life.augmented

Public Site Security Target - ST Greater Noida

TABLE OF CONTENTS

1 PURPOSE

The purpose of this document is to describe the security target for the design center of ST NOIDA

2 SCOPE

This document is the public version of the internal Site Security Target of ST NOIDA hardware development site. It has been written in the context of Site Certification objective in accordance with the Common Criteria Specification.

3 REFERENCE DOCUMENTS

3.1 External References

External references	
[1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 CCMB-2017-04-001.
[2]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components April 2017 Version 3.1 Revision 5 CCMB-2017-04-003
[3]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology April 2017 Version 3.1 Revision 5, CCMB-2017-04-004
[4]	Supporting Document, Site Certification, Version 1.0, Revision 1, CCDB-2007-11-001, October 2007.
[5]	Joint Interpretation Library, Minimum site security requirements, version 3.0, February 2020.
[6]	Security IC Platform Protection Profile with Augmentation Package BSI-CC-PP-0084-2014; Version 1; Issued 13-01-2014.
[7]	Site security target template final v2.0

4 ACRONYMS & DEFINITIONS

4.1 Acronyms

Acronym	Definition
CC	***C**ommon **C**riteria*
CM	***C**onfiguration **M**anagement system*
EAL	***E**valuation **A**ssurance **L**evel*
IC	***I**ntegrated **C**ircuit*
IT	***I**nformation **T**echnology*
OSP	***O**rganizational **S**ecurity **P**olicy*
SAR	***S**ecurity **A**ssurance **R**equirements*
SST	***S**ite **S**ecurity **T**arget*
TOE	***T**arget **O**f **E**valuation*
PP	***P**rotection **P**rofile*

4.2 Definitions

Term	Definition
Client	*The site providing the Site Security Target may operate as a subcontractor of the TOE manufacturer. The term „client" is used here to define this business connection. It is used instead of customer since the terms „customer" and „consumer" are reserved in CC. In this document the terms words „customer" and „consumer" are only used here in the sense of CC.*
Intended TOE	*In the view of this site certification, there is no real product certified as the site certification is - per definition – product independent. Therefore, also no TOE does exist, and this SST is referring to the "intended TOE" only.*
Product	*A "product" would be the result of the development process.*

5 GENERAL

The purpose of this document is to describe the security target for the design center of ST NOIDA

5.1 SST reference

Title	**NOIDA Site Security Target**
Version / date	*V1.0 issued December 16, 2022 (based on document ID DM00859156)*
Company	*STMicroelectronics Private Limited*
Site Location	*ST NOIDA, Plot No. 1, Knowledge Park-III Greater Noida - 201 308, Uttar Pradesh, INDIA*
Assurance level	*EAL6 (ALC class only)*
Evaluation Lab.	*SERMA Safety and Security – ITSEF*
Certification Body	*Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*

Table 1: SST references

ST NOIDA is in charge of **IC Hardware Design** operations. The processes associated to the design

5.2 Identification of the Site

The SST is referring to STMicroelectronics Private Limited NOIDA site, located at NOIDA in INDIA that provides the Hardware design service for automotive Integrated circuits. This SST is specific for site abbreviated as 'NOIDA' which is located at:

- Plot No. 1, Knowledge Park-III Greater Noida - 201 308, Uttar Pradesh, INDIA.

Main activity at this site is Hardware design of Secured and Non-secured Integrated circuits.

5.3 Site Description

This chapter defines the type of activities performed by ST NOIDA and targeted to be in the scope of a Site Certification as defined in CCDB-2007-11-001 - Supporting Document, Site Certification [4].

of hardware security module are the following:

- Management of external components (Security specification, RTL and Firmware): the security module is composed of a set of components some of which are not internally developed within the secure area but instead received from outside. This process refers to the management of such external components, which also include the security specification defining the requirements of the security module.
- Security module Front End design and component integration: this process refers to the activities related to the creation of dedicated components and the integration of all internal and external components, to complete security module design from a logical perspective, following the product security specification.
- Security module Front End verification: this phase targets to check the correctness of security module functionality against the product security specification from a logical point of view. The outcome is a set of corrections to be applied to the logical front-end design to make it compliant with security specifications.

- Design-for-Test (DFT) Front-End integration: this process deals with the definition of those logical structures required to ensure effective test of samples coming out from the production line, without compromising the security requirements during product lifetime.
- Front-to-Back checks on security module: this consists of a defined set of checks on the logical front-end composition of the security module to be sure that all its parts make a consistent package to be further processed for its integration into the host SoC and the related physical implementation.
- Security module subsystem database hands-off to SoC team: this process deals with the management of security module subsystem transfer to SoC team outside the secure area, ensuring that security is preserved while the final integration into the host SoC and device physical implementation is completed.

These processes are all part of the evaluation scope.

Measures are in place for security objectives:

- Badge access control to the site and buildings with security guard available 24/7
- Restricted access to areas associated to secure design processes, with dedicated badge reader.
- Single entry/exit gate continuously monitored by dedicated CCTV camera.
- IR intruder alarm system.
- No laptops allowed in areas associated to secure design processes.
- Dedicated VNC server with restricted mounting of secure project disks
- Management of secure project areas with controlled user list and enforced restricted access permissions

The site allows supporting the Assembly of TOEs targeting an Evaluation Assurance Level up to: EAL6.

5.3.1 Physical scope of the site

The ST NOIDA site is composed of 5 buildings:

- Design Building “A” (4-Storey; includes Security control room “BMS”),
- Design Building “B” (6-Storey; includes Secure Design Area),
- Cafeteria Block (3-Storey includes offices, Lab, Training rooms and HR dept),
- Gas Bank & STP Block,
- Utility Block.

