Site Security Target Lite – LFoundry Avezzano site and LFoundry Landshut site

Control Information

Control Item	Details
Area	Corporate
Security Level	SL4
Document Type	High Level Document
Creation Date	June 15th, 2018
Proposed by	EHSS Security Responsible ICT Security Manager
Verified by	EHSS Security Responsible ICT Security Manager Head of Facilities ICT VP
Approved by	Head of Facilities CEO Vice Chairman
Document ID	
Information related to current release (refer to Revision History section for any previous release details)	
Revision: 1	**Date**: June 13th, 2018
Description: First release	

Any printed copy of this document is not controlled. The controlled copy of this document is available in the DMS. Any printed copy is to be intended for personal reference only.

Table of Contents

1. Documet Information

1.1. Reference

Title:	Site Security Target Lite – LFoundry Avezzano site and LFoundry Landshut site
Version:	1
Date:	June 4th, 2018
Company:	LFoundry
Name of the site:	LFoundry Avezzano (AQ, Italy); LFoundry Landshut (Landshut, Germany)
Product type:	Wafer foundry
EAL-level:	EAL5+

1.2. Version History

Revision	Date (dd/mm/yy)	Revision Description	Originator
1	06/13/2018	First release	T.Lanconelli

2. SST Introduction

This chapter is divided into the following sections: “Identification of the Sites” and “Site Description”. This Site Security Target (SST) refers to Avezzano site and Landshut site. The site can be part of the production flow of the Wafers and dies with Security ICs.

2.1. Identification of the Sites

The LFoundry Avezzano site (manufacturing) and LFoundry Landshut site (design) are located at:

Avezzano site:

LFoundry S.r.l

Via Antonio Pacinotti 7

67051 Avezzano AQ, Italy

Landshut site:

LFoundry Srl Zweigniederlassung Landshut

Ludwig-Erhard-Strasse 6a

84034 Landshut, Germany

Based upon the life-cycle defined in Protection Profile (PP) [Sec_IC], the site covers parts of the life cycle phase 3 related to the:

- integration and photomask fabrication;
- IC production.

Services provided by LFoundry cover the IC Manufacturing (Phase 3) with reference to the following stages:

- integration between LFoundry’s IC structures with those of the customer before the photomask fabrication (Landshut site);
- IC production (Avezzano site).

2.2. Site Description

2.2.1. Avezzano site

The Avezzano site consists of a manufacturing building (wafer Fab) and other areas involved in IC production management within the support building, with additional utilities buildings. The entire site is surrounded by a fence.

The site does not directly contribute to the development of the intended TOE in the sense of CC. Nevertheless, the process flow conducted at the site includes the realization on the IC on wafers. Using the received photomask and the client specifications, the site does perform the IC construction on wafers. The wafers are then delivered to the client. As this is regarded as internal shipment, it is covered under aspect ALC_DVS.2 instead of ALC_DEL.1 that covers the delivery to an external customer which the site does not conduct.

The following LFoundry services are performed during the activities mentioned above:

- receipt, identification, registration and storage of mask sets;
- receipt of GDS2 file provided by Landshut site;
- wafer production;
- quality assurance;
- secure wafer delivery to clients;

Accountability for the management of the previous service is mainly owned by the following Departments/Organization Unit:

- Procurement & Logistics;
- R&D;
- ICT;
- Manufacturing;
- Process Engineering;
- Customer and Product Quality;
- Security.

LFoundry S.r.l is not the only company located within the perimeters. Some of the site premises are leased to MIY (Micron Technology S.r.l., Italy). MIY appliances are clearly separated and all located in areas not involved in manufacturing processes. The physical separation between LFoundry and MIY is realized through a badge reader system installed on all access doors. The MIY employees are not allowed to access the LFoundry areas and the entire security system and access management system is under control of LFoundry's Security Team. Besides that, all the gates of access to areas of LFoundry and MIY they are monitored through the CCTV system that is managed by the Security Control Room of LFoundry.

Support Building Ground Floor

MIY appliances: all MIY appliances are located within the Support Building's ground floor and all the access are controlled by an access control system that uses badge reader. The badge reader system is managed exclusively by LFoundry's Security Team.

Areas involved in IC production: The Support Building ground floor includes the Computer Room, the Security Server Room and the Security Control Room. Within the ground floor are located both the shipping area and the secure finished goods warehouse.

Support Building First Floor

The Support Building first floor includes part of the wafer fab (Probe clean room), the access for the clean room (both for personnel and tools or materials) and for the finished goods outcoming.

The wafer fab is placed at the same level of the Support Building first floor and contains the Clean Room (except the probe area) with the maintenance areas. This is the area in which takes place the production of IC on wafers.

Support Building Second Floor

Within the Support Building second floor are included the GDS2 room (used for the GDS2 transfer data) and the laboratories.

2.2.2. Landshut site

The German site performs the design activities (integration of LFoundry proprietary modules with client design) and technology development, marketing and sales.

The office building is in Ludwig-Erhard-Strasse 6a, in district LANDSHUT WEST. The Landshut's site consists of office area distributed in 4 levels. Various surveillance and alarming systems at the floor and basement levels inside the building ensure site protection and control and alarming 7day by 24 hours. The following LFoundry services are performed during the activities mentioned above:

- receipt of GDS2 file provided by clients;
- mask data preparation;
- mask data transfer to the mask shop;
- GDS2 file transfer to Avezzano site.

Accountable for the management of the previous service are the following Departments/Organization Unit:

- R&D Team Landshut;
- ICT.

The areas involved in design activities are located at the first floor and are the data preparation room and the server room are at basement.

3. Conformance Claim

The evaluation is based on Common Criteria Version 3.1, Release 4.

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

For the evaluation the following methodology will be used:

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

The evaluation of the site comprises the following assurance components:

ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_TAT.2, ALC_LCD.1

The chosen assurance components are derived from the assurance level EAL5+ of the assurance class "Life-cycle Support". For the assessment of the security measures attackers with high attack potential are assumed. Therefore, this site supports product evaluations of products up to EAL5+.

The assurance level chosen for the present SST is compliant to the PP [SEC_IC], which contains the following application note: “This Protection Profile requires EAL4 augmented but allows to add higher hierarchical components” (application note 21 of [Sec_IC]). Hence, the SST is suitable for Security ICs and the evaluation is suitable to support product evaluations up to assurance level EAL5+ conformant to [CCPart3].

Based upon the life-cycle defined in PP [Sec_IC], the site covers parts of the life cycle phase 3 related to the:

- integration and photomask fabrication;
- IC production.

Services provided by LFoundry cover the IC Manufacturing (Phase 3) with reference to the following stages:

- integration between LFoundry’s IC structures with those of the customer before the photomask fabrication (Landshut site);
- IC production (Avezzano site).

The site covers parts of the life cycle phase 3 related to the integration for the photomask fabrication and IC production. According to this premise the site does not cover any aspects that are covered by ALC_TAT so the assurance component ALC_TAT.2 is not applicable.

The CC assurance components of the family ALC_DEL refer to the external delivery of the TOE to the consumer or consumer’s site. The site does not provide external delivery of the TOE to the consumer so the assurance component ALC_DEL.1 is not applicable and the component cannot be used for internal shipment. Internal shipment is covered by ALC_DVS.2.

4. Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site. The security problem is defined in a different way for both sites, according the differences regarding the management of configuration items in Landshut and Avezzano.

The Security Problem Definition is about two sets of security problems. The first set of security problems comprises all kind of possible attacks regarding physical objects (e.g. wafers, or masks). They are mainly related to the unauthorized disclosure of information (e.g. design data) or the theft of the assets.

The second one comprises instead the requirements for the configuration management (e.g. controlled production flow) and the control of security measures.

The security problems are described in terms of Threats, Organizational Security Policies (OSP) and Security Objectives.

4.1. Assets and Configuration Item

This section describes the assets handled at the site which are included in the configuration item list.

The site has proper internal documentation and data relevant to maintain the integrity and confidentiality of an intended configuration item. This comprises security concepts and all the associated security measures as well as keys and cryptographic tools for the encrypted exchange of data. All these items are not explicitly listed in the list of assets below.

Although the integrity of any machine or tool used for production and testing is not considered as an asset, appropriate measures are defined for the site to ensure the correct operation of machines and tools. This is based on regular maintenance and calibration. The machines and tools consist of commercial available hardware and software which are programmed and customized.

4.1.1. Intended Configuration Item List

The following assets are related to the production of wafers with security ICs, and define the list of LFoundry intended configuration item. For each configuration item is then specified the owner organization and the involved LFoundry service from section 2.2.

- development data (GDS2);
  - owner R&D in Landshut;
  - used within mask data preparation at Landshut site;
  - used within wafer production at Avezzano site;
- implementation data (masks data);
  - owner R&D in Landshut;
  - used within mask data preparation at Landshut site;
- photo masks (Mask);
  - owner Manufacturing in Avezzano;
  - used within wafer production at Avezzano site;
- wafers (both final shippable material and scrap);

- owner Manufacturing in Avezzano;
- used within wafer production at Avezzano site;

- rejects (RMA);
  - owner Customer and Product Quality in Avezzano;
  - used within quality assurance at Avezzano site.

4.2. Threats

All threats are dangerous for the integrity and confidentiality of the assets and the representation of parts of the assets. During the development and production, the assets and the representation of parts of the assets are vulnerable to such attacks. The following threats are applicable to LFoundry that provides production services handling the items listed in section 4.1.1 above. The explanation accompanying the listed threats will help to address the Security Objectives according to the site specific aspects.

T.Accident-Change

An employee or contractor may exchange by accident assets of different production lots or different clients during production process.

This threat includes accidental changes due to working tasks or maintenance tasks within the development or production area.

Accidental changes can include the modification of configurations for tools that may have an impact on the configuration item, the wrong assignment of tools for a dedicated process step or machine failure.

A protective concept in use is the automated system for the use of the recipes and the control of process flow.

This threat applies to Avezzano site and Landshut site.

T.Attack-Transport

An attacker might try to get data, specifications or assets during the internal shipment. The target is to compromise confidential information or violate the integrity of the assets during the stated internal shipment to allow a modification, cloning or the retrieval of confidential information.

This threat applies both in Avezzano site and Landshut site.

During the internal shipment all configuration items are identified with a unique ID. Both wafer and mask are always under the tracing of the automated system. Sensitive data are used only in separated network available to authorized staff and the access is allowed through a strong authentication system.

This threat applies in Avezzano site.

T.Computer-Net

A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get data such as design data, test data or other sensitive production data or modify the security relevant processes such as the development process at the site.

Such attackers are considered to have high attack potential because they may have technical equipment to perform such an attack. The attacker may have the resource to buy or develop software or hardware which can exploit known vulnerabilities within the tools and software in use.

A protective concept with more than one level is in use for the company network. This comprises a firewall to the external network, and further limitations of the network. In addition, computer users have individual accounts which require authentication (e.g. password). For specific tasks or processes standalone networks are in use. The protection is supported by appropriate measures to update and maintain the computer and network systems and analyze logs that may provide indications for attack attempts.

This threat applies both in Avezzano site and Landshut site.

T.Smart-Theft

An attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration items. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack the use of standard equipment for burglary is considered.

This threat applies both in Avezzano site and Landshut site. The target of the attack may be wafers, masks, data (Avezzano Manufacturing site) or mask data (Landshut design site).

Special measures like storage of items in safes or strong rooms or permanent automated control as well as the encryption of sensitive data and use of isolated network provide additional support against such attacks.

T.Rugged-Theft

An experienced attacker tries to access sensitive areas of the site for manipulation or theft of sensitive configuration items. The attacker has sufficient time to investigate the site outside the controlled boundary.

For the attack the use of specialized equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to camouflage the intention. Attacker could be paid for such stealing activities.

It is expected that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control, alarms and video-surveillance. An access control concept with two levels is implemented in critical areas (strong authentication). Where strong authentication is implemented, the more restrictive level of the access control shall prevent the simple access using lost or stolen access token.

This threat applies both in Avezzano site and Landshut site.

T.Staff-Collusion

An attacker tries to get access sensitive data or material processed at the site. The attacker tries to get support from one employee through an attempted extortion or an attempt at bribery.

The automation system allows the traceability and the personal accountability as far as possible. Elsewhere procedures with dual control are in use. The measures depend on the assets that must be protected at the site.

This threat applies both in Avezzano site and Landshut site.

T.Unauthorized-Staff

Employees or contractors not authorized to get access to assets or systems used for production get access to assets or affect production systems or configuration systems, so that the confidentiality and/or the integrity of the product is violated. This can apply to any production step and any configuration item of the final asset as well as to the final asset or its configuration.

Access level for the staff (employees or contractors) is assigned according a security matrix managed by the Security Manager. The security matrix itself is built on the "need to know" principle, to avoid the release of not necessary access privilege.

This threat applies both in Avezzano site and Landshut site.

4.3. Organizational Security Policies

The aim of the OSPs is introduced by the requirements of the assurance components of the Assurance Class ALC (Life-cycle support) to obtain the intended assurance level. The site security policy supports the understanding of the production flow and the security measures implemented in the site. The defined policies provide an appropriate mapping to the Security Assurance Requirements (SARs).

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

P.Configuration-Control

The procedures for setting up the production process for a new asset as well as the procedure that allows changes of the initial setup for an asset shall only be applied by authorized personnel. Automated systems shall support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set up of a production process ensures that sufficient information is provided by the client.

The definition of the Security Matrix allows to assign an appropriate security access level to all the staff, according to the "need to know" principle. This avoid that unauthorized people access the configuration items.

P.Configuration-Items

The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of items that are used for production as well as that are produced at the site.

Data provided by customer and mask provided by supplier are identified by a unique ID defined by customer/supplier himself.

Wafers during the manufacturing process are identified by a unique ID generated by an automated system and used for the traceability during the process flow.

P.Configuration-Process

The services and processes provided by the site are controlled in the configuration management plan. This comprises incoming items and tools used for the development and production of the asset, the optimizations of the process flow as well as the documentation that describes the services and processes provided by the site. A released production process is defined for the wafers. All the documentation including the process descriptions and the security measures of the site is under version control (Document Management System). Measures are in place to ensure that the evaluated status is ensured. Wherever it is possible, automated tools are used to support and control the production flow.

