Public

Common Criteria Information Technology Security Evaluation

Samsung Giheung & Hwaseong

(Line 3, Line 5, SR1, SR3 and DSR-B building)

Version 2.0

14th March 2025

SST-lite(Site Security Target-lite)

SAMSUNG ELECTRONICS

SAMSUNG

Important Notice

Samsung Electronics Co. Ltd. (“Samsung”) reserves the right to make changes to the information in this publication at any time without prior notice. All information provided is for reference purpose only. Samsung assumes no responsibility for possible errors or omissions, or for any consequences resulting from the use of the information contained herein.

This publication on its own does not convey any license, either express or implied, relating to any Samsung and/or third-party products, under the intellectual property rights of Samsung and/or any third parties.

Samsung makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Samsung assume any liability arising out of the application or use of any product or circuit and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Customers are responsible for their own products and applications. "Typical" parameters can and do vary in different applications. All operating parameters, including "Typicals" must be validated for each customer application by the customer's technical experts.

Samsung products are not designed, intended, or authorized for use in applications intended to support or sustain life, or for any other application in which the failure of the Samsung product could reasonably be expected to create a situation where personal injury or death may occur. Customers acknowledge and agree that they are solely responsible to meet all other legal and regulatory requirements regarding their applications using Samsung products notwithstanding any information provided in this publication. Customer shall indemnify and hold Samsung and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim (including but not limited to personal injury or death) that may be associated with such unintended, unauthorized and/or illegal use.

Samsung Electronics Co., Ltd.
San #24 Nongseo-Dong, Giheung-Gu
Yongin-City, Gyeonggi-Do, Korea 446-711

Contact Us: *junghyun.kim@samsung.com*

Home Page: *http://www.samsungsemi.com*

Chip Handling Guide

Precaution against Electrostatic Discharge

When using semiconductor devices, ensure that the environment is protected against static electricity:

1. Wear antistatic clothes and use earth band.
2. All objects that are in direct contact with devices must be made up of materials that do not produce static electricity.
3. Ensure that the equipment and work table are earthed.
4. Use ionizer to remove electron charge.

Contamination

Do not use semiconductor products in an environment exposed to dust or dirt adhesion.

Temperature/Humidity

Semiconductor devices are sensitive to:

- Environment
- Temperature
- Humidity

High temperature or humidity deteriorates the characteristics of semiconductor devices. Therefore, do not store or use semiconductor devices in such conditions.

Mechanical Shock

Do not to apply excessive mechanical shock or force on semiconductor devices.

Chemical

Do not expose semiconductor devices to chemicals because exposure to chemicals leads to reactions that deteriorate the characteristics of the devices.

Light Protection

In non- Epoxy Molding Compound (EMC) package, do not expose semiconductor IC to bright light. Exposure to bright light causes malfunctioning of the devices. However, a few special products that utilize light or with security functions are exempted from this guide.

Radioactive, Cosmic and X-ray

Radioactive substances, cosmic ray, or X-ray may influence semiconductor devices. These substances or rays may cause a soft error during a device operation. Therefore, ensure to shield the semiconductor devices under environment that may be exposed to radioactive substances, cosmic ray, or X-ray.

EMS (Electromagnetic Susceptibility)

Strong electromagnetic wave or magnetic field may affect the characteristic of semiconductor devices during the operation under insufficient PCB circuit design for Electromagnetic Susceptibility (EMS).

Revision History

Revision No.	Date	Description
2.0	14th March 2025	Creation for initial version

Table of Contents

List of Figures

Figure Number	Title	Page Number

N/A

List of Tables

List of Conventions

Register RW Access Type Conventions

Type	Definition	Description
R	Read Only	The application has permission to read the Register field. Writes to read-only fields have no effect.
W	Write Only	The application has permission to write in the Register field.
RW	Read & Write	The application has permission to read and writes in the Register field. The application sets this field by writing 1'b1 and clears it by writing 1'b0.

Register Value Conventions

Expression	Description
x	Undefined bit
X	Undefined multiple bits
?	Undefined, but depends on the device or pin status
Device dependent	The value depends on the device
Pin value	The value depends on the pin status

Reset Value Conventions

Expression	Description
0	Clears the register field
1	Sets the register field
x	Don't care condition

Warning: Some bits of control registers are driven by hardware or write operation only. As a result the indicated reset value and the read value after reset might be different.

List of Terms

Terms	Descriptions
Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Composite Product Integrator	Role installing or finalising the IC Embedded Software and the applications on platform transforming the TOE into the unpersonalised Composite Product after TOE delivery. The TOE Manufacturer may implement IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer)
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialisation Data	Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Pre-personalisation Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
TOE Delivery	The period when the TOE is delivered which is either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled. The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance E2PROM) or a combination thereof.
User data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

List of Acronyms

Acronyms	Descriptions
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Feature
TSFI	TSF Interface
TSP	TOE Security Policy

1 DOCUMENT INFORMATION

1.1 Reference

Reference	
Title	Site Security Target-lite of Samsung Electronics Giheung & Hwaseong
Version	Version 2.0
Date	14th March 2025
Company	Samsung Electronics Co., Ltd.
Name of the Site	Samsung Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)
Product type	AP Hardware Development and Production
EAL-Level	EAL6

1.2 List of Abbreviations

Acronyms	Description
CC	Common Criteria
EAL	Evaluation Assurance Level
IC	Integrated Circuit
IT	Information Technology
OSP	Organization Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SST-lite	Site Security Target-lite
ST	Security Target
TOE	Target of Evaluation
AP	Application Processor
ERP	Enterprise Resource Planning
SIMAX	Samsung Integrated Manufacturing Execution System
YMS	Yield Management System
SMOS	Samsung Mobile Operation System
FBGA	Fine Ball Grid Array
BGA	Ball Grid Array
COB	Chip On Board
NFC	Near Field Communication
PCN	Product / Process Change Notice
ECID	Exclusive Chip Identification
Smart D&E	Semiconductor's Methodology of Architecture/Research/Technology Devlopment & Engineering

2 INTRODUCTION

This Site Security Target-lite refers to the site 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'.
The site can be part of the production flow of the Security IC modules for AP and IT Security Products.

2.1 Identification of the Site

1 The site 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' is located at:

- Samsung Electronics. Co., Ltd. (Hwaseong), DSR building

  1-1, Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do,
  18448 Republic of Ko-rea
- Samsung Electronics. Co., Ltd. (Giheung),

  Samsung-ro, Giheung-gu, Yongin-si, Gyeonggi-do,
  17113 Republic of Korea

2.2 Site Description

2 Some parts of the buildings specified in Section 2.1 are in the scope of the SST=lite. But, the entire site area is protected by two surrounding fences. One fence covers overall manufacturing building areas including the scrap house, the other fence covers the Stock.

3 The site comprises the design center, test program development, some production facilities, some data centers and the SOC.