The site area is around 62000 square-meters. Buildings occupy around 53200 square-meters The secure design area is limited to 200 square meters. The secure design operation is located in the Design Building “B” (Ground floor), including the server room (First floor).

Only the Secure Design area at Design Building “B” and IT server room are part of the site certification scope. The other areas are not in the scope.

5.3.2 Logical scope of the site

The sensitive assets manipulated are the design and specifications of security modules.

The activities part of the evaluation are:

- Management of external components
- Security module Front End design and component integration
- Security module Front End verification
- Design-for-Test (DFT) Front-End integration
- Front-to-Back checks on security module subsystem
- Security module subsystem database hands-off to SoC team

They are detailed at 0 - Site Description.

The TOE life cycle is part of the global product life cycle that goes from product development to its usage by the final user.

The product life cycle phases are those detailed in PP0084 [6] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software, OS and potentially Application Layer) and IC development;
- Phases 3 and 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalization steps may occur in Phase 3;
- Phase 5 concerns the product finishing (eg: within a Smartcard, Inlay, eCover…) called "Composite Integration";
- Phase 6 is dedicated to the product personalization prior final use;
- Phase 7 is the product operational phase.

The IC Hardware Design done at ST NOIDA is only involved in Phase 2.

In this context, the specific portion of the IC having security goals (security module) is the one whose hardware is to be designed within the secure design area of ST NOIDA, This security module is composed as per the definition found in PP0084 [6] and it is then integrated into a larger device without providing any access to its internal resources in none of the subsequent phases of its development.

5.4 CONFORMANCE CLAIMS

This SST is conformant with the Common Criteria For Information Technology Security Evaluation Version 3.1 revision 5:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001 Version 3.1 Revision 5 [1],
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003 Version 3.1 Revision 5 [3].

For the evaluation, the following methodology will be used:

- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003 Version 3.1 Revision 5 [3]
- Common Methodology for Information Security Evaluation (CEM), Evaluation Methodology; Version 3.1, Revision 5, April 2017,
- Supporting Document Guidance Site Certification, Version 1.0, Revision 1, CCDB-2007- 11-001, October 2007 [4],
- Minimum Site Security Requirement Version 3.0, February 2020 [5].

This SST is Common Criteria Part 3 conformant.

There are no extended components required for this SST.

The Assurance Components which are in the scope of this site certification are:

- **ALC_CMC.5**: Advanced support,
- **ALC_CMS.5**: Development tools CM coverage,
- **ALC_DVS.2**: Sufficiency of security measures,
- **ALC_LCD.1**: Developer defined life-cycle model,
- **ALC_TAT.3**: Compliance with implementation standards - all parts.

The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) (Ref: BSI-PP-0084) [6]. Therefore, the scope of the evaluation is suitable to support product evaluations up to assurance EAL6 conformant to Part 3 of the Common Criteria.

Assurance components evaluated are based on the assurance level EAL6 of the Assurance class “Life- Cycle Support”. Assessment of the site security measures demonstrates resistance to penetration of attackers, with a high attack potential. This site supports product evaluations up to EAL6.

6 SAFETY/SECURITY REQUIREMENTS

Not applicable

Note to the reader: This section is intended for physical healthy safety or physical security requirements.

7 PROCEDURE

7.1 Security Problem Definition

The Security Problem Definition comprises security problems derived from threats against the assets handled by the site and security problems derived from the configuration management requirements. The configuration management covers the integrity of the TOE and the security management of the site. Goal is to achieve and hold a high security level to counter attacks with high attack potential at the site.

This SST is based on the life-cycle defined in the Security IC Platform Protection Profile (Ref: BSI-PP-0084). The Assets (Section 3.1), Threats (Section 3.2) and Organizational Security Policies (OSP) (Section 3.3) defined in this SST are derived from the life-cycle defined in that PP.

The Security Problem Definition comprises two major security problems. The first set of security problems comprises all kind of attacks regarding theft (e.g. samples) or disclosure (e.g. design data) or manipulation of assets. 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 modification) and the control of security measures. These security problems are described in terms of Organizational Security Policies (OSP).

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

7.1.1 Assets

The following section describes the assets handled at the site regarding the Hardware Design process.

The site has internal documentation and processes relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security policies and measures which aims to protect the assets for the maintenance of appropriate controls

The integrity of any machine or tool used for development, production, testing and personalization is not considered as an asset. However, appropriate measures must be defined for the site to ensure the integrity. These items normally consist of standard hardware and software which are programmed or customized.

The assets handled by the site are:

Designation	Description
Development Data	The site has access to (and optionally copies thereof) electronic development data (specifications, guidance documentation, source code, etc.) in relation to developed products. Both the integrity and the confidentiality of these electronic documents must be protected.
Development Tools	To perform its development activities, the site uses tools (e.g., compiler) to transform source code (and potentially the libraries that come with these tools) into binaries. The integrity of these tools (running on local or remote development computers) must be protected.
Personalization data	The personalization data, such as ROM code, received or issued by the site, is necessary for initialization of the product (Pre-personalization operation). These personalization data shall be maintained, manipulated (and transfer when necessary) in a secure manner for maintaining their Integrity and Confidentiality.

Table 2: Assets

The secure design area of the site does not keep physical objects in relation to developed security modules. There are no samples used and printed documents are forbidden. Dedicated VNC servers with restricted mounting of secure project disks are the only physical entity containing secure data. This is why among the assets there is no mention of any physical object

7.1.2 Threats

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 development, production, test and assembly the TOE and the representation of parts of the TOE are vulnerable to such attacks.

All threats are applicable to the whole site and need to counter them sufficiently.

The Identified Threats related to the site are showed in the table below.

