REVISION HISTORY

REV	FROM		TO
I	- Corrections following SERMA's remarks.		- Complete rewrite.
	ECN : 2871/18	DATE : Nov 30,18	ORIGINATOR : Chayanan S.
J	- Revise the mistake of address at §2.1 and the Production Service is not included testing at §2.2 - Resizing the sentence to Tahoma 10" - Correct the Service of transportation - Number is not correct.		- Revise the §2.1 at correct address of U1 and revise §2.2 for the production service. - Resizing the sentence to Tahoma 10" - Corrected the service of transportation from Security to MH at §2.2 - Renumbering
	ECN : 2929/18	DATE : Nov 06,18	ORIGINATOR : Chayanan S.

Table of Contents

1 Introduction

The purpose of this document is to describe the security target for the Assembly of Secure Wafers and ICs specifics for UTAC Thai Limited.

1.1 Site Security Target Reference

Title	Site Security Target
Document Name	UTAC THAI LIMITED (UTL) : UTL1 PUBLIC SITE SECURITY TARGET
Version Number	J
Date	DEC 6'18
Site	UTL1
Site Location	237 Lasalle Road, Bangna, Bangkok, 10260, THAILAND
Product Type	Security Wafers and ICs
EAL – Level	EAL 6
Evaluation Body	SERMA Safety and Security – ITSEF
Certification Body	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*

*Note that only classes AST and ALC are applicable for Site Certification Objectives in this Security Target

1.2 Site References

REFERENCE

1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model Version 3.1 Revision 5, April 2017 CCMB-2012-09-001[1]
2	Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Components Version 3.1 Revision 5, April 2017 CCMB-2012-09-002 [2]
3	Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Components Version 3.1 Revision 5, April 2017 CCMB-2012-09-003 [3]
4	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology Version 3.1, Revision 5, April 2017 CCMB-2017-04-004
5	Common Criteria Supporting Document Guidance Site Certification October 2007 Version 1.0 Revision 1 CCDB-2007-11-001
6	Joint Interpretation Library Minimum Site Security Requirements Version 2.1 (For trial Use) December 2017
7	Bundesamt für sicherheit der informationstechnik guidance for site certification version 1.0
8	Security IC Platform Protection Profile Version 1.0. (15.06.2017) ref: BSI-PP-0035
9	Security IC Platform Protection Profile with Augmentation package version 7.0 Ref BSI-PP-0084

2 SST Introduction

2.1 Site Identification

The SST is referring to UTAC Thai Limited located in Thailand (UTL) that provided the Assembly service of Secure Wafers and ICs. This SST is specific for site abbreviated as 'UTL1' which is located at:

237 Lasalle Road, Bangna, Bangkok, 10260, THAILAND

Main activity at this site is manufacturing of Secured and Non-Secured products consist of production, engineering, store, waehousing and office. Products and description of buildings utilization;

Products & Services: Assembly of QFN products of Wafers and ICs

Building utilization:

Building 1	:	Manufacturing and Office
Building 2	:	Manufacturing and Canteen
Building 3	:	Facility and Utility
Building 4	:	Store
Building 5	:	Waste Water Treatment Plant
Building 6	:	Office
Building 7	:	Office

Description of the site activities :

Incoming raw Material (Secure IC Wafers and other raw materials)

Clients who need Secured products will send to UTL1 their Security IC Wafers for assembly. Clients also provide the specification, built instruction to the site in order to start the assembly production.

Receiving

Upon physical receipt of the Security IC Wafers (in boxes) or assembly finished Secure products from UTL1 assembly sites or direct from clients at receiving area, the site will key the incoming material into the system. These wafers or finished assembly products have a unique identification code which is electronically setup by the site so that traceability of each wafer is properly recorded and accounted for. The raw materials which are yet to be processed into the manufacturing process are transferred to Die Bank store which entry is accessed only by authorized personnel.