4 In the following sections, the physical and logical scope of the SST-lite is defined.

2.3 Physical Scope

Site / Building	Purpose	Asset
Hwaseong Plant/ DSR Building (DSR-B 17th floor)	Design Center (GDS integration, Ebeam generation and engineer testing)	Design-related Data
Giheung Plant/ SR3 Building (6th floor)	Test program development	Test program
Giheung Plant/ Line 5 (2th floor)	Bump Fabrication	Process Data and Spec., Wafers/scrap in TEST mode, Mask (Reticle), Scrap(Reject) Mask
Giheung Plant/ Line 3 (2th floor)	Wafer EDS Test	Wafer in TEST mode Packaged wafer
Giheung Plant/ SR1 Building (2th floor)	Data preparation	Data
Hwaseong Plant/ DSR Building (DSR-B 2nd floor)	Security Operation Center DSR Building	CCTV Records & access control logs
Giheung Plant/ Control Building (2nd floor)	Security Operation Center Giheung	CCTV Records & access control logs
Giheung Plant/ Line 6 (6th floor)	Data center Giheung	Production data + test data
Hwaseong Plant/ DSR Building (DSR-B 5th floor)	Data center DSR Building	Development data

2.4 Logical Scope

5 SIMAX, Smart D&E and ERP system supports overall employee activities including all production, processes, products, delivery and security controls.

6 The following services and/or processes provided 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' is in the scope of the site evaluation process.

Giheung:

1) Bump fabrication
2) Wafer EDS test,
3) Test program development
4) Data handling and preparation

Hwaseong:

5) Integration of GDS files for full AP chip,
6) GDS file checking and optimisation for mask data generation (Ebeam eneration),
7) Engineer testing

7 The process flow of security product fabricated by the site is as follows. The client transfers the encrypted GDS files to Hwaseong DSR-B and then, the GDS integration and the Ebeam generation is performed in this building.

8 The Ebeam is transferred by SFTP to Giheung SR1 for the data handling and preparation, then it is sent by FTP to customer for the mask production. Depending on the type of mask, they are sent to Giheung Line 5 directly, where the bump fabrication is performed or they are sent to customer first, where the wafer fabrication is performed.

9 The engineer testing for analyzing in the testing lab room

10 Finally, the wafers arrive to Giheung Line 3 where the wafer EDS tests are performed. This test are developed in Giheung SR3.

11 The complete logical flow explained previously is covered by the SST. In addition, the management of the Security IC modules for AP and IT Security Products processes and the site security are covered by the SST. The product flow of the Security IC modules for AP and IT Security Products on the site starts with the receipt of parts of the TOE (raw materials) up to the yield measurement and handover for shipment of the finished goods for Security IC modules for AP and IT Security Products.

12 Security Controlled Access: (Security-Guard, IC-Card, CCTV) When the intrusion happened at the external or secured doors using un-authorized IC-Card, the real-time alarm is informed to the Central security system.

13 Shipment Transport Control: (Access Control, CCTV Surveillance Systems, Patrol Officers). Service and delivery vehicles are tracked and only verified forwarder are used.

14 Stock Control: Security guard surveillances cover the loading dock 24hours / 7days. Only authorized employees and escorted visitors are permitted to access to the Stock.

15 Automation Control: Possible human errors during the following life cycle phases of the Security IC modules for Smart Card, NFC (Near field communication) and IT Security Products are fended off by the automation of the handling procedure.

16 The site contribute to following life cycle phases:
Life cycle:

- Phase 2: IC Development.
- Phase 3: IC Manufacturing.

3 CONFORMANCE CLAIM

17 The evaluation is based on Common Criteria Version 3.1, release 5

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

18 The SST-lite is CC Part 3 conformant.

19 For the evaluation the following methodology will be used:

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

20 The evaluation of the site comprises the following assurance components:
1) ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_TAT.3 and ALC_LCD.1.

21 The assurance level chosen for the SST-lite are taken from the definition of the EAL6 package defined in [2].

22 ALC_DEL.1 is not covered with this certification, as the transportation of wafers between different development sites are not considered here, but in the family Development security (ALC_DVS).

23 For the assessment of the security measures attackers with high attack potential are assumed. This allows an evaluation of products using this site according to the assurance component AVA_VAN.5.

4 SECURITY PROBLEM DEFINITION

24 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 products and the security management of the site.

25 This Site Security Target-lite is based on the life-cycle defined in the Security IC Platform Protection Profile [6]. The assets (Section 4.1), threats (Section 4.2) and Organizational Security Policies (OSP) (Section 4.3) defined in this template are derived from the life-cycle defined in that PP.

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

4.1 Assets

27 The following section describes the assets handled at the site.

28 The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security concepts and the associated security measures.

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

30 The following assets are defined as the assets to be protected during producing the products in the site.

1) Development and implementation data (GDS and Mask data),
2) Specifications and Documentation,
3) Masks,
4) Wafers,
5) Test Program

4.2 Threats

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

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

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

33 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, unregistered or defect wafers or dice that can be used to further investigate the functionality of the device and search for possible vulnerabilities. Such an attacker will provide notable risk.

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

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

35 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 considered to be sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. Those attackers are considered to have the highest attack potential.

36 Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special measures like storage of items in safes or strong rooms or the splitting of sensitive data like keys provide additional support against such attacks.

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 other sensitive production and/or development data or modify the production and/or development process at the site.

37 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. 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.

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

39 The protective concept with more than one level is expected in order to protect the manufacturing operation system network. This shall comprise a firewall to the external network, and further limitations of the network users and the network services for internal sub-networks. In addition, computer users shall have individual accounts which require authentication using e.g. a password.

T. Accident- Change - An employee, contractor may exchange products of different production lots or different clients during production by accident.

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

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

T. Unauthorized-Staff - Unauthorized Employees or subcontractors try to get access to the products, or affect production systems or configuration systems.

As a result of their access the confidentiality and/or the integrity of the product could be violated and affected to make changes to any production step and any configuration item of the final products

42 Especially maintenance tasks of subcontractors may require the access to computer systems storing sensitive data. The implemented security measures may not work because a special dedicated access may be used to the network or specific tools may be used for this dedicated task. This comprises e.g. tools which process the layout data e.g. in the assembly.

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

44 The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to this different measure are required.

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

45 Personal accountability shall be traceable as far as possible. Handover procedures with dual control, enforcement of parallel access by two authorized employees and the split of sensitive knowledge like

personalization keys can be implemented to prevent such an attack. The measures depend on the assets that must be protected at the site.

T. Attack-Internal-Transport - 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 process to allow a modification, cloning or the retrieval of confidential information at later life cycle states. Confidential information comprises design information, documentation and data as far as classified as sensitive.

46 The protection of the internal shipment is based on the configuration of the products that are manufactured in 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'.

T. Delivery-Accidents – During the overall delivery procedure, any personnel including the logistics, forwarders and drivers could make an unwanted human error – a product mix, a product quantity inconsistency, destination error, It violate the integrity and the availability of the TOE.

47 Because even experienced personnel could make mistake during delivery procedure, mistake proofing measures shall be considered - the delivery planning using ERP, shipping process automation, dual personnel control of the handover.