Designation	Description
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. The affected assets are “Development Data” and “Personalization Data”. This attack already includes a variety of targets and aspects with respect to the various assets listed in the section above. It covers the range of individuals that try to get information about the functionality of the device and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However, the time that can be spent by such an attacker to prepare the attack and the flexibility of such an attacker will provide notable risk. It is attended that such an attacker can be defeated by state of the art physical, technical and procedural security measures like access control and surveillance. The technical measures 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. The affected assets are “Development Data” and “Personalization Data”. This attack is applicable for the location. 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 specifications or personalization data that can be sold or misused in an application context. Those attackers are considered to have the highest attack potential. Such attackers may not be completely defeated by the physical, technical and procedural security measures. In the premises of secure areas, the usage is paper document or removable storage devices is forbidden, so to ensure that no physical object is there to be stolen.
T.Computer-Net	A hacker with substantial expertise, standard equipment, who may be paid to attempt to remotely access sensitive network segments to get access to development systems with the intention to modify the development. The affected assets are “Development Data”, “Development Tools” and “Personalization Data”. 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. 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.
T.Unauthorised-Staff	Unauthorized employees or subcontractors get access to assets or systems used for development, configuration management, so that the confidentiality and/or the integrity of the intended TOE is violated. This can apply to any development step and any asset related to the intended TOE or its configuration. . The affected assets are “Development Data” and “Personalization Data”.

	As no physical assets are present in the secure design area, the only threat here might come from maintenance tasks of subcontractors, who 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. The attack potential depends on the trustworthiness of the subcontracted company and the access required within the company. Related to this, different measures 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. The affected assets are “Development Data” and “Personalization Data”. While the site conducts security training and security talks for the employees, they have to also sign the confidentiality agreement during their term of employment with the site. Such agreement is renewed periodically and a regular training to refresh security concepts is also planned. As no physical assets are managed in the secure site, this is the only measure that is taken.
T.Attack-Transport	An attacker might try to get hold of any assets during their transfer. The target is to compromise confidential information or violate the integrity of the assets during transfer to allow a modification, cloning or the direct/indirect retrieval of confidential information Confidential information comprises design data, customer and/or consumer data like code and data (including personalization data) stored in Memories or classified product documentation. . The affected assets are “Development Data” and “Personalization Data”. The protection of the internal shipment and/or the external delivery is based on the configuration items that are provided by ST NOIDA assumes that the configuration items are protected according to assumption A.Product-Integrity

Table 3: Threats

7.1.3 Organizational Security Policies

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

The documentation of the site under evaluation must be under configuration management. This comprises all procedures regarding the evaluated development flow and the security measures that are in the scope of the evaluation.

Designation	Description
P.Config-Items	The configuration management system shall be able to uniquely identify all configuration items. This includes the unique identification of items that are created, generated, developed or used at a site as well as the received and transferred and/or provided items.
P.Config-Control	The procedures for setting up the development process for a new product as well as the procedure that allows changes of the initial setup for a product is only applied by authorized personnel. Automated systems support the configuration management and ensure access control or interactive acceptance measures for set up and changes. The procedure for the initial set-up of a development process ensures that sufficient information is available.
P.Config-Process	The services and/or processes provided by the site are controlled in the configuration management plan. This comprises incoming items, tools used for the development 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 the site. A released development process is defined and under version control. The documentation describing the processes and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status is ensured. Tools and data bases are used to support the development process of the site. This comprises e.g. configuration management tools and commercial data base systems.
P.Reception Control	The inspection of incoming items done at the site ensures that the received configuration items comply with the properties initially stated. Furthermore, it is verified that the received configuration items can be identified and a released development process is defined. If applicable this aspect includes the check that all required information and data is available to process the items. This applies to external IPs and ROM code received from outside the secure design area, for which a specific incoming checklist procedure is in place. No other item is received.
P. Accept-Product	The validation tests and quality control of the site ensures that the released products comply with the specification. 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 or externally shipped. This applies to the verification activity, where security specification compliance of the design is ensured, prior to the delivery.
P.Data-Transfer	Confidential/ sensitive data transfers in electronic form must be sent in a signed, encrypted and secured manner. All sensitive configuration or information (include product specifications, test programs, test program specifications, design layout etc.) is also encrypted to ensure security before sending out to contractors or clients through logical way (email, SFTP, etc.).

Table 4: Organizational Security Policies

7.1.4 Assumptions

Designation	Description
A.Item-Identification	Each configuration item (IP) shipped from a client to the development site is uniquely labelled by the client to ensure the identification of the configuration item.
A.Product-Setup	The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product the site and STM agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by STM.
A.Shipment	To enable the site to realize shipment such that assurance of integrity is assured throughout transport of security objects STM will adhere to the shipment method as described in the life cycle documentation.