Die Bank Store

Upon physical receipt of lot at Die Bank Store, the die bank personnel will transact the lot into the MES (Manufacturing Execution System). After which, it is unpacked and sent Wafers for Incoming Quality Inspection. The Process Traveller is generated and attached to the lot prior to sending lot to other process or to Wafer Sort process. Transfers between Die Bank store and the different production process are also monitored using the electronic production WIP system which tracks the traceability of the wafers.

Assembly (for QFN Products)

Before any mass production is conducted in assembly process, the site will have already optimized the production process during the NPI (New Product Introduction) stage where the site will review the client spec requirements, run qualification and pre-production lots. Data on the runs are sent to client for their review and final approval for full production. For every mass production launch, each job is assigned a unique production lot ID which will be traced from the start to finish through the MES. The site also practices Zero Balancing where each die in the wafer or each packaged unit is traced and accounted through-out the process. An assembly process traveller document is attached to each production lot.

Wafer Taping [option]:

This is the process where the active side is protected with a back grinding tape to protect while the wafer undergoes back-grinding during the next process. Lot In/Out is transacted in the MES.

Wafer Back Grinding:

The taped wafers are then back-grinded to the desired thickness as required by the client in the Assembly Build Instruction. Back-grinding process recipe is auto-download by scanning of the barcode in the process traveler. Lot In/Out is transacted in the MES. Once completed back-grinding process the tape is then removed from the wafer.

Wafer Grooving/Dicing:

For low K wafers (< 65 nano), grooving process is required prior to wafer saw. When wafers are un-sawn, the site will need to perform a sawing process to isolate the different ICs in a wafer. Both grooving and wafer saw recipe are auto-downloaded through UTL1's Recipe Management System. Lot In/Out is transacted in the MES. Once the wafers are completely sawn, the lot goes through UV cure, Post saw inspection and then goes to start the die attach process. Lot In/out are transacted in the MES for each process stage. Wafer Map diagrams of the wafers are either provided by the client or downloaded through their secured server, each wafer is uniquely identifiable with their wafer lot numbers. Lot In/out are transacted in the MES for each process stage.

Wafer Taping:

This is the process where the active side is protected with a back-grinding tape to protect while the wafer undergoes back-grinding during the next process. Lot In/Out is transacted in the MES.

Wafer Back Grinding:

The taped wafers are then back-grinded to the desired thickness as required by the client in the Assembly Build Instruction. Back-grinding process recipe is auto-download by scanning of the barcode in the process traveler. Lot In/Out is transacted in the MES. Once completed back-grinding process the tape is then removed from the wafer.

Wafer Mount:

The back-grinded wafers are then mounted on a wafer ring to prepare it for the grooving and/or wafer dicing processes. Lot In/Out is transacted in the MES.

Wafer Grooving/Dicing:

For low K wafers (< 65 nano), grooving process is required prior to wafer saw. When wafers are un-sawn, the site will need to perform a sawing process to isolate the different ICs in a wafer. Both grooving and wafer saw recipe are auto-downloaded through UTL1's Recipe Management System. Lot In/Out is transacted in the MES. Once the wafers are completely sawn, the lot goes through UV cure, Post saw inspection and then goes to start the die attach process. Lot In/out are transacted in the MES for each process stage. Wafer Map diagrams of the wafers are either provided by the client or downloaded through

their secured server, each wafer is uniquely identifiable with their wafer lot numbers. Lot In/out are transacted in the MES for each process stage.

Die Bonding (Process of attaching die to substrate):
The strong adhesion of the die to the substrate would be the key in this process and the adhesion is made possible using a die attach paste and with the use of thermal oven curing. Lot In/Out is transacted in the MES. For wafers which are already sawn, this will be the first production process step.

Epoxy cure:
Generate the proper adhesion among die's back side, epoxy and substrate (lead frame) by heating to assure it is completion create the cross link.

Plasma Cleaning:
Clean the die's surface & substrate (lead frame)'s surface for improving the wire bond capability.

Wire bonding:
After the die attach is completed, the dies would need to be bonded to the substrate using gold wires, copper wire or copper wire coated with palladium or other material depended on client requirement, and the different pads of the dies are bonded to the bonding pads of the substrate to ensure connectivity. Lot In/Out is transacted in the MES.