P.Organise-Product

For the development and production of the asset is ensured that the specified process is properly applied. An automated system is in use to prevent misprocess or unauthorized activities during the

production flow. In line controls ensure that the process is properly applied and compliant with technical specifications. The development process is applied as specified by LFoundry's quality management documentation.

P.Product-Transport

Technical and organizational measures are used to ensure that the asset is correctly labeled. 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 asset during transport.

P.Reception-Control

The inspection of incoming items done at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the items can be identified and assigned to a specific asset.

P.Security-Control

To protect security of configuration items, technical and organizational measures shall be in place to identify security risks, monitor the physical and logical site environment, detect security events, manage such events with appropriate actions.

P.Transfer-Data

Any data in electronic form (e.g. asset specifications, GDS2 files, release information and so on) that is classified as sensitive or higher security level by the client is encrypted when exchanged between Site and client or sub-contractors to ensure confidentiality of the data. In addition, measures are used to control the integrity of the data after the transfer.

Electronic data exchange is allowed only through authorized pathway and in encrypted mode. This kind of data are managed in a dedicated and standalone network. The access to this network is allowed only to authorized people through a strong authentication system.

P.Zero-Balance

The site ensures that all sensitive configuration items handled are separated and traced on a device basis. For each hand over, either an automated or an organizational “two-employees-acknowledgement” (two-man rule) is applied for functional and defect assets. According to the released production process the defect assets are either stored at the site or sent back to the client or customer and/or consumer (depending on the production-setup).

4.4. Assumptions

Since the site covers only parts of the life cycle phase 3, related to the integration and photomask fabrication and IC production, LFoundry must rely on preconditions provided by the owner of the other parts of the life cycle.

This is reflected by the assumptions defined below for the interface between the client, the site and the part of the production flow that is not under LFoundry direct control.

A.Internal-Shipment

The recipient client of the transferred configuration items is identified by the address of the client site for physical items and by corresponding information for electronic items (e.g. e-mail address and digital signature).

A.Item-Identification

Each configuration item received at the site is appropriately labeled by the sender, to ensure the identification of the configuration item and that the object is uniquely identified.

A.Mask-Support

The Photo Shop provides photo masks for the wafer production that are compliant with the production process released at the site. Further the masks must include an ID that fits to the production support of the site and are included in the CM system.

A.Product-Specification

The client provides all the appropriate information (e.g. specifications, definitions, test requirements, test limits) to ensure the appropriate production process. The provided information includes the classification of the documents and asset. The information provided by the client clarifies the documents or items developed by the site that have to undergo a release process.

A.Product-Test

The client is responsible for the functional testing of the finished devices on the wafer. Further the masks include appropriate test structure to support the parameter testing of the finished wafers.

A.Design-Integration

The client's device design is such that no potential vulnerabilities are added to it by the integration for the photomask fabrication performed by the Data Preparation process at Landshut site, detailed in section 7.1.1.

A.Security

All Sites' clients and suppliers are responsible for all security certifications related to their internal management and processing of physical and logical goods, as well related to exchanging goods with LFoundry. Based upon those certifications, the configurations items exchanged between LFoundry and its clients or suppliers are not compromised by internal management and processing performed by clients or suppliers as part of the life cycle activities that are not under LFoundry direct control.

5. Security Objectives

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

O.Alarm-Response

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 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 if needed. The reaction time to a security breach is short enough to prevent a successful physical attack.

O.Configuration-Control

The site applies a release procedure for the setup of the production process for each new asset. 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 assets. A designated team is responsible for the release of new assets and for the management of changes and their release. Automated systems are used to support configuration management and production control validating production material before start processing. Internal changes are classified; the minor ones are handled by the site, but the major changes are previously approved by the client.

O.Configuration-Items

The site has a configuration management system that manages different mask sets for different assets and customers. A unique internal identification is assigned to each asset to uniquely identify configuration items and allow an assignment to a client. The internal procedures and guidance are covered by the configuration management tool.

O.Configuration-Process

The site controls its processes using a configuration management plan. The configuration management is controlled by tools and procedures for the production of wafers, for the management and optimizations of the process flow as well as for the documentation that describes the processes provided by LFoundry.

O.Control-Scrap

The site has measures in place to destruct sensitive documentation, erase electronic media and to handle scrap to be destroyed or to be shipped and destroyed by the client so that they are not exposed to an attacker.

O.Internal-Monitor

The site performs security management meetings at least every six months. The security management meetings are used to review security breaches, to verify that maintenance measures are applied and to reconsider the assessment of risks and security measures. An internal audit is performed every year to control the application of the security measures.

O.Internal-Shipment

An appropriate internal shipment procedure is applied for sensitive configuration items. Only a controlled process can change the address for shipment. For every sensitive configuration item, the protection measures against manipulation are completely defined.

O.Logical-Access

The site maintains a logical separation between the internal network and the internet including a firewall. The security measures are aimed to ensure that only defined services and defined connections are accepted on the internal network. Access to the production network and associated systems is restricted to authorized employees. Every user of an ICT system has its own user account and password. User accounts and associated user authentication are needed for network segments transferring sensitive data.

O.Logical-Operation

Network and computer systems architecture are structured to enable control of the data exchanged. The backup of sensitive data and security relevant logs is applied according to the classification of the stored data. The backup is stored in separate and controlled areas. 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, including the access control system, to ensure that only authorized employees have access to sensitive areas as well as computer and network systems.

O.Organise-Product

Technical and organizational tools are used to ensure that the Site performs development and production of the configuration items in compliance with the specified process requirements provided by the client.

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 site enforces four levels (from level 4 the lowest to level 1 the higher) of access control to sensitive areas of the site. The access control measures ensure that only authorized person can access restricted areas. Sensitive assets are handled in restricted areas only. A strong authentication system is in use for the management of sensitive areas.

O.Reception-Control

Upon reception of photo masks is performed an immediate incoming inspection. This inspection comprises the received amount of photo masks and the identification and assignment of the asset to a related internal production process. Parameter tests and optical checks are performed on incoming raw materials to ensure the compliance with the client’s specification.

O.Security-Control

The technical and organizational measures for security ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item. After the alarm is triggered, the unauthorized person still has not yet access to the sensitive configuration item and the reaction time of the staff or guards has the aim to prevent a successful completion of the attack.

O.Staff-Engagement

All employees are trained and qualified for their job. Employees who have access to sensitive configuration items and who can move parts of the asset out of the defined production flow are checked regarding security concerns and have to sign a non-disclosure agreement.

O.Transfer-Data

Sensitive electronic configuration items (documents in electronic form or data) are protected with cryptographic algorithms to ensure integrity and confidentiality. The associated keys are communicated to individuals such that only authorized employees can extract the sensitive electronic configuration item.

O.Zero-Balance

The site ensures that all wafers and photo masks are separated and traced. Automated control and/or two employees' acknowledgement during hand over is applied for functional and defective wafers and photo masks. According to the agreed production flow the defect wafers are either destroyed or sent to the client.