T. Attack–External-Transport - An attacker might try to make an intentional car accident and access to the TOE after breaking down the key and opening the door of the truck during the delivery route. The target is to access to the TOE and violate the integrity or availability of them.

48 During the delivery procedure outside of the company, various vehicle attacks could be happened, therefore the site shall monitor the vehicle status and control the emergency situation.

4.3 Organizational Security Policies

49 The following policies are introduced by the requirements of the assurance components of ALC for the assurance level EAL6.

The chosen policies shall support the understanding of the production flow and the security measures of the site. In addition, they shall allow an appropriate mapping to the Security Assurance Requirements (SAR).

50 The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding production process of the product and mask that are in the scope of the evaluation.

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

51 The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receipt and the item each item is assigned to an internal unique identification. For configuration items that are

created, generated or developed at the site the naming and identification must be specified.

P. Config-Control - The procedures for setting up the production process for a new product as well as the procedure that allows changes of the initial setup for a product shall only be applied by 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 developer.

52 The product setup may include the following information

1) Product Id (Part Number)
2) Properties of the final product
3) Mask set IDs
4) Any configuration of the processed item as part of the services provided by the site

P. Config-Process - The services and/or processes provided by a site are controlled in the configuration management plan. This comprises tools used for the assembly 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.

53 The documentation with the process descriptions and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is ensured. In most cases tools are used to support the processes at the site.

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 clients. Furthermore, it is verified that the product can be identified and a released production process is defined for the product. If applicable this aspect includes the check that all required information and data is available to process the items.

P. Accept-Product - The quality control of the site ensures that the released products comply with the specification agreed with the client. The acceptance process is supported by automated measures. Records are generated for the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when internally shipped.

P. Zero-Balance - The site ensures that all sensitive items are separated and traced on a process and product basis. For each hand-over, either an automated or an organizational "two - employees acknowledgement" (four - eyes principle) is applied for functional and defect assets. According to the released production process the defect assets are scrapped into the designated box and moved to the destruction-house along with security guard.

54 The following policy covers the packing and handover of products at the site after the applied

production flow.

55 All finished products in the line are moved to the Stock using a rocked vehicle from the line to the Stock and then stored in the Stock for a few days until the delivery order is issued.

P. Product-Transport Technical and organizational measures ensure the correct labeling of the product. The products are packed as required by the client. A forwarder selected by the client is verified before the handover of security products. Measures to support traceability during the transport are applied by a controlled internal shipment.

56 The following policy supports the electronic transfer of sensitive assets as specified in section 4.1.

P. Data-Transfer - Any data in electronic form (e.g. product specifications, release information etc.) that is classified as sensitive or higher security level by the client is encrypted to ensure confidentiality of the data.

4.4 Assumptions

57 Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/subcontractor. This is reflected by the assumptions defined below for the interface with 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'.

A. Item-Identification Each configuration item received by the site is appropriately labeled and informed on SIMAX system to ensure the identification of the configuration items.

A. Product-Spec The client must provide appropriate specification and relative production information.

The provided information includes the classification of the delivered items, documents, drawings and data.

The client has to define the Mask house which should be used for mask production.

To be able to exchange data securely, the necessary keys have to be exchanged.

The site does not provide any mask production service, only data prep services are offered. The client is responsible to select the mask shop.

The site does provide wafer test services. If the optional service of inking is used, the client is responsible to provide a wafer map indicating good and bad dies.

A.Internal-Shipment The recipient of the products and rejects is well-defined by the client. The client provides the address and shipping information (e.g., selected forwarder) via a reliable channel to the site. The client defines the requirements for packing of the products. The client takes care for secure transportation to/from the site.

The client has to provide data according to the respective classification, e.g. in encrypted form.

A.Destruct-Scrap: Either scrap is transferred to the client or scrap is destructed at the site. The selected option is defined as part of the product spec.

58 The above assumptions are explained to the clients by means of communication with a developer during the sample evaluation step and also explained by the PCN procedure during the client's audit.

5 SECURITY OBJECTIVES

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

O. Physical-Access - Buildings or facilities are installed with physical security systems so that only authorized personnel can be allowed to physically access into the areas set by access control devices. The access control devices equipped in each site of the buildings or the facilities are controlled in order to allow entrance to the areas to only essential personnel who need to do their jobs and very limited number of persons are granted to access to important control areas. Persons who are registered to have authorization to access to each control area shall be reviewed periodically to make sure that restriction of their authority to access is properly controlled.

O. Security-Control - Building entrances are guarded by security personnel and security personnel are to perform access control for visitors or unauthorized persons to the buildings or the facilities and to inspect carrying-out goods out of the buildings or the facilities. Security Command Center is used to monitor CCTV along with alarm sensors located at important sites in order to keep monitoring risks or emergencies and to take actions to deal with the situations. Security Officers ensure that all the persons including visitors, vendors, contractors, etc. are checked and inspected for controlling their access.

Building entrance is allowed to the restricted person who have registered according to their visiting purpose and then monitored with CCTV under the surveillance of Security Command Center. Security Guard is working in the first floor of every manufacturing-buildings and Stock, and in front of the scrap house to take action against possible risks or emergencies and check the quantity of security products during loading and unloading.

O. Alarm-Response - Alarm systems are under the normal operation all the time during office hours and after office hours, and the alarm systems are connected to Security Command Center for around-the-clock monitoring and controlling. During the hours when officers are off duty and the hours at night, extra patrols by Security Officers are performed to monitor specific areas, as well. In any case when an intruder approaches to the facilities with bad motives, alarm systems are utilized to enhance prevention effects by generating warning signals to prevent his/her approaches to the facilities and his/her attempts to break or destroy entrance gates.

O. Internal-Monitor - The site performs security management meetings at every weeks. 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 a sufficient protection.

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

O. Logical-Access - The site enforces a logical separation between the internal network and the internet by a firewall. The firewall ensures that only defined services and defined connections are accepted. Additionally, the internal network is divided into a production network and an office network. Only authorized employees who work for the production line and configuration tasks in the related area are accessed to the production and office networks.

O. Logical-Operation - All network segments and the computer systems are kept up-to- date (software updates, security patches, virus protection, spyware protection). The backup of sensitive data and security relevant logs is applied according to the classification of the stored data.

O. Config-Items - The site has a configuration management system in SIMAX that has information about unique product identification, process step sequences, bill of materials, product drawing and label information.

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

O. Config-Process - The site controls its services and/or processes using a configuration management plan. The configuration management is controlled by tools and procedures for the development of programs and the assembly of the products, 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. Staff-Engagement - All employees who have access to sensitive configuration items and who can move parts of the product out of the defined production flow are checked regarding security concerns and have to sign a non-disclosure agreement. Furthermore, all employees are trained and qualified for their job.

O. Zero-Balance - The site ensures that all security products are separated and traced on a lot basis. Automated control and/or two employees acknowledgement during hand-over is applied for functional and defective devices. All devices are tracked until they are shipped.