Molding:
Encapsulation process is to ensure that the wire bonded products are properly protected by plastic mold compound which is covering the entire area of the package. High Temperature resin is used in this process. Lot In/Out is transacted in the MES.

Post Mold Cure:
After molding, the dies are encapsulated with thermo-setting molding compound and cured. Lot In/Out is transacted in the MES.

Detaping:
This process is to remove back grinding tape out of the substrate. Lot In/Out is transacted in the MES.

Buffing/Frame Cleaning:
This cleaning process is to remove mold flash on the leadframe and substrate by buffing machine or by high pressure water at the entire area of the package. Lot In/Out is transacted in the MES.

Plating:
A manufacturing process to apply a thin layer of metal coats to metal part of the substrate by electroplating, which requires an electric current. Lot In/Out is transacted in the MES. For the substrate using pre-plated lead frame, the plating process is not requiring.

Package Cure:
Generate the proper adhesion of mold compound by heating to assure it is completion create the cross link.

Marking :
This process is to produces a highly legible and completely indelible mark over the package. Marking can be both contact process using ink and a non-contact process using laser to be produced as needed. Lot In/Out is transacted in the MES.

Saw Singulation:
Encapsulated packages are mechanically sawn to isolate into individual units. Lot In/Out is transacted in the MES.

UV erase:
Reduce the adhesion between singulated unit and dicing tape for easier removal.

Auto VM:
After singulation, the lot is sent for 100% auto visual-mechanical inspection. Visual defect/reject units are separated from the good units. Lot In/Out is transacted in the MES. The rejected units are placed inside a plastic bag and security sealed before sent to the Reject Control Center. (Note: Rejects are placed inside a caged trolley with combination lock when transporting to the Reject Control Center)

Packing:
Depending on the client's packing requirements, the final assembly packaging of the secure devices are packed in tube, tray or canister format based on the requirement of client or the re-test process need. For product do not require re-test, will pack in intermediate boxes and then proper outer boxes with identification labels as required by the client. For product require re-test, will pack into intermediate boxes then put into transfer cart with security seal and send to re-test at other site.

Destruction of secured reject materials (MES):
The good and bad dies in the wafers are all tracked using the Zero Balancing from start of production to the end of the production and are also recorded electronically in the manufacturing production system. For client who has requested that the scrap dies and wafers to be ship back to them, they will arrange the appropriate transportation to be ship back to their facility. For client who has requested that the scrap material to be destroyed, the site will dispose the secured scrap material in proper containers with the relevant procedure before the scrap materials are collected and transported to client's site.

Internal Shipment to clients:
Shipments are considered to the internal shipment as they are route back to the client whereby the client will arrange their own contractors which UTL1 security performs the necessary security checks before they are allowed to collect the materials. The site will inform the client upon completion of the production order and the completed products are ready for collection.

2.2 Site Description

The site consists of production facilities, incoming and outgoing material / finished products, warehousing, production, product and process engineering, client service and information technology (IT) management.

Physical security :

The following areas of the site are in scope of the Site Security Target: The entire perimeter of the building premises, surrounded with a fence and gate. The main entrance of the building, secured with a car barrier for vehicle. The Building 1 is meaning for Manufacturing, equipped with full height turnstiles with SAM Access for first protection layer. The CCTV cameras, installed on strategic locations along the perimeter. The building entry.