5.1. Security Objectives Rationale

The SST includes a Security Objectives Rationale divided in two different parts. The first one describes how the threats and OSPs are covered by the Security Objectives. The second part shows how all threats and OSPs are effectively addressed by the Security Objectives.

Note that the assumptions of the SST cannot be used to cover any threat or OSPs 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. For this reason, they do not contribute to the security of the site under evaluation.

5.1.1. Mapping of Security Objectives

This section provides the justifications that show that all threats and OSPs are effectively addressed by the security objectives.

THREAT and OSP	SECURITY OBJECTIVE	RATIONALE
T.Accident-Change	O.Configuration-Control O.Configuration-Item O.Configuration-Process O.Logical-Access O.Logical-Operation O.Organise-Product	They diminish this threat with a combination of technical and organizational measures and allow an appropriate response.
T.Attack-Transport	O.Internal-Shipment O.Reception-Control O.Transfer-Data	They ensure the integrity of the data transfer from/to the site.
T.Computer-Net	O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security	They diminish this threat with a combination of technical and organizational measures and allow an appropriate response.

THREAT and OSP	SECURITY OBJECTIVE	RATIONALE
T.Rugged-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access O.Reception-Control O.Security-Control O.Staff-Engagement O.Zero-Balance	Identification, authentication and access control security mechanisms that ensure only authorized users can access to configuration item resources. They grant periodical review of security measures and log's control.
T.Smart-Theft	O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Physical-Access O.Security-Control	Identification, authentication and access control security mechanisms that ensure only authorized users can access to configuration item resources. They grant periodical review of security measures and log's control.
T.Staff-Collusion	O.Control-Scrap O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O.Transfer-Data O.Zero-Balance	They diminish this threat with a combination of technical and organizational measures and allow an appropriate response.
T.Unauthorized-Staff	O.Alarm-Response O.Internal-Monitor O.Logical-Access O.Logical-Operation O.Maintain-Security O.Physical-Access O.Security-Control	Identification, authentication and access control security mechanisms that ensure only authorized users can access to configuration item resources.
P.Configuration-Control	O.Configuration-Control O.Configuration-Items O.Logical-Access	They ensure introduction and controlled change of CM components.
P.Configuration-Items	O.Configuration-Items O.Reception-Control	They cover all relevant items.
P.Configuration-Process	O.Configuration-Process	The services and processes provided by the site are controlled through the configuration management plan.
P.Organise-Product	O.Logical-Access O.Organise-Product	They ensure the compliance of the production process with the specifications.
P.Product-Transport	O.Internal-Shipment O.Staff-Engagement	They ensure correct internal shipment.
P.Reception-Control	O.Configuration-Control O.Configuration-Process O.Reception-Control	They ensure the correct identification and management of received configuration items.

THREAT and OSP	SECURITY OBJECTIVE	RATIONALE
P.Security-Control	O.Alarm-Response O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Physical-Access O.Security-Control O.Staff-Engagement	Identification, authentication and access control security mechanisms, periodically reviewed, ensure that only authorized users can access to configuration item resources.
P.Transfer-Data	O.Transfer-Data	All data received or transmitted are handled accordingly to appropriate security measures.
P.Zero-Balance	O.Control-Scrap O.Staff-Engagement O.Zero-Balance	All configuration items are in the scope of the traceability.

6. Extended Assurance Components Definition

No extended components are currently defined in this SST.

7. Security Assurance Requirements

Clients using this SST require an evaluation according to the assurance level EAL5+. This evaluation assurance level requires the SARs listed below from the Assurance Class ALC (Life-cycle support):

- ALC_CMC.4 (CM capabilities)
- ALC_CMS.5 (CM scope)
- ALC_DEL.1 (Delivery)
- ALC_DVS.2 (Development security)
- ALC_LCD.1 (Life-cycle definition)
- ALC_TAT.2 (Tools and techniques)

The following SARs are not applicable:

ALC_TAT.2: the site covers parts of the life cycle phase 3 related to the integration and photomask fabrication and IC production. According to this premise the site does not cover any aspects that are covered by ALC_TAT so the assurance component ALC_TAT.2 is not applicable.

ALC_DEL.1: the CC assurance components of the family ALC_DEL refer to the external delivery of the TOE to the consumer or consumer's site. The site does not provide external delivery of the TOE to the consumer so the assurance component ALC_DEL.1 is not applicable.

The dependencies for the SARs named above are as follows:

- ALC_CMC.4: ALC_CMS.1, ALC_DVS.1, ALC_LCD.1
- ALC_CMS.5: none
- ALC_DEL.1: none
- ALC_DVS.2: none
- ALC_LCD.1: none
- ALC_TAT.2: ADV_IMP.1

The following dependencies are not fulfilled or not completely fulfilled:

ADV_IMP.1: it relates to asset specific implementations representations and is therefore not part of this SST. This dependency is not satisfied. Take into account that even ALC_TAT.2 is not applicable to this SST as explained above.

7.1. Application Notes and Refinements

The description of the site certification process includes specific application notes. The most notable item is that an asset 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 configuration items are in the focus and described in this SST. These processes are subject of the evaluation of the site.

7.1.1. Overview and Refinements regarding CM Capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of configuration items within the whole LFoundry supply chain.

A production control system is employed to guarantee the traceability and completeness of configuration items. The number of masks and wafers is tracked by this system. Appropriate procedures are implemented for managing masks and wafers which are being removed from the

production-process in order to verify and to control predefined quality standards and production parameters. It is ensured that masks and wafers removed from the production stage are returned to the production stage from where they were removed or are securely stored or destroyed. The processes and configuration items rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below.

The configuration control and a defined change management 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 control of the asset during the production process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be under configuration management for these cases. The configuration items for the considered asset type are listed in section 4.1.1. and are kept within the configuration management system. The CM documentation of the site is able to maintain the items listed for the relevant lifecycle step and the CM system is able to track the configuration items. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

7.1.2. Overview and Refinements regarding CM Scope (ALC_CMS)

The scope of the configuration list for the site certification process is limited to the documentation relevant for the SARs claimed in the SST and the configuration items handled at the site. For the production of wafers with Security ICs the scope of the configuration management includes a number of configuration items.

The configuration items already defined in section 4.1.1 are considered and they include:

development data (GDS2)
implementation data (masks data)
photo masks (Mask)
wafers (both final shippable material and scrap)
rejects (RMA)

7.1.3. Overview and Refinements regarding Delivery Procedure (ALC_DEL)

The CC assurance component ALC_DEL.1 refers to the external delivery of the configuration items or parts of them to the consumer. Procedures and technical measures for external delivery of asset or part of it are required to maintain the confidentiality and integrity of the asset.

LFoundry site is not involved in external delivery since does not provide any configuration item to the consumer, so ALC_DEL.1 is out of scope for this certification. Moreover, ALC_DEL.1 cannot be used for internal shipment which is instead covered by ALC_DVS.2.

However, the component ALC_DEL.1 is included here to support the reuse of the evaluation results.