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

O. Internal-Transport - The internal shipment procedure is applied to the configuration item. The address for shipment can only be changed by a controlled process. The packaging is part of the defined process and applied as agreed with SIMAX.

The forwarder supports the tracing of configuration items during internal shipment. For every sensitive configuration item, the protection measures against manipulation are defined.

O. Data-Transfer - Sensitive electronic configuration items (data or documents in an 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 extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected.

O. Scrap-Control - Rejected or defect devices if not requested by the client are gathered into the metal box carrier and transferred to the scrap house and finally incinerated under the security guard's surveillance in the designated place of the outside company.

5.1 Security Objectives Rationale

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

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

Table 5-1 Mapping of Security Objectives

Threat and OSP	Security Objective	Rationale
T. Smart-Theft	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security	Unauthorized access is detected by structural, technical and organizational measures. This allows an appropriate response to this threat. Security Objective O. Physical-Access directly counters Threat T. Smart-Theft. Security Objective O. Security-Control directly counters Threat T. Smart-Theft. Security Objective O. Alarm-Response directly counters Threat T. Smart-Theft. Security Objective O. Internal-Monitor directly counters Threat T. Smart-Theft. Security Objective O. Maintain-Security directly counters Threat T. Smart-Theft.
T. Rugged-Theft	O. Physical-Access O. Security-Control O. Alarm-Response	Unauthorized access is detected by structural, technical and organizational measures. This allows an appropriate response to this threat.

	O. Internal-Monitor O. Maintain-Security	Security Objective O. Physical-Access directly counters Threat T. Rugged-Theft. Security Objective O. Security-Control directly counters Threat T. Rugged-Theft. Security Objective O. Alarm-Response directly counters Threat T. Rugged-Theft. Security Objective O. Internal-Monitor directly counters Threat T. Rugged-Theft. Security Objective O. Maintain-Security directly counters Threat T. Rugged-Theft.
T. Computer-Net	O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Staff-Engagement	Unauthorized access to the internal network is prevented by technical and organizational measures. Security Objective O. Internal-Monitor directly counters Threat T. Computer-Net. Security Objective O. Maintain-Security directly counters Threat T. Computer-Net. Security Objective O. Logical-Access directly counters Threat T. Computer-Net. Security Objective O. Logical-Operation directly counters Threat T. Computer-Net. Security Objective O. Staff-Engagement directly counters Threat T. Computer-Net.
T. Accident-Change	O. Logical-Access O. Config-Items O. Zero-Balance O. Config-Process O. Staff-Engagement	Accidental changes by untrained employees are pre-vented by technical and organizational measures. Security Objective O. Logical-Access directly counters Threat T. Accident-Change. Security Objective O. Config-Items directly counters Threat T. Accident-Change.

		Security Objective O. Zero-Balance directly counters Threat T. Accident-Change. Security Objective O. Config-Process directly counters Threat T. Accident-Change. Security Objective O. Staff-Engagement directly counters Threat T. Accident-Change.
T. Unauthorized-Staff	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Logical-Operation O. Staff-Engagement O. Config-Control O. Zero-Balance O. Scrap-Control	Configuration items are protected by a physical and logical access control that limits the access to authorized persons only. Additionally, there are organizational measures preventing uncontrolled access to sensitive data. Security Objective O. Physical-Access directly counters Threat T. Unauthorized-Staff. Security Objective O. Security-Control directly counters Threat T. Unauthorized-Staff. Security Objective O. Alarm-Response directly counters Threat T. Unauthorized-Staff. Security Objective O. Internal-Monitor directly counters Threat T. Unauthorized-Staff. Security Objective O. Maintain-Security directly counters Threat T. Unauthorized-Staff. Security Objective O. Logical-Access directly counters Threat T. Unauthorized-Staff. Security Objective O. Logical-Operation directly counters Threat T. Unauthorized-Staff. Security Objective O. Staff-Engagement directly counters Threat T. Unauthorized-Staff. Security Objective O. Config-Control directly counters Threat T. Unauthorized-Staff.

		Security Objective O. Zero-Balance directly counters Threat T. Unauthorized-Staff. Security Objective O. Scrap-Control directly counters Threat T. Unauthorized-Staff.
T. Staff-Collusion	O. Internal-Monitor O. Maintain-Security O. Staff-Engagement O. Zero-Balance O. Scrap-Control O. Data-Transfer	Only trustworthy persons are hired and internal security measures like four-eyes principle help to prevent unauthorized access to sensitive data or items. Security Objective O. Internal-Monitor directly counters Threat T. Staff-Collusion. Security Objective O. Maintain-Security directly counters Threat T. Staff-Collusion. Security Objective O. Staff-Engagement directly counters Threat T. Staff-Collusion. Security Objective O. Zero-Balance directly counters Threat T. Staff-Collusion. Security Objective O. Scrap-Control directly counters Threat T. Staff-Collusion. Security Objective O. Data-Transfer directly counters Threat T. Staff-Collusion.
T. Attack-Internal-Transport	O. Internal-Transport O. Data-Transfer	For every sensitive configuration item, the protection measures against manipulation are defined, packing is applied as agreed with the client and the internal shipment procedure is applied. Modification or disclosure of electronic configuration items during the transport is prevented by appropriate security measures. Security Objective O. Internal-Transport directly counters Threat T. Attack-Internal-Transport. Security Objective O. Data-Transfer directly counters Threat T. Attack-Internal-Transport.

T. Attack-External-Transport	O. Staff-Engagement O. Internal-Monitor	For every sensitive configuration item, the protection measures against manipulation are defined, packing is applied as agreed with the client and the internal shipment procedure is applied. Modification or disclosure of electronic configuration items during the transport is prevented by appropriate security measures. Security Objective O. Staff-Engagement directly counters Threat T. Attack-External-Transport. Security Objective O. Internal-Monitor directly counters Threat T. Attack-External-Transport.
T. Delivery-Accidents	O. Zero-Balance O. Internal-Monitor	Delivery accidentals are prevented by structural, technical and organizational measures. Additionally, there are organizational measures preventing uncontrolled access to sensitive products. Security Objective O. Zero-Balance directly counters Threat T. Delivery-Accidents. Security Objective O. Internal-Monitor directly counters Threat T. Delivery-Accidents.
P. Config-Items	O. Reception-Control O. Config-Items	All relevant items are covered by the configuration management system and can be uniquely identified. Security objective O. Reception-Control directly enforces OSP P.Config-Items. Security objective O. Config-Items directly enforces OSP P. Config-Items.
P. Config-Control	O. Config-Items O. Config-Control O.Logical-Access	The security of the development process is supported by configuration control and logical access control. Security objective O. Config-Items directly enforces OSP P. Config-Control. Security objective O. Config-Control directly enforces OSP P. Config-Control.