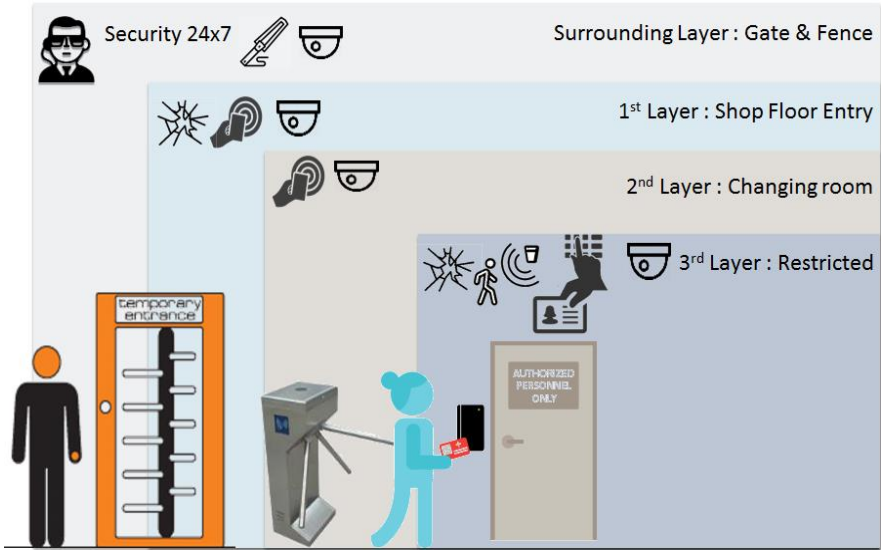

Figure 1 UTL Security layer and premises control

The Security Control Room for surveillance monitoring. Access controls, restricted access and CCTV surveillance cameras are also located at various locations within UTL1 facility. The Access with SAM for security control room is for dual authentication.

Supporting services are located at Building 3 and Building 5, this service includes the Facility and Utility. IT department at Building 1 and failure analysis at Building 6.

The backup center is located back site of Building 1 with same protection measures and is administrated by the same IT department. The Security Control room is CCTV footages in the identified secure areas within UTL1 facility are housed in the Security Command Center for surveillance. UTL1 provides the isolate network infrastructure and physical security of production.

Security guards are stationed at Employee entrance, Loading Bay, Shipping areas. Security checks/patrols are also conducted within night time. The guards operated by 24 hours and 7 days a week. In general, the relevant physical sections that are target of the evaluation process are the areas that are directly involved in the services and/or processes of the site used for security products as well as areas that support these either from operational point of view (configuration control, operation control, location of IT-system, warehouse, etc) or from organizational point of view (site security

organization and control, maintenance of systems and tool, Failure Analysis and Reliability services, Customer services etc).

The Transportation of materials is physically secured and controlled by Material Handler of Production.

Employee card is handled with Mifare DesFire EV2. The Access into the building is restricted by a series of contactless card reader under SAM.

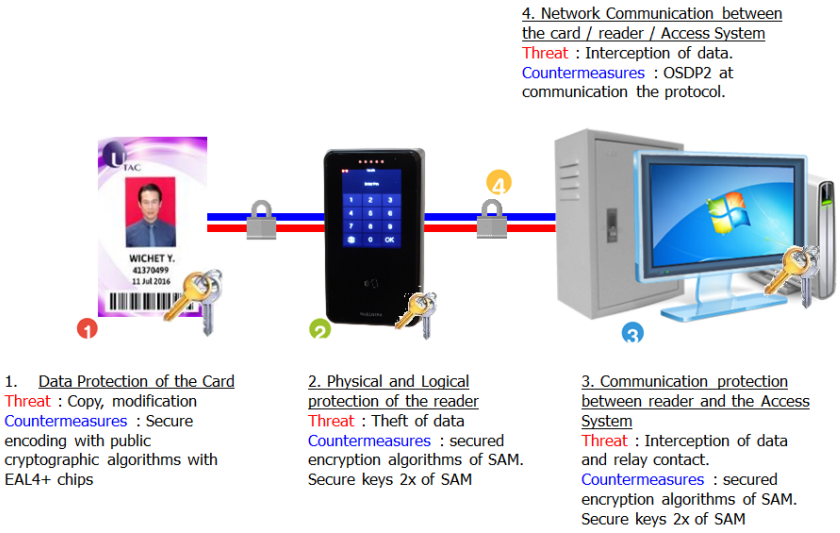

Figure 2 UTL Security for Badge & Reader

Life cycle scope :

The services provided by UTL are part of the phase 4: IC Packaging, as defined in [8] and [9]. After manufacturing the products are returned to the owner of the product (the client).