7.1.4. Overview and Refinements regarding Development Security (ALC_DVS)

The component ALC_DVS.2 “Sufficiency of security measures” requires additional evidence for the suitability of the security measures. The confidentiality and integrity of design information, test data,

configuration data and pre-personalization data must be guaranteed; access to any kind of samples (customer specific samples or open samples) development tools and other material must be restricted to authorized persons only. Scrap must be controlled and destroyed.

According to these requirements, the physical security as well as the logical security of the site are 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 (or two separated area of same site) 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. During internal shipment security measures have to be in place to provide the necessary level of protection to maintain the confidentiality and integrity of the configuration items.

7.1.5. Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

LFoundry is not the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only the life-cycle phases which are in the scope of the site have to be evaluated.

With reference to TOE life cycle for IC [Sec_IC], in case of LFoundry only the IC Manufacturing phase (Phase3 as per [Sec_IC] section 1.2.3) is applicable, where for LFoundry Landshut Design site the “integration” is relevant while for LFoundry Avezzano Manufacturing site the “IC Production” is relevant.

7.1.6. Overview and Refinements regarding Tools and Techniques (ALC_TAT)

The CC assurance components of family ALC_TAT refer to the tools that are used to develop analyze and implement the TOE.

Since the site covers parts of the life cycle phase 3 related to the integration and photomask fabrication and IC production, the site does not cover any aspects that are covered by ALC_TAT so the assurance component ALC_TAT.2 is not applicable.

The site ensures only a reproducible production process within the limits defined for the released wafer production process. Relevant parameters are controlled during the production process and this is subject of the configuration management.

However, the component ALC_TAT.2 is included here to support the reuse of the evaluation results.

7.2. Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components to the Security Objectives defined in this SST. The refinements described above in section 7.1 are considered.

The site has a process in place to ensure an appropriate and consistent identification of the assets. If the site already receives configuration items, this process is based on the assumption (A.Item-Identification) that the received configuration items are appropriately labeled and identified.

The SARs reported in section **Error! Reference source not found.** are taken from [CCPart3] with the term TOE replaced by configuration items in most cases while in specific cases it is replaced by product. The content elements that are changed from the original [CCPart3] are written in *italic*.

SAR	Security Objective	Rationale
ALC_CMC.4.1C: the *configuration item* shall be labeled with its unique reference.	O.Reception-Control O.Configuration-Items	O.Reception-Control ensures that the incoming inspections guarantee the correct asset identification and labeling. O.Configuration-Items ensure that wafers are labeled with a unique ID and automated tools are used for the correct setup of this labeling.
ALC_CMC.4.2C: the CM documentation shall describe the method used to uniquely identify the configuration items.	O.Reception-Control O.Configuration-Items O.Configuration -Control	O.Reception-Control ensures that the incoming inspections guarantee the correct asset identification and labeling. O.Configuration-Items ensure the unique identification of every asset. O.Configuration-Control ensure that each part is managed by the appropriate process.
ALC_CMC.4.3C: the CM system shall uniquely identify all configuration items.	O.Reception-Control O.Configuration-Items O.Configuration-Control	O.Reception-Control includes the incoming labeling. O.Configuration-Items ensure internal unique identification. O.Configuration-Control allows the correct asset setup comprising all necessary items.
ALC_CMC.4.4C: the CM system shall provide automated measures such that only authorized changes are made to the configuration items.	O.Configuration-Process O.Configuration-Control O.Logical-Access O.Logical-Operation	O.Configuration-Process includes the controls of the production processes. O.Configuration-Control defines the correct setup for each asset, including processes and items for the production. O.Logical-Access and O.Logical-Operation ensure the security support by limiting access to operations only to the authorized staff and requires the authentication of each user before any change can be applied to a configuration item.
ALC_CMC.4.5C: the CM system shall support the production of the *configuration item* by automated means.	O.Configuration-Process O.Zero-Balance O.Organise-Product	O.Configuration-Process includes the controls of the production processes including the automated management of the processes. O.Zero-Balance ensure the control of the secure asset during the production cycle. O.Organise-Product ensures that development and production fulfill the specified process requirements
ALC_CMC.4.6C: the CM documentation shall include a CM plan.	O.Configuration-Control O.Configuration-Process	O.Configuration-Control describes the change management of configuration items. O.Configuration-Process provides the CM plan in use at the site.

SAR	Security Objective	Rationale
ALC_CMC.4.7C: the CM plan shall describe how the CM system is used for the development of the *configuration item*.	O.Configuration-Control O.Configuration-Process	O.Configuration-Control describes the change management of configuration items. O.Configuration-Process provides the CM plan in use at the site.
ALC_CMC.4.8C: the CM plan shall describe the procedures used to accept modified or newly created configuration items *or their components*.	O.Reception-Control O.Configuration-Items O.Configuration-Control O.Configuration-Process	O.Reception-Control ensures the identification of the configuration items managed in LFoundry. O.Configuration-Item ensures the unique identification of each asset produced at LFoundry. O.Configuration-Control ensures a release for each new or changed configuration item. O.Configuration-Process ensures an automated control of the configuration item processing.
ALC_CMC.4.9C: the evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Reception-Control O.Configuration-Control O.Configuration-Process O.Zero-Balance O.Internal-Shipment	O.Reception-Control, O.Configuration-Control, and O.Configuration-Process contribute to ensure control of all configuration items produced and managed. O.Zero-Balance ensure the tracing of all secure assets. O.Internal-Shipment covers internal shipment including packaging requirements, reports, logs and notification.
ALC_CMC.4.10C: the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O.Configuration-Control O.Configuration-Process	O.Configuration-Control includes a release procedure as evidence. O.Configuration-Process ensures the compliance of the process.
ALC_CMS.5.1C: the configuration list shall include the following: *the configuration items*; the evaluation evidence required by the SARs; *the parts that comprise the configuration items*; the implementation representation; security flaw reports and resolution status; and development tools and related information.	O.Configuration-Items O.Configuration-Control O.Configuration-Process	Due to the fact that the process is the object of the evaluation in the configuration list are not mentioned specific products. O.Configuration-Items assures the existence of unique parts ID's and the list of all items and processes for these parts. O.Configuration-Control defines the release process for each client part ID. O.Configuration-Process defines the configuration control including part ID, processes and procedures.
ALC_CMS.5.2C: the configuration list shall uniquely identify the configuration items.	O.Configuration-Items O.Configuration-Control O.Configuration-Process O.Reception-Control O.Internal-Shipment	O.Configuration-Items gets unique identification for configuration items. O.Configuration-Control and O.Configuration-Process support this unique identification by automated tools and a configuration management plan. O.Reception-Control supports the identification of the received items. O.Internal-Shipment defines the labeling and packaging for LFoundry internal transportation.