		Security objective O. Logical-Access directly enforces OSP P. Config-Control.
P. Config-Process	O.Config-Process	The control of services and processes by the configuration management plan is ensured by O.Config-Process since controls by tools and procedures for the production of wafers, 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 the site are in place. Security objective O. Config-Process directly enforces OSP P. Config-Process.
P. Reception-Control	O.Reception-Control	The incoming inspection comprises the received amount of products and the identification and assignment of the product to a related internal production process. Security objective O. Reception-Control directly enforces OSP P. Reception-Control.
P. Accept-Product	O.Config-Control O.Config-Process	Only products are delivered which comply with the specification provided by the client. Wafer production quality and acceptance tests are performed to ensure this. Security objective O. Config-Control directly enforces OSP P. Accept-Product. Security objective O. Config-Process directly enforces OSP P. Accept-Product.
P. Zero-Balance	O.Internal-Monitor O.Staff-Engagement O.Zero-Balance O.Scrap-Control	Mainly O.Zero-Balance enforces P.Zero-Balance by ensuring that all security products (intended TOE of different clients) are separated and traced on a device basis. Automated control and/or two employees acknowledgement during hand over is applied for functional and defective devices. Rejected or defect devices are

		either destroyed at the site or returned to the client. The other objectives contribute to O.Zero-Balance. Security objective O. Internal-Monitor directly enforces OSP P. Zero-Balance. Security objective O. Staff-Engagement directly enforces OSP P. Zero-Balance. Security objective O. Zero-Balance directly enforces OSP P. Zero-Balance. Security objective O. Scrap-Control directly enforces OSP P. Zero-Balance.
P. Product-Transport	O.Config-Process O.Internal-Transport O.Data-Transfer	The products are correctly labelled, packed and prepared for internal transport as required by the client. This process is ensured by technical and organisational measures. The address for delivery and the forwarder are determined by the client. Security objective O. Config-Process directly enforces OSP P. Product-Transport. Security objective O. Internal-Transport directly enforces OSP P. Product-Transport. Security objective O. Data-Transfer directly enforces OSP P. Product-Transport.
P. Data-Transfer	O.Data-Transfer	Data or documents in electronic form are protected with cryptographic algorithms to ensure confidentiality and integrity. Security objective O. Data-Transfer directly enforces OSP P. Data-Transfer.

6 SECURITY ASSURANCE REQUIREMENTS

3 Client using this Site Security Target-lite requires an evaluation against evaluation assurance level EAL6.

4 The Security Assurance Requirements (SAR) are chosen from the class ALC (Lifecycle support) as defined in [2]:

1) CM capabilities (ALC_CMC.5)

2) CM scope (ALC_CMS.5)

3) Development security (ALC_DVS.2)

4) Life-cycle definition (ALC_LCD.1)

5) Tools and techniques (ALC_TAT.3)

5 The Security Assurance Requirements listed above fulfill the requirements of [4] because hierarchically higher components are used in this Site Security Target-lite.

6 The dependencies for the assurance requirements named above are as follows:

1) ALC_CMC.5: ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
2) ALC_CMS.5: None
3) ALC_DVS.2: None
4) ALC_LCD.1: None
5) ALC_TAT.3: ADV_IMP.1

7 The following dependencies are not fulfilled or not completely fulfilled:

8 ALC_LCD.1: ALC_LCD.1 is part of this Site Security Target-lite but does not cover TOE specific information of the life-cycle definition.

9 ALC_TAT.3: There is a dependency from ALC_TAT.1 (and hierarchically higher) to ADV_IMP.1. Since there is not necessarily a specific TOE while evaluating/certifying a site this dependency can only be partially fulfilled. This work can be completed while evaluating ADV_IMP during the TOE evaluation.

6.1 Application Notes and Refinements

1) 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 is not available during the evaluation. Since the term "TOE" is not applicable in the SST-lite the associated processes for the handling of products (or "intended TOEs") are in the focus and described in this Site Security Target-lite. These processes are subject of the evaluation of the site.

2) Note: The content elements that are changed from the [2] according to the application notes in the process description [4] are written in *italic*.

6.2 Overview and Refinements regarding CM Capabilities (ALC_CMC)

3) A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The number of masks and wafers is tracked by this system. Appropriate administration procedures are implemented for managing masks and wafers which are being removed from the production-process in order (i) to verify and to control predefined quality standards and production parameters (ii) to securely store and destroy.

4) According to [4] the processes rather than a TOE are in the focus of the CMC examination. The changed content elements are presented below. Since the application notes in [4] are defined for ALC_CMC.5.

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.

6) The life-cycle described in [6] is a complex production process. Only parts of this production process are normally provided at a specific site. 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. Verification procedures and the associated expected results must be under configuration management for these cases.

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

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

6.3 Overview and Refinements regarding CM Scope (ALC_CMS)

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

9) In the particular case for the production of wafers with Security ICs the scope of the configuration management includes a number of configuration items. The scope of the configuration management can include a number of configuration items. The configuration items which this site should control are already defined in section CMS documentation.

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

6.4 Overview and Refinements regarding Development Security (ALC_DVS)

10) 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.

11) 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, 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 sent to the client or destroyed.

12) Based on these requirements the physical securities 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 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.

6.5 Overview and Refinements regarding Life-Cycle Definition (ALC_LCD)

13) 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 have to be evaluated which are in the scope of the site. The PP [6] provides a life-cycle description there 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. initialization is performed at the site or not.

14) The PP [6] does not include any refinements for ALC_LCD. The site under evaluation does not initiate a life cycle change of the intended TOE. The products which are assembled, tested and packed into the cardboard boxes are delivered to the client in the end.

15) All scrap products are gathered into the metal tray in the machine, and then move into the Metal Box with a lock, and finally move to the outside scrap house to the client with security guard and qualified handler guy

6.6 Overview and Refinements regarding Tools and Techniques (ALC_TAT)

16) The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyze and implement the TOE. The component ALC_TAT.3, "Compliance with implementation standards-all parts",

requires definition and evidence for the suitability of the tools and techniques used for the development process of the TOE.

6.7 Security Assurance Rationale

17) The Security Assurance Rationale maps the content elements of the selected assurance components of [2] to the Security Objectives defined in this Site Security Target-lite. The refinements described above are considered.

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

19) The term TOE can be replaced by configuration items in most cases. In specific cases it is replaced by product (in the sense of "intended TOE").