The provided services include the following processes: Receiving and storage of security wafers, Production/manufacturing of the security ICs, Logistics-Incoming wafers, outgoing finish goods, Storage, Handling of Scrap materials from production process to destruction.

The complete logical flow of the Security ICs at the site is covered by this SST. The management of the related processes and site security are also covered by this SST. The product flow of the security ICs on the site begins with the receipt of parts of the TOE (raw materials) up to the packing and handover for the shipment of the finished Security ICs.

Logical Security (IT)

The Network Diagram is main of Network design. Linkage between site with redundancy devices and carrier are provided with site to site secure connection with [esp – aes 256 bit]

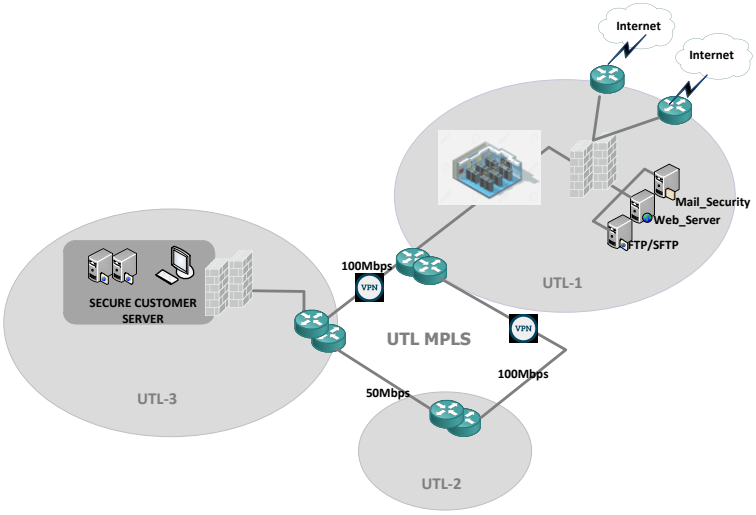

Figure 3 UTL Network Diagram

The associated scripts and keys remain security items during receiving, handling and production just like the physical chips or their chip firm of software. There are measures and processes in place which ensure the unique correlation of products and scripts through the production flow. The scripts used for the initialization can be developed by the client or by UTL. The overall integrity control of the initialization process must be supply by security keys. The Pre-Personalization of security modules includes the testing and operating system, loading of complete modules as any logical part of the TOE.

The Security Architecture Protection is provided on site with redundancy firewall devices and dedicated management (MGT) server (located at UTL1). The security functions allow only specific service of deny by default from external DMZ zone. IT infrastructure is located and managed from UTL1.

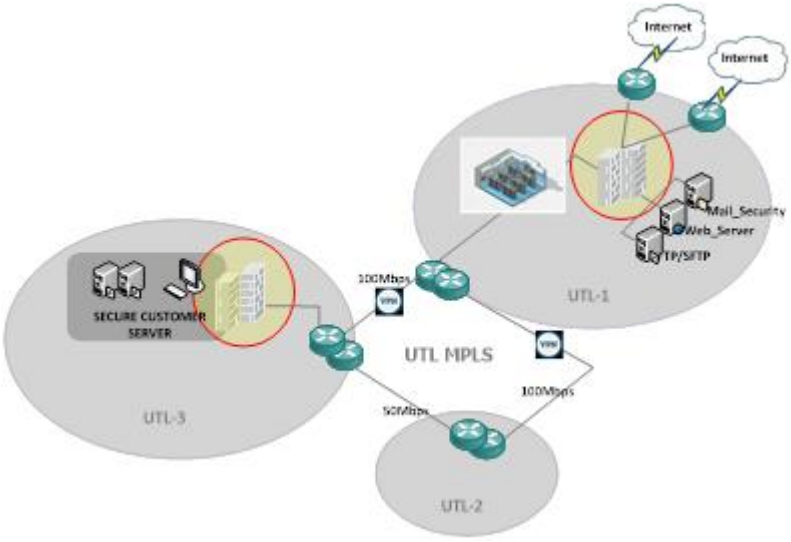

Figure 4 UTL Security Architecture Protections

The terminal for managing the firewall is in secured data centre (at UTL1); only administration area with no access from outside and internal, must direct to manage the firewalls which limited by IP address, this IP address is fixed and reserve in DHCP. Wireless connection that provide for production and operation usage shall be encrypted.

