OSP are mapped to at least one security objective. The more detailed explanation of this mapping is as follows.

Table 7.1 Mappings among the Security Objectives, and Threats / OSPs

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

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

- O.Acceptance-Test

Mask production quality and acceptance tests are introduced and released based on the elated specifications. The tools, specifications and procedures for these tests are controlled by the means of O.Config-Items and O.Config-Control.

- O.Alarm-Response

  The alarm system is connected to the central command center that is manned 7/24. Additional patrolling and the CCTV system support the alarm respond. Additionally, the employees are responding the alarm system during working hours. O.Physical-Access requires certain time to overcome the different level of access control. The response time of the guard and the physical resistance match to provide an effective alarm response.

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

- O.Config-Control

  Procedures arrange for a formal release of configuration documents and specifications for set-up of mask 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 by passwords. Each user has access rights limited to the needs of his function. Thereby only authorized changes are possible.

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

- O.Config-Items

  All product configuration information is stored in the database. The information stored is covering used materials, process specifications, acceptance test instructions and specifications. Products are identified by unique client part IDs which are linked to the unique ID of the associated configuration items. Set-up a new production is performed by the responsible manager using automated tools

  This addresses the threat T.Accident-Change and the OSP P.Config-Items, P.Config-Control and P.Product-Transport.

- O.Config-Process

  The control of the released production process and the controlled introduction of changes ensure a reproducible and consistent production. Procedures for setting up the production process as well as changes to the released processes and documents are in place. Changes can on be done by authorised personnel

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

- O.Control-Scrap

  Scrap masks are stored internally in a secure location. Scrap masks are destructed in a controlled and documented way. The destruction of scrap masks is done under supervision of a qualified employee

  Supported by O.Physical-Access, O.Reception-Control, and O.Staff-Engagement this addresses the

threats T.Unauthorized-Staff and T.Staff-Collusion and the OSP P.Zero-Balance and P.Scrap-Mask.

- 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 physical security access control system, firewall, and virus protection. Major changes of security systems and security procedures are reviewed and approved by the responsible security managers. Upon introduction of a new process a formal review and release for mass production is made before being generally introduced.

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

- O.Internal-Shipment

  The recipient of a production lot is linked to production system and can 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.Product-Transport are addressed by the internal shipment.

- O.Logical-Access

  The internal network (intranet) is separated from the internet with a firewall. The intranet is further separated by authentication measures for critical data such as mask data. Each user logs into the system with his user ID and password. 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 configuration is stored in the database of the system.

  Supported by O.Config-Items this addresses the threats T.Accident-Change and T.Unauthorized-Staff and the OSP P.Config-Control.

- O.Logical-Operation

  All logical protection measures are regularly maintained and updated as required. Critical items such as virus scanners are updated daily. The backup of security relevant logs is applied according to the classification of the stored data. Access to the backup is also restricted to authorized person only.

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

- O.Maintain-Security

  The security relevant systems enforcing or supporting O.Physical-Access, O.Security-Control and O.Logical-Access are checked and maintained regularly. In addition the configuration is updated as

required either by employees (for the access control system) of the supplier. Logging files are checked regularly 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.Physical-Access

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

Thereby the threats T.Smart-Theft and T.Rugged-Theft can be prevented. The physical security measures provided by O.Security-Control enforce the recording of all actions.

Thereby also T.Unauthorized-Staff is addressed.

- O.Reception-Control

At reception of GDS file, the integrity is verified and assigned to the related client order. The link between the data and the client order ensures the unique identification

The OSP P.Config-Items and P.Reception-Control are addressed by the reception control.

- O.Security-Control

The security guards are monitoring the site and the surveillance system 7/24. According to the security level the areas are patrolled by the guards frequently. The alarm system and the CCTV system support the security control. Further on the security control is supported by O.Physical-Access requiring different level of access control for the access to the related assets during operation as well as during off-hours.

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

- O.Staff-Engagement

All employees are interviewed before hiring. They must sign an NDA (Non-Disclosure Agreement), which is integrated in the employee-contracts, and a code of conduct for the use of computers before they start working in the company. The formal training and qualification includes security relevant

subjects and the principles of handling and storage of security products. The security objectives O.Physical-Access, O.Logical-Access and O.Config-Items support the engagement of the staff.

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

- O.Transfer-Data

The integrity of the data transfer from/to the site and within the site is protected against modification and/or disclosure by cryptographic means during transfer.

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.Transfer-Data.

- O.Zero-Balance

Automated tacking within the process flow and the application of a 4-eyes-principle outside the process flow ensures a continuous tracking of sensitive items. This security objective is supported by O.Physical-Access, O.Config-Items and O.Staff-Engagement.

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

## 7.4 Security Assurance Requirements Rationale

The Security Assurance Rational is given in section 6.2. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in [2]. Therefore the following Security Assurance Requirements rationale provides the justification for the selected Security Assurance Requirements. In general, the selected Security Assurance Requirements fulfil the needs derived from the Protection Profile [6]. Because they are compliant with the Evaluation Assurance Level EAL6 all derived dependencies are fulfilled. The Security Assurance Requirements (SARs) are:

Class ALC: Life-cycle support

- Configuration management capabilities (ALC_CMC.5)
- Configuration management scope (ALC_CMS.5)
- Development security (ALC_DVS.2)
- Life-cycle definition (ALC_LCD.1)

### 7.4.1 ALC_CMC.5

Content and presentation elements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.4.2 ALC_CMS.5

Content and presentation elements:

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

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

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

The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the production and test environment. This includes product related documentation and data as well as the documentation for the configuration management and the site security measures. Since the site certification process focuses on the processes based on the absence of a concrete TOE these security assurance requirements are considered to be suitable.