Table 6-1 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	O. Config-Items	All products assembled at 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' get a unique Part ID automatically generated by a data base as defined by O. Config-Items.
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	O. Reception-Control O. Config-Items O. Config-Control O. Config-Process	Incoming inspection according O. Reception-Control ensures product identification with Material lot-ID and the associated labeling. This labeling is mapped to the internal identification as defined by O. Config-Items. This ensures the unique identification of security products. O. Config-Control ensures that each Part ID is setup and releases based on a defined process. This comprises also changes related to a Part ID. The configurations can only be done by authorized staff. O. Config-Process provides a configured and controlled production process.
ALC_CMC.5.3C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate	O. Reception-Control O. Config-Items O. Config-Control	O. Reception-Control comprises the incoming labeling and the mapping to internal identifications. O. Config-Items comprises the internal unique identification of all items that belong to a Part ID. Each product is setup

review of changes to all configuration items.		according to O. Config-Control comprising all necessary items.
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items.	O. Reception-Control O. Config-Items O. Config-Control	O. Reception-Control comprises the incoming labeling and the mapping to internal identifications. O. Config-Items comprises the internal unique identification of all items that belong to a Part ID. Each product is setup according to O. Config-Control comprising all necessary items.
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	O. Config-Control O. Config-Process O. Logical-Access O. Logical-Operation	O. Config-Control assigns the setup including processes and items for the production of each Part ID. O. Config-Process comprises the control of the production processes. O. Logical-Access and O. Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorized staff.
ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.	O. Config-Process O. Zero-Balance	O. Config-Process comprises the automated management of the production processes. O. Zero-Balance ensures the control of all security products during production.
ALC_CMC.5.7C The CM system shall ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.	O. Reception-Control O. Logical-Access O. Logical-Operation	O. Reception-Control comprises the incoming labeling and the mapping to internal identifications. for masks, scrap, and wafers. 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.5.8C The CM system shall identify the configuration items that comprise the *product*.	O. Config-Items O. Config-Control O. Config-Process	O. Config-Items ensure the unique identification of each product produces at 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' by the Part ID. O. Config-Control ensures a release for each new or changed Part ID. O. Config-Process ensures the automated control of released products.
ALC_CMC.5.9C The CM system shall support the audit of all changes to the *product* by automated means, including the originator, date, and time in the audit trail.	O. Config-Items O. Config-Control O. Config-Process	O. Config-Items ensure the unique identification of each product produces at 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' by the Part ID. O. Config-Control ensures a release for each new or changed Part ID.

		O. Config-Process ensures the automated control of released products.
ALC_CMC.5.10C The CM system shall provide an automated means to identify all other configuration items that are affected by the change of a given configuration item.	O. Config-Control O. Config-Process	O. Config-Control ensures a release for each new or changed Part ID. O. Config-Process ensures the automated control of released products.
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the *product* is generated.	O. Reception-Control O. Logical-Access O. Config-Process O. Config-Control	O .Reception-Control comprises the incoming labeling and the mapping to internal identifications. O. Logical-Access supports the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. O. Config-Control describes the management of the client part IDs at the site. According to O. Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.12C The CM documentation shall include a CM plan.	O. Config-Process O. Config-Control	O. Config-Control describes the management of the client part IDs at the site. According to O. Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product*.	O. Config-Process O. Config-Control	O. Config-Control describes the management of the client part IDs at the site. According to O. Config-Process the CM plans describe the services provided by the site.
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the *product*.	O. Reception-Control O. Config-Items O. Config-Process O. Config-Control	O. Reception-Control supports the identification of configuration items. O. Config-Items ensure the unique identification of each product produced by the client part ID. O. Config-Control ensures a release for each new or changed client part ID. O. Config-Process ensures the automated control of released products.
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O. Reception-Control O. Config-Control O. Config-Process O. Zero-Balance O. Internal-Transport	The objectives O. Reception-Control, O. Config-Control, O. Config-Process ensure that only released client part IDs are produced. This is supported by O. Zero-Balance ensuring the tracking of all security products. O. Internal-Transport include the packing requirements, the reports, logs and

		notifications including the required evidence.
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	O. Config-Process O. Config-Control	O. Config-Control comprises a re-lease procedure as evidence. O. Config-Process ensures the compliance of the process.

SAR	Security Objective	Rationale
ALC_CMS.5.1C The configuration list shall include the following*: clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle*; security reports and resolution status; *development and production tools and related information.*	O. Config-Items O. Config-Control O. Config-Process	Since the process is subject of the evaluation no products are part of the configuration list. O. Config-Items ensure unique part IDs including a list of all items and processes for this part. O. Config-Control describes the release process for each client part ID. O. Config-Process defined the configuration control including part IDs procedures and processes.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O. Config-Items O. Config-Control O. Config-Process O. Reception-Control O. Internal-Transport	Items, products and processes are uniquely identified by the data base system according to O. Config-Items. Within the production process the unique identification is supported by automated tools according to O. Config-Control and O. Config-Process. The identification of received products is defined by O. Reception-Control. The labeling and preparation for the transport is defined by O. Internal-Transport.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer/*subcontractor* of the item.	O. Config-Items	‘ Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)’ does not involve subcontractors for the assembly of security products. According to O. Config-Items all configuration items for secure products are identified.

SAR	Security Objective	Rationale
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the *product* design and implementation in its development environment.	O. Physical_Access O. Security-Control O. Alarm-Respose O. Logical-Operation O. Logical-Access O. Staff-Engagement O. Maintain-Security O. Scrap-Control	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 procedural and personnel protection is provided by O. Staff-Engagement. Any scrap that may support an attacker is controlled according to O. Scrap-Control.
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*.	O. Internal-Monitor O. Logical-Operation O. Maintain-Security O. Zero-Balance O. Data-Transfer O. Internal-Transport	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The associated control and continuous justification is subject of the objectives O.Internal-Monitoring, O.Logical-Operation, O. Internal-Transport, O. Data-Transfer and O. Maintain-Security. All devices including functional and non-functional are traced according to O. Zero-Balance.

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

SAR	Security Objective	Rationale
ALC_TAT.3.1C: Each development tool used for	O. Config-Items	Each tool is identified and inducted as a configuration information for the configuration item which identifies the

implementation shall be well-defined.		relevant TOE for which the tool is used for development (O.Config-Items).
ALC_TAT.3.2C: The documentation of each development tool shall unambiguously define the meaning of all statements used in the implementation.	O. Config-Process	The development methodologies (O.Config-process) are defined according to the exploited tools purposes and their utilization in the development activities. These purposes and utilization procedures are defined in the documentation issued by the tool's provider. This documentation unambiguously defines the meaning of all statements used in the implementation.
ALC_TAT.3.3C: The documentation of the development tool shall unambiguously define the meaning of all implementation dependent options.	O. Config-Process	The development methodologies (O.Config-process) are defined according to the exploited tools purposes and their utilization in the development activities. These purposes and utilization procedures are defined in the documentation issued by the tool's provider. This documentation unambiguously defines the meaning of all implementation dependent options used in the development.

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

7 SITE SUMMARY SPECIFICATION

7.1 Preconditions Required by the Site

60 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' provides mask data preparation according to the client requirements.

61 For the setup and control of the production process, the appropriate specification and relative production information is provided by the client.

62 Each configuration item received by the site is appropriately labelled and informed on SIMAX system to ensure the identification of the configuration items.

63 The site provide any data prep services are offered.

64 The site provide wafer test services. If the service of Inkless is used, the client has to provide a wafer map indicating good and bad dies.

65 To be able to exchange data securely, the necessary keys shall be exchanged before confidential material is transferred.

66 The production at 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' is released after the client accepted the initial sample lot produced by 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'. Therefore, each client is in charge for the verification of his products based on the sample lot provided by 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'.

67 If specific requirements are needed for the transport of the finished products the related specifications and further items e.g. seal tape must be provided by client.