SAR	Security Objective	Rationale
ALC_CMS.5.3C: for each *configuration item*, the configuration list shall indicate the *developer/supplier* of the item.	O.Configuration-Items O.Configuration-Process O.Reception-Control	O.Configuration-Items identifies all the configuration items defined for secure assets. O.Configuration-Process contains the CM documentation including developer information for each configuration item in the configuration list. O.Reception-Control supports the identification of the received items including supplier information.
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 *configuration items*' design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Maintain-Security O.Control-Scrap	The physical protection is ensured according to the O.Physical-Access which is supported by the O.Security-Control, O.Alarm-Response and O.Maintain-Security. The O.Logical-Access provides the logical protection of data, supported by the O.Logical-Operation where are described logical measures. The O.Staff-Engagement is used to provide the personnel security measures and awareness. O.Control-Scrap ensures that non transferrable parts are properly destroyed.
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 *configuration item*.	O.Internal-Monitor O.Internal-Shipment O.Logical-Operation O.Maintain-Security O.Reception-Control O.Transfer-Data O.Zero-Balance	O.Internal-Monitor and O.Logical-Operation ensure that the security measures in place provide effective protection, supported by O.Maintain-Security. O.Internal-Shipment ensures that configuration items are internally transferred with appropriate security measures. O.Reception-Control and O.Transfer-Data ensure that configuration items are transferred ensuring integrity and confidentiality. O.Zero-Balance ensures that all configuration items are correctly traced.
ALC_LCD.1.1C: the life-cycle definition documentation shall describe the model used to develop and maintain the *configuration item*.	O.Configuration-Control O.Configuration-Process	O.Configuration-Control defines the maintenance of the configuration items. O.Configuration-Process defines the process used for the development of the configuration items.
ALC_LCD.1.2C: the life-cycle model shall provide for the necessary control over the development and maintenance of the *configuration item*.	O.Configuration-Process O.Reception-Control O.Zero-Balance O.Organise-Product	O.Configuration-Process controls the production process. O.Reception-Control ensure the receiving phase is performed adequately. O.Zero-Balance ensure all secure assets are traced. O.Organise-Product ensures that the development and production fulfill the specified process requirements.

The following SARs are not mapped since ALC_TAT and ALC_DEL are not applicable as detailed in section **Error! Reference source not found.**: ALC_TAT.2.1C, ALC_TAT.2.2C, ALC_TAT.2.3C, ALC_DEL1.1C.

8. LFoundry Summary Specification

8.1. Preconditions Required by the Site

The LFoundry site covers parts of the life cycle phase 3 related to the integration for the photomask fabrication and the IC production. The security certifications owned by the clients' and suppliers' sites for their internal management and processing of physical and logical goods, as well as for exchanging items with LFoundry, are adequate to ensure that the confidentiality and integrity of the items exchanged between LFoundry and its clients or suppliers are not compromised by any activity that is not under LFoundry direct control (A.Security). In addition to this, no additional vulnerabilities are added during the integration for the photomask fabrication performed by the Data Preparation process (A.Design-Integration). All information relating to the execution of the testing phase, which includes the inoculation of the software inside the device and the functional testing, are entrusted to Test House directly by the client which is responsible for this phase (A.Product-Test).

The client provides adequate information to setup and control the process (A.Product-Specification); this includes the photo mask identification, the specification of the mask set and the options supported by the production process. This also includes the GDS2 file identification, the photo mask identification, the specification of the mask set, and the options supported by the production process (A.Item-Identification).

The LFoundry production process includes both the tool configuration and set-up for the GDS2 file integration using the received GDS2 file as well as tool configuration (A.Product-Specification). Within the production process are included the parameters and limits that must be fulfilled by the photo mask that are used at the site. The Photo Shop responsibility is to ensure the delivery of appropriate photo masks (A.Mask-Support) and the related labeling (A.Item-Identification).

Included within the photo masks there is the security classification (A.Item-Identification) that allows the handling according to the specific roles for this security classification. LFoundry uses its own standard procedure for packing of finished goods (wafers) and preparation of shipment. If the client needs special packing requirements they are provided by the client (A.Product-Specification) and are included in the process setup. For each asset the client must provide the destination for the shipment of the finished wafers (A.Internal-Shipment). In addition, the client must define the additional packaging requirements needed to support the confidentiality and integrity of the asset (A.Product-Specification).

8.2. Services of the Site

LFoundry produces IC on wafers, based on a released enhanced CMOS process. The development process for devices using this production process is supported by an appropriate gate library. LFoundry has capability for integrate proprietary module with customer's ones.

LFoundry site provides three services.

Data Preparation service at Landshut site: the client sends to LFoundry (Landshut site) the device design (GDS2) in order to integrate it with the LFoundry property modules and build the mask layout to be produced by the Mask Shop.

Wafer Manufacturing at Avezzano site: wafers with Security ICs are built according to the received specifications.

RMA analysis at Avezzano site: LFoundry Laboratory provides investigation on RMA to analyze the cause of functional failures found during processes performed after the end of the production cycle of LFoundry.

8.3. Objectives Rationale

8.3.1. O.Alarm-Response

Assigned personnel of the site or guards operate the security systems like access control and surveillance and respond to alarms. The physical alarm system is connected to a Security Control Room and in case of Avezzano site this is linked with the CCTV monitoring system. This allows the guards getting an immediate control of a potential security breach and the reaction time to a security breach is short enough to prevent a successful physical attack. In case of Avezzano site the alarm and monitor system is integrated by a patrolling through the sensitive areas done by armed guard. Failure of physical access authentication is logged and monitored.

Threats addressed: T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.2. O.Configuration-Control

Procedures in place support a documented release of configuration documents and specifications for set-up of wafer production. Engineering Change Notifications are in place to classify and introduce changes. The system implemented for the Engineering Change Notifications utilization requires individual access controlled by passwords and provides to each user the access rights based on “need to know” principle, thereby only authorized changes are possible.

Threat addressed: T.Accident-Change

Supporting OSPs: P.Configuration-Control, P.Reception-Control

8.3.3. O.Configuration-Items

Assets are identified by unique client part IDs which are linked to the unique ID numbers of the associated configuration items. Actions in production environment are performed by the responsible using automated tools and reading IDs with bar code readers.

Threat addressed: T.Accident-Change

Supporting OSPs: P.Configuration-Control, P.Configuration-Item

8.3.4. O.Configuration-Process

The released configuration information, including production and acceptance specifications, is automatically associated to every configuration item. The production set-up and the controlling measurements, that ensure the compliance with the specification, are automatically loaded to the production tool according to the configuration information of the configuration item to be processed.

Threat addressed: T.Accident-Change

Supporting OSPs: P.Configuration-Process, P.Reception-Control

8.3.5. O.Control-Scrap

Any scrap is identified uniquely, is handled in the same way as any configuration items, and is stored internally in a secure location until it is destroyed. Upon client request, the scrap is shipped to the client instead of being destroyed. Sensitive information and information storage media are collected internally in a safe location and destroyed following a documented process.

Threat addressed: T.Staff-Collusion

Supporting OSP: P.Zero-Balance

8.3.6. O.Internal-Monitor

Security management meetings are held on regular basis to monitor security issues as well as changes or updates of security relevant processes. This comprises also logs' controls and security events of security relevant systems like access control system, information systems monitoring, and information security systems. Mayor changes of security systems and security procedures are reviewed and approved by the deputy authorities. In addition to the described activities, the application of the security measures is controlled with appropriate audit.

Threats addressed: T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.7. O.Internal-Shipment

Packing procedures and internal shipment are regulated by specific procedures and documented in the asset configuration. This includes a possible specific requirement of the customer.