Table 5: Assumptions

7.2 Security Objectives

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

Designation	Description
O.Physical-Access	The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows enough separation of employees to enforce the “need to know” principle. The access control shall support the limitation for the access to these areas including the identification and rejection of unauthorized people. Special features of secure design areas include batch access control to the building with security guard available 24/7, single entry/exit to the secure areas, dedicated batch reader to allow access only to secure design team members, CCTV camera monitoring the access, IR intruder alarm system batch access.
O.Security-Control	Assigned personnel of the site or guards operate the systems for access control and surveillance and respond to alarms. Technical security measures like video control, motion sensors and similar kind of sensors support the enforcement of the access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors, and suppliers.
O.Alarm-Response	The technical and organizational security measures ensure that an alarm is generated before an unauthorized person gets access to any sensitive configuration item (asset). After the alarm is triggered the unauthorized person still has to overcome further security measures. The reaction time of the employees or guards is short enough to prevent a successful attack.
O.Internal-Monitor	The site performs security management meetings at least every six months. 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 may be 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 that they are configured as required to ensure the protection of the networks and computer systems.
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. Furthermore, the internal network is separated into a development network and an office network. Additional specific networks are physically separated from any internal network to enforce access control. Access to the development network and related systems is restricted to authorized employees that work in the related area or that are involved in the configuration tasks or the development systems. Every user of an IT system has its own user account and password. An authentication using user account and password is enforced by all computer systems.
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 that assigns a unique internal identification to each product to uniquely identify configuration items. Also, the internal procedures and guidance are covered by the configuration management.
O.Config-Control	The site applies a release procedure for the setup of the development 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 concern team. 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 authorised personnel only. Automated systems support configuration management and development 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 the product, 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.Acceptance-Test	The site delivers assets that fulfil the specified properties. Parameter checks, functional and/or visual checks and tests are performed to ensure the compliance with the specification. The test results are logged to support tracing and the identification of systematic failures.
O.Staff-Engagement	All employees who have access to sensitive configuration items and who can move parts of the product out of the defined development flow are checked regarding security concerns and have to sign a nondisclosure agreement. Furthermore, all employees are trained and qualified for their job.
O.Data-Transfer	Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secure measures and they are sufficiently protected
O.Control-Scrap	The site has measures in place to destruct sensitive documentation, erase electronic media and destroy sensitive configuration items so that they do not support an attacker.

Table 6 – Security Objectives Description

7.3 Security Objectives Rationale

The SST 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.

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

Threat / OSP	Security Objective	Justification
T.Smart-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control-Scrap	The combination of structural, technical, and organizational measures detects unauthorized access and allow for appropriate response on any threat. O.Physical-Access ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a Secure Room O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Smart_Theft.
T.Rugged-Theft	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Control-Scrap	The combination of structural, technical, and organizational measures detects unauthorized access and allow for appropriate response on any threat O.Physical-Access ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a Secure Room O.Alarm-Response supports O.Physical_Access and O.Security_Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T.Rugged_Theft.

T.Computer-Net	O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement	The technical and organizational measures prevent unauthorized access to the internal network. The development network is not connected to anything that an attacker could use to set up a remote connection. O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. O.Logical-Operation ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus, and spyware protection). O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Computer-Net.
T.Unauthorised-Staff	O.Physical-Access O.Security-Control O.Alarm-Response O.Internal-Monitor O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Control-Scrap	Physical and logical access control limits the access to sensitive product or data to authorized persons. In addition, organizational measures prevent uncontrolled access to products or product related items (including secure scrap). O.Physical-Access ensures that the Secure Rooms are physically partitioned and access restricted, so a burglar cannot just walk in. O.Security-Control ensures that an attacker will be detected when trying to reach the assets through a Secure Room O.Alarm-Response supports O.Physical-Access and O.Security-Control by ensuring that a response will be given to the alarm systems and that this response is quick enough to prevent access to the assets. O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Logical-Operation ensures that all computer systems used to manage the Business Unit network are kept up to date (software updates, security patches, virus, and spyware protection). O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Unauthorised Staff
T.Attack-Tranport	O.Data-Transfer	The applied security measures on sensitive data during their transfer prevent modification or disclosure of any sensitive items. O. Data-Transfer ensures the integrity and Confidentiality of the secure delivery of data. This objective will therefore counter T. Attack-Transport.

T.Staff-Collusion	O.Internal-Monitor O.Maintain-Security O.Staff-Engagement O. Data-Transfer O.Control-Scrap	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to assets. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Data-Transfer-ensures the integrity of the secure delivery of data. O.Control-Scrap ensures that scrap material cannot be accessed by unauthorized party O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Staff Collusion
P.Data-Transfer	O.Data-Transfer	The Security Objective directly enforces the OSP.
P.Config Process	O.Config-Process	The Security Objective directly enforces the OSP.
P.Reception-Control	O.Data-Transfer	O.Data-Transfer-ensures the integrity of the secure received of data. This objective therefore counter P.Reception-Control
P.Accept-Product	O.Config-Control O.Config-Process O.Acceptance-Test	Application of a configuration management plan and change management monitored by authorized people ensure that the intended TOE is conformant to the accepted on by the customer. O.Config_Control ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. O.Config-Process ensures that configuration management is used and applied for sites services control. O. Acceptance-Test to ensure that the products are compliant with their specifications. Together, these objectives will therefore counter P. Accept-Product.
P.Config-Item	O.Data-Transfer O.Config-Items	The Security Objective directly enforces the OSP O.Config-Item. O.Data-Transfer-ensures the integrity of the secure received of data. O.Config-Item ensures that all configuration items for secure products are identified. Together, these objectives will therefore counter P. Config-Items
P.Config-Control	O.Config-Items O.Config-Control O.Logical-Access	Network and Logical protection (O. Logical – Access) and the usage of configuration management tools by authorized people ensure the OSP. O.Config-Items ensures that all configuration items for secure products are identified. O.Config_Control ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. Together, these objectives will therefore counter P. Config-Control.

Table 7: Mapping of Security Objectives

7.4 Extended Assurance Components Definition

There are no extended components required for this SST.

7.5 SECURITY ASSURANCE REQUIREMENTS

The security assurance requirements for this Site Security Target shall support an evaluation according to the assurance level EAL6.

Therefore, this security assurance requirement is applied in this Site Security Target instead of ALC_DVS.1, ALC_CMC.4, ALC_CMS.4 as defined for the package EAL4 as requested by PP-0084, because ALC_DVS.2 and ALC_CMC.5 are the hierarchically higher components. This Site Security Target is then suitable for EAL4 to EAL6 evaluations.

The Security Assurance Requirements (SAR) are from the class ALC (Life cycle support):

- CM capabilities (ALC_CMC.5),
- CM scope (ALC_CMS.5),
- Development security (ALC_DVS.2),
- Life cycle Definition (ALC_LCD.1),
- Tools and techniques (ALC_TAT.3).