68 Data shall be exchanged according to their classification, e.g. confidential material is exchanged in encrypted form.

69 The client is responsible for delivery and transfer of the finished wafers, comprising the selection of the forwarder and the provision of data for the verification of the transport order.

7.2 Services of the Site

70 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)' has adopting 12 inch process technology to provide the various products required by the client.

71 Bump fabrication, wafer EDS test, test program development and data handling and preparation are performed in Giheung.

72 Meanwhile, integration of GDS files for full AP chip, GDS file checking and optimization for mask data generation (Ebeam generation) is performed in Hwaseong.

73 The process flow of security product fabricated by the site is as follows. The client transfers the encrypted GDS files to Hwaseong DSR-B and then, the GDS integration and the Ebeam generation is performed in this building.

74 The Ebeam is transferred by SFTP to Giheung SR1 for the data handling and preparation, then it is sent by FTP to customer for the mask production. Depending on the type of mask, they are sent to Giheung Line 5 directly, where the bump fabrication is performed or they are sent to customer first, where the wafer fabrication is performed.

75 The engineer testing for analyzing in the testing lab room

76 Finally, the wafers arrive to Giheung Line 3 where the wafer EDS tests are performed. This test are developed in Giheung SR3.

7.3 Objectives Rationale

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

O. Physical-Access - The building is surrounded by two fences. One fence covers overall manufacturing lines and the other covers ware house. The areas around the fence are monitored by surveillance CCTV. The inside of the buildings and gates of each entrance are monitored and recorded by CCTV. Physical access to the buildings is allowed through access-control gates and visitors are allowed to enter into the buildings only when they are escorted by employees. Access control systems are also installed inside the buildings, so accessing is controlled by the systems to allow only authorized personnel to enter. Especially important areas are controlled by alarm devices to detect any second intrusion and protect from risks. When physical security devices and countermeasures against outside threats and burglaries are concerned, the important aspect to consider is its purpose of prevention of these risks, so physical access control, surveillance, and actions are properly and timely provided for safety and protection.

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

O. Security-Control - Alarm systems continue to operate during office hours and after office hours when officers are off duty and the alarm systems are connected to Security Command Center for around-the-clock monitoring and controlling. The locations where the alarm systems are installed are supported with CCTV devices for monitoring. Scheduled and nonscheduled patrol by Security Officers are carried out to protect products and to detect any risk of intrusion, regardless of office hours and non-office 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 also the Threat T. Unauthorized-Staff is addressed.

O. Alarm-Response - Alarm systems are connected to Security Command Center where Security Officers are on duty for 24 hours. To support the alarm systems during off-duty periods, extra Security Officers perform patrol to monitor specific areas. Security and alarm system devices are effectively operated as per the procedures of CCTV Surveillance - Alarm Signal-Access Control-On-site arrival by Security Officer-Actions. In any case when an intruder approaches to the facilities with bad motives, alarm systems are utilized to enhance prevention effects by generating warning signals to prevent his/her approaches to the facilities and his/her attempts to break or destroy entrance gates.

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

O. Internal-Monitor - Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes (every week). This comprises also logs and security events of security relevant systems like Firewall, Virus protection and access control. Mayor changes of security systems and security procedures are reviewed in RMC (Risk Management Committee) every month. Upon the 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, T. Attack-External-Transport, T. Delivery-Accidents and the OSP P. Zero-Balance.

O. Maintain-Security -The security relevant systems enforcing or supporting O. Physical-Access, O. Security control and O. Logical-Access are checked and maintained regularly by the suppliers. In addition the configuration is updated as required either by employees (for the access control system) of the supplier. Logging files are checked at least monthly for technical problems and specific maintenance requests.

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

O. Logical-Access - The internal network is separated from the internet with a firewall. The internal network is further separated into sub networks by internal firewalls. These firewalls allow only authorized information exchange between the internal subnetworks. Each user is logging into the system with his personalized user name 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 ERP 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 maintained and updated as required, at least once a month. Critical items such as Anti-virus Software are updated whenever new version software is released. The backup is sufficiently protected and is only accessible for the administration.

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

O. Config-Items - All product configuration information is stored in the database of the SIMAX system. The information stored is covering used materials, process specifications, acceptance instructions and specifications, programs and packing instructions. Products are identified by unique client part IDs which are linked to the unique lot–ID and lot numbers of the associated configuration items.

This is addressing the threat T. Accident-Change and the OSP P. Config-Items and P. Config- Control.

O. Config-Control - Procedures arrange for a formal release of specifications and test programs based on an engineering run. The information is also stored in the configuration database. Engineering Change Procedures are in place to classify and introduce changes. These procedures also define the separation between minor (internal) and major changes and the relevant interactions and releases with client s if required. The ERP requires personalized access controlled by passwords. Each user has access rights limited to the needs of his function. Thereby only authorized changes are possible. Supported by O. Config-Items this addresses the threat T. Unauthorized-Staff and the OSP P. Config-Control and P. Accept-Product.

O. Config-Process - The released configuration information including production and acceptance specifications is automatically shared through SIMAX. The test program for screening the electronic malfunction is automatically loaded to the test machine according to the configuration information of the work order by SIMAX. The test program shall not be changed during the test process by an operator or a technician.

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

O. Staff-Engagement - All employees are interviewed before hiring. They must sign an NDA 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. PhysicalAccess, 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, T. Attack-External-Transport and the OSP P. Zero-Balance

O. Zero-Balance - Products are uniquely identified throughout the whole process. Further on the amount of functional and non-functional dice on a wafer and for a production order is known. Handover and storage of security products is controlled by the 4-eyes principle and documented. Scrap and rejects are managed on every process step. At every process step the registration of good and scrapped/rejected products is updated. Before a production order is closed a zero balance calculation is documenting the history of good and bad parts of this order. 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, T. Delivery-Accidents and the OSP P. Zero-Balance.

O. Reception-Control - At reception each configuration item including security products are identified by the shipping documents, packaging labels and information in the ERP system based on shipment alerts from the client s and supported by O. Config-Items. If a product cannot be identified it is put on hold in a secure storage. Inspection at reception is counting the amount of boxes and checking the integrity of security seals of these boxes if applicable. Thereby only correctly identified products are released for production.

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

O. Internal-Transport - The recipient of a production lot is linked to the work order in the ERP system and can only be modified by authorized users. Packing procedures are documented in the product configuration. This includes specific requirement of the client. This security objective is supported by O. Staff-Engagement and O. Config-Items.

The threat T. Attack-Internal-Transport and the OSP P. Product-Transport are addressed by the transport.

O. Data-Transfer - Sensitive electronic information is stored and transferred encrypted using the EDM. Supported by O. Logical-Acces and O. Staff-engagement this addresses the threats T. Staff-Collusion and T. Attack-Internal-Transport as well as the OSP P. Product-Transport and P. Data-Transfer.

O. Scrap-Control - Scrap is identified and handled with automated logistics system or semi-automated logistic system. They are stored internally in a secure metal box carrier and then move to the designated location along with Security-Guard. Transport and actual destruction of security products is done under supervision of a qualified employee in collaboration with the destructor.