Threat addressed: T.Attack-Transport

Supporting OSP: P.Product-Transport

8.3.8. O.Logical-Access

A firewall separates the internal network from the internet and connection to internal network is protected by authentication measures. The internal network is appropriately separated to prevent interference between the production and the office environment. The separation of the network is logical (e.g. by a firewall or VLAN). Each user owns a personal username and password to access network resources and the access is based on the "need to know" principle after appropriate approval process.

Threats addressed: T.Accident-Change, T.Computer-Net, T.Unauthorized-Staff

Supporting OSPs: P.Configuration-Control, P.Organise-Product

8.3.9. O.Logical-Operation

All logical protection measures are maintained and updated as required on regular basis. Secure configuration items or classified data are managed with dedicated infrastructure and encryption tools which are applied to both production environment and backup.

Threats addressed: T.Accident-Change, T.Computer-Net, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.10. O.Maintain-Security

The systems enforcing or supporting security access, security control, and logical access are monitored, maintained and reviewed on regular basis. The systems' configuration is updated as required by employees or suppliers under employees' review.

Threats addressed: T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.11. O.Organise-Product

Technical and organizational tools are used to ensure that the development and production of the configuration items fulfill the specified process requirements. This includes measurements of physical characteristic of the wafers as provided by the client specification and in case a wafer is found non conformant then it became a scrap and it is handled accordingly to O.Control-Scrap.

Threat addressed: T.Accident-Change

Supporting OSP: P.Organise-Product.

8.3.12. O.Physical-Access

LFoundry Landshut Design site is within one building while LFoundry Avezzano Manufacturing site, being formed by several buildings, is surrounded by a fence. The access is allowed only through controlled gates. The access control and security checks to the gates are aimed to ensure that only registered persons can access sensitive areas and the contained configuration items. The gates and the critical areas of the sites are under a CCTV control system and an anti-intrusion alarm system.

At Avezzano site the security systems are monitored by security guards 24x7; the highest sensitive areas have all the entrance points alarmed and such areas are accessible only through a strong authentication system.

At Landshut site the highest sensitive area has the entrance points controlled by security control systems; the security systems are monitored by security guards when no staff is present at the site.

Threats addressed: T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.13. O.Reception-Control

At reception each configuration item is identified by the shipping documents, and packaging labels. Inspection at reception is counting the number of boxes and checking the integrity of security seals of these boxes if applicable. Thereby only correctly identified items are accepted for production.

Physical acceptance tests are performed on incoming raw materials based on the related client's specifications. The test results are logged to support tracing and the identification of systematic failures.

Threats addressed: T.Attack-Transport, T.Rugged-Theft

Supporting OSPs: P.Configuration-Items, P.Reception-Control

8.3.14. O.Security-Control

Technical and organizational security measures ensure that reaction time to a security breach is short enough to prevent a successful physical attack. In case of LFoundry Avezzano Manufacturing site, the security team ensures a patrolling of the critical areas and monitors the site 24 hours a day with the support of a CCTV control system and an anti-intrusion alarm system. In case of Landshut site, the guards monitor the site when no staff is present at the site.

Threats addressed: T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff

Supporting OSP: P.Security-Control

8.3.15. O.Staff-Engagement

All employees are interviewed and scrutinized before hiring. They must sign a NDA, which is integrated in the employee's contract, and a code of conduct before they start working at the company. The formal training and qualification covers also security relevant subjects, including physical and electronic security measures and procedures used within LFoundry and the principles of handling, storing and disposal of security assets.

Threats addressed: T.Rugged-Theft, T.Staff-Collusion

Supporting OSPs: P.Product-Transport, P.Security-Control, P.Zero-Balance

8.3.16. O.Transfer-Data

The security and integrity of the data transferred from/to the site (specifically GDS2 data and mask data) and within the site is ensured by defined protocols and measures, including eventual specific client requirements. The highest sensitive data is transferred using cryptographic techniques.

Threats addressed: T.Attack-Transport, T.Staff-Collusion

Supporting OSP: P.Transfer-Data

8.3.17. O.Zero-Balance

The site ensures that configuration items are uniquely identified and tracked throughout the entire process. Handover and storage of configuration items is controlled and documented. Scraps are monitored and identified through the whole production process. At every process step the registration of good and scrapped wafers is updated. A zero balance calculation exists and documents the history of good and bad wafers. Documentation is kept and is available for each wafer.

Threats addressed: T.Rugged-Theft, T.Staff-Collusion

Supporting OSP: P.Zero-Balance.

8.4. Security Assurance Requirements Rationale

The Security Assurance Rationale given in section 7.2 provides the justification for the selected SARs. Considering that the SARs are compliant with the EAL5 augmented by ALC_DVS.2 all derived dependencies are to be considered fulfilled.

The SARs are taken from [CCPart3] with the term TOE replaced by configuration items in most cases while in specific cases it is replaced by product. The content elements that are changed from the original [CCPart3] are written in *italic*.

8.4.1. ALC_CMC.4

ALC_CMC.4.1C: the *configuration item* shall be labeled with its unique reference.
ALC_CMC.4.2C: the CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C: the CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C: the CM system shall provide automated measures such that only authorized changes are made to the configuration items.
ALC_CMC.4.5C: the CM system shall support the production of the *configuration item* by automated means.
ALC_CMC.4.6C: the CM documentation shall include a CM plan.
ALC_CMC.4.7C: the CM plan shall describe how the CM system is used for the development of the *configuration item*.
ALC_CMC.4.8C: the CM plan shall describe the procedures used to accept modified or newly created configuration items or part of them.
ALC_CMC.4.9C: the evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C: the evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

The assurance level ALC_CMC.4 of the assurance family "CM capabilities" is suitable to support the production of wafers due to the acceptance process and the automated support. The identification of all configuration items supports an automated production process. The requirement for authorized changes supports the confidentiality and integrity required for the assets. Therefore, these SARs meet the requirements for the configuration management.

8.4.2. ALC_CMS.5

ALC_CMS.5.1C: the configuration list shall include the following: *the configuration items*; the evaluation evidence required by the SARs; *the parts that comprise the configuration items*; the implementation representation; security flaw reports and resolution status; 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/supplier* of the item.

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

8.4.3. ALC_DEL.1

The CC assurance component ALC_DEL.1 refers to the external delivery of the configuration items or parts of them to the consumer or consumer's site. Procedures and technical measures for external delivery of asset or part of it are required to maintain the confidentiality and integrity of the asset.

LFoundry site is not involved in external delivery since does not provide any configuration item to the consumer, so ALC_DEL.1 is out of scope for this certification. Moreover, ALC_DEL.1 cannot be used for internal shipment which is instead covered by ALC_DVS.2.

However, the component ALC_DEL.1 is included here to support the reuse of the evaluation results.

8.4.4. ALC_DVS.2

ALC_DVS.2.1C: the development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *configuration items'* 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 *configuration item*.

The configuration items and information handled at the site during production can be used by potential attackers for the development of attacks. Therefore, the handling and storage of these items must be sufficiently protected.

8.4.5. ALC_LCD.1

ALC_LCD.1.1C: the life-cycle definition documentation shall describe the model used to develop and maintain the *configuration item*.