7.4.3 ALC_DVS.2

Content and presentation elements:

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

ALC_DVS.2.2C The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the product.

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

7.4.4 ALC_LCD.1

Content and presentation elements:

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

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

The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled 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 production of Security ICs the focus is limited to this site. However, the assurance requirements are considered to be suitable to support the application of the site evaluation results for the evaluation of an intended TOE.

## 7.5 Assurance Measure Rationale

- O.Acceptance-Test

The testing of the processed control module of the products is considered as automated procedure as require by ALC_CMC.5.6C. ALC_CMC.5.9C requires the CM system shall support the audit of all changes to the CM items by automated means, including the originator, date, and time in the audit trail. In addition, ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Alarm-Response

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

- O.Config-Control

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.9C requires the CM system shall support the audit of all changes to the CM items by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires the CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the mask data are generated. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requests evidence demonstrating that all configuration items have been and are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is

being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. In addition, ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products.

- 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. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. In addition ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.9C requires the CM system shall support the audit of all changes to the CM items by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the mask data are generated. 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 product. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that the developer of each configuration item is indicated in the configuration list. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Config-Process

  ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. The provision of automated measures such that only authorized changes is made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.7C requires the CM system shall ensure that the person responsible for accepting a con-figuration item into CM is not the person who developed it. ALC_CMC.5.9C requires the CM system shall support the audit of all changes to the CM items by automated means, including the originator, date, and time in the audit trail. ALC_CMC.5.10C requires the CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the mask data are generated. ALC_CMC.5.12C requires that the CM documentation includes a CM plan. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requests evidence showing that all configuration items have been and are being maintained under the CM system. ALC_CMC.5.16C

requires that the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_LCD.1.1C requires that the life-cycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

- O.Control-Scrap

  ALC_DVS.2.1C requires that physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the TOE design and implementation. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Internal-Monitor

  ALC_DVS.2.2C requires that 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. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Internal-Shipment

  ALC_DVS.2.2C requires that 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. This includes also the protection during the transport between production sides. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items have been and are being maintained under the CM system. ALC_CMS.5.2C according the unique identification of the packing as configuration item. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Logical-Access

  ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design, implementation and in its development and production environment. Thereby this Security Assurance Requirement is suitable to meet the security objective. 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.5.7C requires the CM system shall ensure that the person responsible for accepting a con-figuration item into CM is not the person who developed it. Thereby this Security Assurance Requirement is suitable to meet the security objective. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Logical-Operation

  ALC_DVS.2.1C: requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the TOE design,

implementation and in its development and production environment. Thereby this Security Assurance Requirement is suitable to meet the security objective. 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 product. Thereby this Security Assurance Requirement is suitable to meet the security objective. 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 Security Assurance Requirement is suitable to meet the security objective.

- O.Maintain-Security

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

- 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 Security Assurance Requirement is suitable to meet the security objective.

- O.Reception-Control

  ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labeling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires the CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the mask data are generated. Thereby, this Security Assurance Requirement is suitable to meet the security objective. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the product. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items have been and are being maintained under the CM system. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the product during the transfer between sites. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Security-Control

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

- O.Staff-Engagement

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

- O.Transfer-Data

  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 product. This includes also the protection during the transport between production sides. Thereby this Security Assurance Requirement is suitable to meet the security objective.

- O.Zero-Balance

  ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means. ALC_CMC.5.15C requires evidence demonstrating that all configuration items have been and are being maintained under the CM system. ALC_DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the product. ALC_LCD.1.2C requires control over the development and maintenance of the TOE. Thereby this Security Assurance Requirement is suitable to meet the security objective.

### 7.6 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and the complete documentation of the site provided for the evaluation. The mapping between the internal site documentation and the Security Assurance Requirements is only available within the full version of the Site Security Target.

## 8. Reference

### 8.1 Literature

The following documentation was used to prepare this SST:

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

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

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

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

[5] JIL-Minimum Site Security Requirements version 3.0, February, 2020

[6] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-PP-0084-2014, January 13, 2014

[7] Eurosmart Site Security Target Template version 1.0, 21 June 2009

## 8.2 Definitions

Client: The word “client” is used here instead of “customer” since the words “customer” and “consumer” are reserved in Common Criteria.

## 8.3 Abbreviations

The abbreviations table is described in Table 8.1.

Table 8.1 Abbreviations Table

| Abbreviation | Definition |
|---|---|
| BOA | Background Quality Assurance |
| CC | Common Criteria |
| CE | Customer Engineer |
| CTM | Customer |
| CP | Chip Probe |
| CMP | Chemical Mechanical Polishing |
| CS | Customer Service |
| Div | Division |
| DRC | Design Rule Check |
| EAL | Evaluation Assurance Level |

| | |
|---|---|
| EBO | E-Beam Operation |
| Diff | Diffusion |
| Etch | Etching |
| FA | Failure Analysis |
| FG | Finish Goods |
| FTP | File Transfer Protocol |
| GDS | Graphic Database System |
| IC | Integrated Circuit |
| IT | Information Technology |
| JDV | Job Deck View |
| Litho | Litho |
| MES | Manufacturing Execution System |
| MFG | Manufacturing |
| OPC | Optical Proximity Correction |
| OQA | Outgoing Quality Assurance |
| OSP | Organizational Security Policy |
| PP | Protection Profile |
| PE | Process Engineer |
| PC | Production Control Planner |
| PIE | Process Integration Engineer |

| | |
|---|---|
| ROM | Read Only Memory |
| RTR | Reticle Tooling Request |
| SAR | Security Assurance Requirement |
| SST | Site Security Target |
| TF | Thin Film |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| WAT | Wafer Acceptance Test |