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

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

7.4 Security Assurance Requirements Rationale

22) The Security Assurance Rational is given in section 7.2. 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 fulfill the needs derived from the Protection Profile [6]. Because they are compliant with the Evaluation

Assurance Level EAL6 all derived dependencies are fulfilled.

7.5 ALC_CMC.5

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

7.6 ALC_CMS.5

24) The chosen assurance level ALC_CMS.5 of the assurance family "CM scope" supports the control of the production 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.

7.7 ALC_DVS.2

25) 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 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 IC modules for Smart Card, NFC (Near field communication) and IT Security Products.

7.8 ALC_LCD.1

26) The chosen assurance level ALC_LCD.1 of the assurance family "Life-cycle definition" is suitable to support the controlled development and production process. This includes the documentation of these processes and the procedures for the configuration management. Because the site provides only a limited support of the described life-cycle for the development and production of Security IC modules for Smart Card and NFC (Near field communication) related device 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.

7.9 ALC_TAT.3

27) The security assurance requirements of the assurance class "Tools and Techniques" shall support the secure development and production of the TOE. The control, capabilities and configuration of the tools contribute to achieve reproducible and consistent development, production and test processes. Therefore, this Security assurance requirement is suitable for this type of product.

7.10 Assurance Measure Rationale

O. Physical-Access

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

O. Security-Control

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

O. Alarm-Response

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

O. Internal-Monitor

• ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Maintain-Security

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

• ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

O. Logical-Access

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

• ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

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

• ALC_CMC.5.11C requires the CM system shall be able to identify the version of the implementation representation from which the wafer and the mask data are generated. Thereby this objective contributes to meet the Security Assurance Requirement. Thereby these Security Assurance Requirements are 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 objective contributes to meet the Security Assurance Requirement.

• ALC_DVS.2.2C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

• ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

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

O. Config-Items

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

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

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

• ALC_CMC.5.4C requires that the CM system uniquely identify all configuration items.

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

• 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.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the product.

• ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

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

• ALC_CMS.5.3C requires for each configuration item that the configuration list indicates the developer / subcontractor of the item.

• ALC_TAT.3.1C requires that each development tool used for implementation be well-defined.

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

O. Config-Control

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

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

• ALC_CMC.5.4C requires that the CM system uniquely identify all configuration items.

• ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

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

• 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 wafers 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 new-ly created configuration items as part of the product.

• ALC_CMC.5.15C requires 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 sys-tem is being operated in accordance with the CM plan.

• ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

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

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

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

O. Config-Process

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

• ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the Security Assurance Requirement.

• ALC_CMC.5.6C re-quires that the CM system supports the production by automated means.

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

• 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 wafers 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.

• ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, development tools and related information.

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

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

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

• ALC_TAT.3.2Crequires that the documentation of the development tool unambiguously defines the meaning of all statements used in the implementation.

• ALC_TAT.3.3C requires that the documentation of the development tool unambiguously defines the meaning of all implementation dependent options.

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 the objective fulfills this combination of Security Assurance Requirements.

O. Zero-Balance

• ALC_CMC.5.6C requires that the CM system supports the production 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 TOE.

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

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

O. Reception-Control

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

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

• ALC_CMC.5.4C requires that the CM system uniquely identify all configuration items.

• 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 wafers are generated.

• 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.5.3C.

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

O. Internal-Transport

• 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.

• ALC_DVS.2.2C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. This includes also the protection during the transport between production sides.

O. Data-Transfer

• ALC_DVS.2.2C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. This includes also the protection during the transport between production sides.

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

O. Scrap-Control

• 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 objective is suitable to meet the Security Assurance Requirement.

7.11 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 'Samsung Electronics Giheung & Hwaseong (Line 3, Line 5, SR1, SR3 and DSR-B building)'.

Table 7-1 Mapping for ALC_CMC.5

SAR	Aspects	References
ALC_CMC.5.1C *The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.*	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2.2
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2.2
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.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 4
ALC_CMC.5.4C The CM system shall uniquely	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2.2

identify all configuration items.		
ALC_CMC.5.5C The CM system shall provide automated measures such that only authorised changes are made to the configuration items.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 4
ALC_CMC.5.6C The CM system shall support the production of the *product* by automated means.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
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.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
ALC_CMC.5.8C The CM system shall identify the configuration items that comprise the *product*.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2.2
ALC_CMC.5.9C The CM system shall support the audit of all changes to the *product* by automated means, including the originator, date, and time in the audit trail.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
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.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
ALC_CMC.5.11C The CM system shall be able to idenytify the version of the implementation representation from which the *product* is generated.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
ALC_CMC.5.12C The CM documentation shall include a CM plan.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the *product*.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3 and 4

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*).	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3 and 4
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3
ALC_CMC.5.16C: The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 3

Table 7-2 Mapping for ALC_CMS.5

SAR	Aspects	References
ALC_CMS.5.1C The configuration list shall include the following*: clear instructions how to consider these items in the list*; the evaluation evidence required by the SARs *of the life-cycle*; security reports and resolution status; *development and production tools and related information.*	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2
ALC_CMS.5.3C: For each *configuration item*, the configuration list shall indicate the developer/*subcontractor* of the item.	All	Giheung&Hwaseong_ALC_CMC_CMS_V1.4. Section 2

Table 7-3 Mapping for ALC_DVS.2

SAR	Aspects	References
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 *product* design	All	Giheung&Hwaseong_ALC_DVS_V1.7. Section 2 to 7

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*.	All	Giheung&Hwaseong_ALC_DVS_V1.7. Section 11

Table 7-4 Mapping for ALC_LCD.1

SAR	Aspects	References
ALC_LCD.1.1C: The lifecycle definition documentation shall describe the model used to develop and maintain the *product*.	All	Giheung&Hwaseong_ALC_LCD_V1.5. Section 2
ALC_LCD.1.2C: The lifecycle model shall provide for the necessary control over the development and maintenance of the *product*.	All	Giheung&Hwaseong_ALC_LCD_V1.5. Section 3 and 4

Table 7-5 Mapping for ALC_TAT.3

SAR	Aspects	References
ALC_TAT.3.1C: Each development tool used for implementation shall be well-defined.	All	Giheung&Hwaseong_ALC_TAT_V1.3. Section 2.2
ALC_TAT.3.2C: The documentation of the development tool shall unambiguously define the meaning of all the statements used in the implantation.	All	Giheung&Hwaseong_ALC_TAT_V1.3. Section 2
ALC_TAT.3.3C: The documentation of the development tool shall unambiguously define the	All	Giheung&Hwaseong_ALC_TAT_V1.3. Section 2

meaning of all implementation dependent options.		

8 REFERENCES

8.1 Literature

[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, October 2007, Version 1.0, Revision 1, CCDB-2007-11-001

[5] Guidance for Site Certification, Bundesamt für Sicherheit in der Informationstechnik, Date 2010, Version 1.0

[6] Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014.