Because hierarchically higher components are used in this SST, the Security Assurance Requirements listed above fulfill the requirements of:

- [3]'Common Criteria Supporting Document Guidance Site Certification'
- 'Security IC Platform Protection Profile - Eurosmart'
- [5] 'Minimum Site Security Requirements'

7.5.1 Application Notes and Refinements

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

7.5.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.1 ‘Application Notes for ALC_CMC’.
- ‘Refinements of the TOE Assurance Requirements’ in [6] §6.2.1.4 ‘Refinements regarding (ALC_CMC)’.

A development control system is employed to guarantee the traceability and completeness of TOE development. The configuration items are tracked with this system. Appropriate administration procedures are implemented for managing the development flow.

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

The life cycle described includes development. The control of the product after development process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results are under configuration management for these cases.

The configuration items for the considered product type are listed at section 7.1.1- Assets. The CM documentation of the site is able to maintain the items listed for the relevant life cycle step and the CM system is able to track the configuration items.

7.5.1.2 Overview and Refinements regarding CM Scope (ALC_CMS)

Refer to subsections:

- ‘Application Notes for Site Certification’ in [4]§5.2 ‘Application Notes for ALC_CMS’.
- ‘Refinements of the TOE Assurance Requirements’ in [6] §6.2.1.3 ‘Refinements regarding (ALC_CMS)’.

The scope of the configuration management for a site certification process is limited to the documentation relevant for the security assurance requirements for the claimed life cycle assurance requirements and the configuration items handled at the site.

In the particular case of a Security IC hardware development, the scope of the configuration management can include a number of configuration items. The configuration items, defined at section 7.1.1 - Assets, that are considered as “TOE implementation representation”, includes:

- Development data,
- Classified documentation,
- Personalization data (ROM Code).

Final RTL design data and hands-off related data.

7.5.1.3 Overview and Refinements regarding Development Security (ALC_DVS)

Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.4 ‘Application Notes for ALC_DVS’.
- ‘Refinements of the TOE Assurance Requirements’ in [6] §6.2.1.2 ‘Refinements regarding (ALC_DVS)’.

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

The TOE developer must ensure that the development of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, test data, configuration data and pre-personalization data must be guaranteed, access to development tools and other material must be restricted to authorized persons only.

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

7.5.1.4 Overview and Refinements regarding Development Security (ALC_LCD)

Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.6 ‘Application Notes for ALC_LCD’.

The site is the entire development environment. Therefore, the ALC_LCD criteria are in the scope of the site. The Protection Profile (BSI-PP-0084) provides a life-cycle description there specify life-cycle steps can be assigned to the tasks at site.

The Protection Profile (BSI-PP-0084) does not include any refinements for ALC_LCD

7.5.1.5 Overview and Refinements regarding Development Security (ALC_TAT)

Refer to subsections:

- ‘Application Notes for Site Certification’ in [4] §5.7 ‘Application Notes for ALC_TAT’.

The CC assurance components of family ALC_TAT refer to the tools that are used to develop, analyze, and implement the TOE. Therefore, the ALC_TAT criteria are in the scope of the site. The component ALC_TAT.3, “Compliance with implementation standards”, requires evidence for the suitability of the tools and technique used for the development process of the TOE.

7.5.2 Security Assurance Rationale

The Security Assurance Rationale maps the content elements of the selected assurance components of [3] to the Security Objectives defined in this SST. The refinements described above are considered.

7.5.2.1 Security Requirements Rationale – Dependencies

The dependencies for the assurance requirements are as follows:

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

One of the dependencies is not fulfilled:

- There is a dependency from ALC_TAT.3 to ADV_IMP.1. Since there is not necessarily a specific TOE while evaluating/certifying a site this dependency cannot be fulfilled at that time. This is in-line with and further explained in [4] at §5.7 ‘Application Notes for ALC_TAT’.

7.5.2.2 Security Requirements Rationale – Mapping

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
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	The unique ID of the configuration items is managed in automatic and transparent way by the configuration management system 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.Config-Items O.Config-Control O.Config-Process	Product 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 released based on a defined process. This comprises also changes related to part ID.The configurations can only be done by authorized staff. O.Config-Process provides a configured and controlled development process.
ALC_CMC.5.3C: The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.	O.Config-items O.Config-control	O.Config-Items comprise the internal unique identification of all items. Each product is setup according to O.Config-Control comprising all necessary items.
ALC_CMC.5.4C: The CM system shall uniquely identify all configuration items.	O.Config-Items O.Config-Control	O.Config-Items comprise the internal unique identification of all item. 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.Data-Transfert	O.Config-Control assigns the setup including processes and items for the development of each part ID. O.Config-Process comprises the control of the development processes. O.Logical-Access support the control by limiting the access and ensuring the correct operation for all tasks to authorized staff. O.Data-Transfer to ensure received data are recorded in CM system.
ALC_CMC.5.6C: The CM system shall support the production of the product by automated means.	O.Config-Process O.Config-Control O.Acceptance-Test O.Data-Transfer	O.Config-Process comprises the automated management of the development processes. O.Config-Control assigns the setup including processes and items for the development of each part ID. O.Acceptance-Test provides an automated testing of the product quality and supports the tracing. O.Data-Transfer to ensure received data are transferred and managed in CM system.