ALC_LCD.1.2C: the life-cycle model shall provide for the necessary control over the development and maintenance of the *configuration item*.

The assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process; in this are included the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of Security ICs the focus is limited to this site.

8.4.6. ALC_TAT.2

The CC assurance components of family ALC_TAT refer to the tools that are used to develop analyze and implement the TOE.

Since the site covers parts of the life cycle phase 3 related to the integration and photomask fabrication and IC production, the site does not cover any aspects that are covered by ALC_TAT so the assurance component ALC_TAT.2 is not applicable.

The site ensures only a reproducible production process within the limits defined for the released wafer production process. Relevant parameters are controlled during the production process and this is subject of the configuration management.

However, the component ALC_TAT.2 is included here to support the reuse of the evaluation results.

8.5. Assurance Measure Rationale

Mapping of Assurance Components and Security Objectives is reported in **Error! Reference source not found.**.

The SARs are taken from [CCPart3] with the term TOE replaced by configuration items in most cases while in specific cases it is replaced by product.

8.5.1. O.Alarm-Response

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SAR.

8.5.2. O.Configuration-Control

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.4.3C requires that the CM system shall uniquely identify all configuration items.

ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.

ALC_CMC.4.6C requires a CM documentation that includes a CM plan.

ALC_CMC.4.7C requires that the CM plan describes how the CM system is used for the development of the configuration items.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items or their components.

ALC_CMC.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMS.5.1C requires that the configuration list shall include the configuration items, the evaluation evidence required by the SARs, the parts that comprise the configuration items, the implementation representation, security flaw reports and resolution status, and development tools and related information.

ALC_CMS.5.2C requires that the configuration list uniquely identifies the configuration items.

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

Thereby this objective contributes to meet the above SARs.

8.5.3. O.Configuration-Items

ALC_CMC.4.1C requires that the configuration items shall be labelled with its unique reference.

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.4.3C requires that the CM system shall uniquely identify all configuration items.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items or their components.

ALC_CMS.5.1C requires that the configuration list shall include the configuration items, the evaluation evidence required by the SARs, the parts that comprise the configuration items, the implementation representation, security flaw reports and resolution status, and development tools and related information.

ALC_CMS.5.2C requires that the configuration list uniquely identifies the configuration items.

In ALC_CMS.5.3C the configuration list shall indicate the developer/supplier for each configuration item.

Thereby this objective contributes to meet the above SARs.

8.5.4. O.Configuration-Process

ALC_CMC.4.4C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items.

ALC_CMC.4.5C requires that the CM system supports the production of the configuration items by automated means.

ALC_CMC.4.6C requires a CM documentation that includes a CM plan.

ALC_CMC.4.7C requires that the CM plan describe how the CM system is used for the development of the configuration items.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items or their components.

ALC_CMC.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMC.4.10C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

ALC_CMS.5.1C requires that the configuration list shall include the configuration items, the evaluation evidence required by the SARs, the parts that comprise the configuration items, the implementation representation, security flaw reports and resolution status, and development tools and related information.

ALC_CMS.5.2C requires that the configuration list uniquely identifies the configuration items.

ALC_CMS.5.3C requires that the configuration list indicates the developer/supplier for each configuration item.

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

ALC_LCD.1.2C requires that the life-cycle model provides control over the development and maintenance of the configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.5. O.Control-Scrap

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SAR.

8.5.6. 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 configuration items.

Thereby this objective contributes to meet the above SAR.

8.5.7. O.Internal-Shipment

ALC_CMC.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMS.5.2C requires that the configuration list uniquely identifies the configuration items.

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 configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.8. O.Logical-Access

ALC_CMC.4.4C requires that the CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SARs.

8.5.9. O.Logical-Operation

ALC_CMC.4.4C requires that the CM system shall provide automated measures such that only authorized changes are made to the configuration items.

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

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 configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.10. O.Maintain-Security

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

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 configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.11. O.Organise-Product

ALC_CMC.4.5C requires that the CM system supports the production of the configuration items by automated means.

ALC_LCD.1.2C requires that the life-cycle model provides control over the development and maintenance of the configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.12. O.Physical-Access

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SAR.

8.5.13. O.Reception-Control

ALC_CMC.4.1C requires that the configuration items shall be labelled with its unique reference.

ALC_CMC.4.2C requires a CM documentation that describes the method used to uniquely identify the configuration items.

ALC_CMC.4.3C requires that the CM system shall uniquely identify all configuration items.

ALC_CMC.4.8C requires the description of the procedures used to accept modified or newly created configuration items or their components.

ALC_CMC.4.9C requests evidence demonstrating that all configuration items are being maintained under the CM system.

ALC_CMS.5.2C requires that the configuration list uniquely identifies the configuration items.

ALC_CMS.5.3C requires that the configuration list indicates the developer/supplier for each configuration item.

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 configuration items.

ALC_LCD.1.2C requires that the life-cycle model provides control over the development and maintenance of the configuration items.

Thereby this objective contributes to meet the above SARs.

8.5.14. O.Security-Control

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SAR.

8.5.15. O.Staff-Engagement

ALC_DVS.2.1C requires that security documentation describes physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the configuration items' design and implementation.

Thereby this objective contributes to meet the above SAR.

8.5.16. 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 configuration items.

Thereby this objective contributes to meet the above SAR.

8.5.17. O.Zero-Balance

ALC_CMC.4.5C requires that the CM system supports the production of the configuration items by automated means.

ALC_CMC.4.9C requests evidence demonstrating 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 configuration items.

ALC_LCD.1.2C requires that the life-cycle model provides control over the development and maintenance of the configuration items.

Thereby this objective contributes to meet the above SARs.

8.6. Mapping of the Evaluation Documentation

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

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

9. References

9.1. Literature

[CCPart1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012

[CCPart2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012.

[CCPart3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology (CEM); Version 3.1, Revision 4, September 2012 has been taken into account.

[CCDB] Supporting Document Guidance - Site Certification - October 2007 - Version 1.0 - Revision 1.

[Tech] Technical information on the IT security certification of assets, protection profiles and sites (including confirmations in accordance with SigG) - Bundesamt für Sicherheit in der Informationstechnik BSI 7138 - Version 2.1, as per 5 November 2012.

[GuideST] Guidance for Site Certification - Version 1.1 - 2013-12-04 - Bundesamt für Sicherheit in der Informationstechnik.

[Sec_IC] Security IC Platform Protection Profile Version 1.0 15.06.2007, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.

[GuideDev] Guidelines for Developer Documentation according to Common Criteria Version 3.1 - Version 1.0 – 2007.

9.2. Definitions

According to the reserved use of the words “customer” and “consumer” in the CC in this document the word “client” is used instead of customer.

9.3. List of Abbreviations

CEO	Chief of Executive Officer
EHSS	Environment Health Safety Security
CC	Common Criteria
EAL	Evaluation Assurance Level
GDS2	Graphic Database System 2
IC	Integrated Circuit
ICT	Information & Communication Technology
ID	Identification Data

OSP	Organizational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
RMA	Return Material Authorization
SAR	Security Assurance Requirement
SST	Site Security Target
TOE	Target of Evaluation