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
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.Logical-Access O.Logical-Operation O.Data-Transfer.	O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staffs difference access assignment. O.Data-Transfer ensure that the data received from third party is managed locally in the CM system
ALC_CMC.5.8C: The CM system shall clearly identify the configuration items that comprise the TSF.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items comprises the internal unique identification of all items. O.Config-Control describes the management of the part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site.
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.Acceptance-Test O.Config-Control O.Config-Process	O.Config-Items comprise the internal unique identification of all items. O.Config-Control describes the management of the part IDs at the site the development control comprises steps and there by includes the required audit trail including the originator. According to O.Config-Process the CM plans describe the services provided by the site. O.Acceptance-Test provides an automated testing and supports the tracing.
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 describes the management of the part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site. O.Config-Process also ensures that only controlled changes are applied.
ALC_CMC.5.11C: The CM system shall be able to identify the version of the implementation representation from which the delivered configurations item.	O.Logical-Access O.Config-Control O.Config-Process O.Logical-Operation	O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operation for all tasks to authorised staff. O.Config-Control describes the management of the 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-Control O.Config-Process	O.Config-Control describes the management of the 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 TOE.	O.Config-Control O.Config-Process	O.Config-Control describes the management of the part IDs at the site. According to O.Config-Process the CM plans describe the services provided by the site

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
ALC_CMC.5.14C: The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the product.	O.Config-Items O.Config-Control O.Config-Process	O.Config-Items ensure the unique identification of each item. 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.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O.Config-Control O.Config-Process	The objectives: O.Config-Control, O. Config-Process ensure that only released part IDs are produced.
ALC_CMC.5.16C: The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.	O.Config-Control O.Config-Process	O.Config-Control comprises a release procedure as evidence. O.Config-Process ensures the compliance of the process.

Table 8: Security Assurance Rationale for ALC_CMC.5

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
ALC_CMS.5.1C: The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and related information. The CM documentation shall include a CM plan	O.Config-Items O.Config-Control O.Config-Process	Since the process is 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 developed for this part. O.Config-Control describes the release process for each part ID. O.Config-Process defined the configuration control including part ID's procedures and processes.
ALC_CMS.5.2C: The configuration list shall uniquely identify the configuration items.	O.Config-Items O.Config-Control	Items, products and processes are uniquely identified by the data base system according to O.Config-Items. Within the development process the unique identification is supported by automated tools according to O.Config-Control.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O.Config-Items	According to O.Config-Items all configuration items for secure products are identified.

Table 9: Security Assurance Rationale for ALC_CMS.5

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.	O.Physical-Access O.Security-Control O.Alarm-Response O.Maintain-Security O.Logical-Access O.Logical-Operation O.Staff-Engagement O.Data-Transfer O.Control-Scrap	The physical protection is provided by: O.Physical-Access, supported by O. Security-Control, O.Alarm- Response. The associated control and continuous justification is subject of the objectives O.Logical-Operation and O.Maintain-Security. The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical- Operation. The personnel security measures are provided by O.Staff- Engagement. Sensitive data received and send by the site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only. Any scrap that may support an attacker is controlled according to O.Control-Scrap.
ALC_DVS.2.2C: The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Acceptance-Test O.Data-Transfer	The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical-Operation and O.Maintain-Security. O.Acceptance-Test supports the integrity control by testing of the finished products. Sensitive data received and send by the site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.
ALC_DVS.2.3C: The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.	O.Internal-Monitor O.Logical-Operation O.Maintain-Security O.Acceptance-Test O.Data-Transfer	The associated control and continuous justification is subject of the objectives O.Internal-Monitor, O.Logical- Operation and O.Maintain-Security. O.Acceptance-Test supports the integrity control by testing of the achieved TOE development. Sensitive data received and send by the site is encrypted according to O.Data-Transfer to ensure access by authorized recipients only.

Table 10: Security Assurance Rationale for ALC_DVS.2

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
ALC_LCD.1.1C: The lifecycle Definition documentation shall describe the model used to develop and maintain the TOE.	O. Config-Control O. Config-Process	The processes used for identification and manufacturing are covered by O.Config-Control and O. Config-Process.
ALC_LCD.1.2C: The lifecycle model shall provide for the necessary control over the development and maintenance of the TOE.	O.Acceptance-Test O. Config-Process	The applied development process is controlled according to O.Config- Process. The finished products are tested according O.Acceptance-Test.

Table 11 Security Assurance Rationale for ALC_LCD.1

SARs	Security Objective	Rationale (text of objectives in this column can/shall be modified by ST NOIDA to reflect the truth)
ALC_TAT.3.1C Each development tool used for implementation shall be well-defined.	O.Config- Control	O.Config-Process comprises the automated management of the development processes, including the development tools.
ALC_TAT.3.2C The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	O.Config-Process O.Config-Control	O.Config-Process comprises the automated management of the development processes, including the development tools. O.Config-Control assigns the setup including processes and items for the development of each part ID and tools.
ALC_TAT.3.3C The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.	O.Config-Process O.Config-Control	O.Config-Process comprises the automated management of the development processes, including the development tools. O.Config-Control assigns the setup including processes and items for the development of each part ID and tools.

Table 12 Security Assurance Rationale for ALC_TAT.3

7.6 SITE SUMMARY SPECIFICATION

The Site Summary Specification describes how the site meets the SARs.

7.6.1 Preconditions Required by the Site

This section provides background information on the assumptions.

Assumption	Precondition
A.Item-Identification	Each configuration item (IP) shipped from a client to the development site is uniquely labelled by the client to ensure the identification of the configuration item.
A.Product-Setup	The site participates in the development of products. To define the participation of the site in the development while maintaining quality, for each product the site and STM agree on the activities to be performed by the site, the specifications of the input for the site and the acceptance of the results by STM.
A.Shipment	To enable the site to realize shipment such that assurance of integrity is assured throughout transport of security objects STM will adhere to the shipment method as described in the life cycle documentation.

Table 13: Precondition of Assumptions

A.Item-Identification: Every portion coming from outside the development site that is necessary for the secure development activities (IPs, ROM Code, Security specifications) is tagged with a unique hash at the source. Such hash code is sent separately from the item itself and it is checked against the received package to uniquely identify it.

A.Product-Setup: The development activities performed in the site are a subset of the standard set of activities defined by the Product-Development-Process, a document that guides all the development activities across the company. The extent of the activity subset performed at the site, in terms of definition of inputs and deliverables is defined to be limited to the logical design and verification of the security modules to be embedded into the products.

A.Shipment: The security modules logically designed and verified in the site, are packaged in an encrypted form so that their content cannot be inspected, and separately accompanied by a hash code that must be matched at the destination to ensure the integrity of the package.

7.6.2 Services of the Site

ST NOIDA provides Hardware Design services for automotive products, and in particular the secure portion of the site is providing logical design and verification of security modules.

The only service provided by the site can be summarized as “Design and verification of security modules/subsystems”

It is detailed at section 5.3 Site Description.

7.6.3 Rationale

The objectives rationale is provided at Security Objectives Rationale section. The following rationale gives more justification on how all threats and organizational security policies are effectively addressed by the security objectives.

7.6.3.1 Objectives mapping

The table below demonstrates that all threats and OSP are mapped to at least one security objective.

	O.Physical-Access	O.Security-Control	O.Alarm-Response	O.Internal-Monitor	O.Maintain-Security	O.Logical-Access	O.Logical-Operation	O.Config-Items	O.Config-Control
T.Smart-Theft	X	X	X	X	X				
T.Rugged-Theft	X	X	X	X	X				
T.Computer-Net				X	X	X	X		
T.Unauthorized-Staff	X	X	X	X	X	X	X		
T.Staff-Collusion				X	X				
T.Attack-Transport									
P.Config-Items								X	
P.Config-Control						X		X	X
P.Config-Process									
P.Reception-Control									
P.Accept-Product									X
P.Data-Transfer									

Table 14 - Objectives mapping

	O.Config-Process	O.Acceptance-Test	O.Staff-Engagement	OData-Transfer	O.Control-Scrap
T.Smart-Theft					X
T.Rugged-Theft					X
T.Computer-Net			X		
T.Unauthorized-Staff			X		X
T.Staff-Collusion			X	X	X
T.Attack-Transport				X	
P.Config-Items				X	
P.Config-Control					
P.Config-Process	X				
P.Reception-Control				X	
P.Accept-Product	X	X			
P.Data-Transfer				X	

Table 15 - Objectives mapping (continued)

7.6.3.2 Objectives Rationale

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

O.Physical- Access

The site is surrounded by a fence and controlled by CCTV. The access to the site is only possible via access controlled doors. The enabling of the alarm system and the additional external controls are managed according to the running operation at the site. The physical, technical and organizational security measures ensure a separation of the site into several security levels. The access control ensures that only registered and authorized persons can access sensitive areas.

This is supported by O. Security- Control that includes the maintenance of the access control and the control of visitors. The physical security measured is supported by O. Alarm-Response providing an alarm system.

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

O.Security-Control

During working hours, the security officer will monitor the site and surveillance system. During off-hours, the alarm system is used to monitor the site. The CCTV systems support these measures because it is always enabled.

Further on the security control is supported by O. Physical Access requiring different level of access control for the access to security product during operation as well as during off hours.

This addresses the threats T. Smart-Theft and 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

During working hours, the security officer will monitor the alarm system. The alarm system is connected to a control center that is running 24 hours. O. Physical-Access requires certain time to overcome the different level of access control. The response time of the security officer and security response team (who is on duty) are needed to provide an effective alarm response

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

O.Internal-Monitor

Regular security management meetings are implemented to monitor security incidences as well as changes or updates of security relevant systems and processes. This comprises also logs and security events of security relevant systems like firewall, Virus protection and success control. Major changes of security systems and security procedures are reviewed in general management security review meetings (min. 1 per year

This addresses T. Smart-Theft, T.Rugged-Theft, T. Computer-Net, T.Unauthorised-staff, T.staff-Collusion.

O.Maintain Security

The security relevant systems enforcing or supporting O. Physical-Access, O. security-Control and O. Logical-Access are checked regularly by the security officer. In case of maintenance, it is done by the suppliers. In addition, the configuration is updated as required by authorized security officer (for the access control system). Log files are also checked for technical problems and specific maintenance requests.

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

O.Logical-Access

The internal network is separated from the internet with a firewall. The internal network is further separated into sub networks by internal firewalls. These firewalls allow only authorized information exchange between the internal sub networks. Each user is logging into the system with his personalized user ID and password. The objective is supported by O.Internal-Monitor based on the checks of the logging regarding security relevant events.

The individual accounts are addressing T. Computer-Net.

All configurations items are stored in the development database system. Supported by O. Config-Items.

This addresses the threats T. Unauthorized-Staff, T.Computer-Net and the OSP P. Config-Control.

O.Logical-Operation

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

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

O.Config-Items

The configuration management system is in place and assigns a unique internal identification to each product under development to uniquely identify configuration. Items.

This addresses the OSP P. Config-Items and P. Config-Control.

O.Config-Control

Procedures arrange for a formal release of achieved TOE development. Engineering Change Procedures are in place to classify and introduce changes. These procedures also define the separation between minor and major changes. The CM system requires restricted access controlled by login and passwords. Each user has limited access rights based on “the need to know” principle. Thereby only authorized changes are possible. Supported by O. Config-items

This addresses the OSP P. Config-Control and P.Accept-Product.

O.Config-Process

The product is developed following on the development procedure. Release configuration items are maintained in a dedicated directory of the development database.

This addresses the OSP P.Config-process and P.Accept Product.

O.Acceptance-Test

Third-party IPs acceptance is managed once received by the developer in charge of their integration in the development project. For validation test after TOE development achievement, the TOE is subject to validation test before physical layout operation is performed. The tools, specifications and procedures for tests are controlled by the means of O. Config items and O. Config-Control. Acceptance results are logged and linked to a work order in the ERP system.

This addresses the OSP P. Accept-Product.

O. Staff-Engagement

All employees are interviewed before hiring. They must sign and NDA and the staff compliance agreement on Security matters before they start to work in the company. The formal training and qualification include security relevant subjects and the principles of maintaining security during development.

The security objectives O. Physical-Access, O. Logical-Access and O. Config-Items support the engagement of the staff.

This addresses the threats T. Computer-Net, T. Unauthorized-Staff, T. Staff-Collusion.

O.Data-transfer

Sensitive electronic information is received and transferred encrypted using PGP. Supported by O. Logical Access and O. Staff-engagement

This addresses the threats T. Staff Collusion and T. Attack-Transport as well as the OSPs P. Data-transfer, P.Config-Items and P.Reception-Control.

O.Control-Scrap

Scrap is identified and handled as sensitive assets. The scrap is destructed with appropriate tool (e.g. paper shredder). Sensitive information and information storage media are collected internally in a safe location and destructed in supervised and documented process. Supported by O. Physical-Access and O. Staff-engagement.

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

7.6.4 Security Assurance Requirements Rationale

The Security Assurance rationale is provided in Security Assurance Rationale. The following rationale gives more justification for the selected Security Assurance Requirements:

- ALC_CMC.5: Advanced support,
- ALC_CMS.5: Development tools CM coverage,

- ALC_DVS.2: Sufficiency of security measures,
- ALC_LCD.1: Developer defined life-cycle model,
- ALC_TAT.3: Compliance with implementation standards - all parts.

ALC_CMC.5

The chosen assurance level ALC_CMC.5 of the assurance family “CM capabilities” is suitable to support the development due to the formalized acceptance process and the automated support. The identification of all configuration items supports an automated and industrialized process. The requirement for authorized changes and ability to identify the changes and version of the implementation will support the integrity and confidentiality required for the products under development. Responsibility of different departmental teams is also cleared identified for accepting or authorizing any change on the configuration items. Therefore, these assurance requirements stated will meet the requirements for the configuration management.

ALC_CMS.5

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

ALC_DVS.2

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

ALC_LCD.1

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

ALC_TAT.3

The chosen assurance level ALC_TAT.3 of the assurance family “Tools and techniques” are necessary to support the development process. The site defines which tools and techniques have to be used. The company provides the complete environment with all necessary tools. The proper usage of the provided tools and defined techniques is verified during audits.

7.6.5 Assurance Measure Rationale

O.Physical-Access

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

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.

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.

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. ALC_DVS.2.3C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the 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 and ALC_DVS.2.3C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Access

ALC_CMC.5.5C: Requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. Thereby this objective contributes to meet the security Assurance Requirement. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified.

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.

Thereby this objective contributes to meet the Security Assurance Requirement.

O.Logical-Operation

ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified.

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. ALC_DVS.2.3C: The development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

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

O.Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. A method used to uniquely identify the configuration items is required by ALC_CMC.5.3C. In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.14C requires that the CM plan describes the procedures used to accept modified or newly created configuration items as part of the TOE. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration items is indicated in the configuration list.

The objective meets the set of Security Assurance Requirements.

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. A method used to uniquely identify the configuration items is required by ALC_CMC.5.3C. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. 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 (production) 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 TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfillment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC CMC.5.4C.

In addition, ALC_LCD.1.1C requires that the life cycle definition describes the model used to develop and maintain the products.

ALC_TAT.3.1C requires that each development tool used for implementation shall be well-defined. ALC_TAT.3.2C requires that documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation. ALC_TAT.3.3C requires that documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

The objective meets the set of Security Assurance Requirements.

O.Config-Process

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. The provision of automated measures such that only authorized changes are made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. ALC_CMC.5.9C requires the support of audit information for all changes to the TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a chance given to a configuration item. ALC_CMC.5.11C requires that the version of test programs and the production processes used for production can be identified. 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 TOE. ALC_CMC.5.15C requests evidence to demonstrate that all configuration items are being maintained under the CM system. ALC_CMC.5.16C requires that the evidence shall demonstrate that the CM system is operated in accordance with the CM plan.

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

ALC_LCD.1.1C requires that the lifecycle definition documentation describes the model used to develop and maintain the products. ALC_LCD.1.2C requires control over the development and maintenance of the TOE.

ALC_TAT.3.2C requires that documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation. ALC_TAT.3.3C requires that documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

The objective meets the set of Security Assurance Requirements.

O.Acceptance-Test

Product acceptance is introduced and released based on the client approval with the tools, specification and procedure for these tests. They are controlled by the means of O. Config-items and O. Config-Control. Acceptance test results are logged and linked to a work order in the MES.

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

ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the TOE during production. ALC_DVS.2.3C requires that evidence justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

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

Thereby the objective fulfils this combination of Security Assurance Requirements.

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Thereby the objective fulfills this combination of Security Assurance Requirements.

O.Data-Transfer

ALC_DVS.2.1C requires security measures that are necessary to protect the confidentiality and integrity of the TOE

ALC_DVS.2.2C: The development Security documentation shall describe all the Physical, Procedural, personnel and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.2.3C requires confidentiality and integrity of the product during internal shipment.

ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it.

This objective will meet the Security Assurance Requirement.

O.Control-Scrap

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

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

8 QUALITY REQUIREMENTS

All records described in this procedure shall be stored in the company-controlled document system and characterized according to specific attributes.

9 ENVIRONMENTAL/ECOLOGICAL REQUIREMENTS

STMicroelectronics recommends viewing documents on the screen rather than printing to limit paper consumption.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.