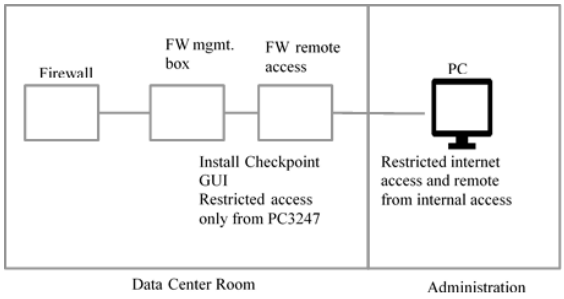

Figure 6 UTL firewall's client access

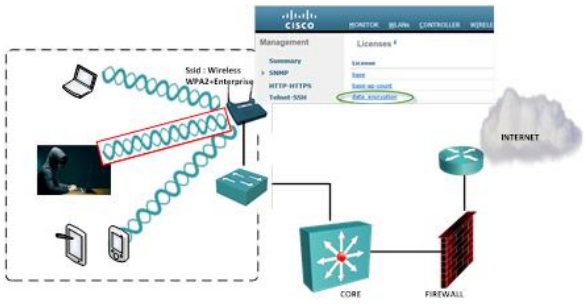

Figure 7 UTL wireless security

3 Conformance Claims (AST_CCL)

3.1 Version on Common Criteria

- The Supporting Document: Site Certification, Revision 1 October 2007 [CC0B-2007-11-001]
- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model Version 3.1 Revision 5, April 2017 CCMB-2012-09-001[1]
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Components Version 3.1 Revision 5, April 2017 CCMB-2012-09-003 [3]

3.2 The methodology used for the evaluation:

- Common Methodology for IT security Evaluation, Evaluation Methodology, April 2017 Version 3.1 Revision 5.
- Minimum Site Security Requirement, version2.1, December 2017

3.3 Conformance claim:

This SST is conformant with Common Criteria Version 3.1, revision 5

This SST is CC Part 3 conformant

There are no extended components required for this SST

3.3.1 Evaluated Assurance Components are from the assurance level EAL6 Package:

- ALC_CMC.5 Advance support
- ALC_CMS.5 Development tools CM Coverage
- ALC_DVS.2 Sufficiency of security measures
- ALC_LCD.1 Developer defined life-cycle model

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

The assurance components chosen for the Site Security Target are compliant to the Protection Profile (PP) [9]. Therefore, the scope of the evaluation is suitable to support product evaluations up to assurance EAL6 conformant to Part 3 of the Common Criteria.

The site does not directly contribute to the development of the intended TOE in the sense of Common Criteria. The site ensures a reproducible production process within the limits defined for the production process. This is subject of the configuration management. Therefore, the site does not cover any aspects that are covered by ALC_TAT.

Since the security product is returned to the client after processing and not to the user, thence the site does not perform Delivery at the meaning of Common Criteria. Thus the site does not cover any aspects that are covered by ALC_DEL. Internal shipment is covered under ALC_DVS2.

4 Security Problem Definition (AST_SPD.1)

The security problems are derived from the potential threats based on the assets owned by the site and the Organizational Security Policies (OSP) are also defined in this section. The security problem definition comprises of mainly: Theft of information, physical theft of assets and lapse in Physical/ Logical Security-in Production Process. These threats are described generally in the SST to cover the aspect of potential attacks which the site has detailed procedures, access matrix, layout, blueprints that governs the security of the site.

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

5 Assets

This section describes the assets handled at the site. The site has internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE. This comprises site security policies and measures which aims to protect the assets for the maintenance of appropriate controls.

Assets refer to the security elements which are received/ consigned by clients/ owned by the site as follow (but not limited to): Client's Secure Wafers and ICs, Client's finished products and other forms of identity ICs packages, Secure ICs and Wafers which are rejected in the manufacturing process or intended for scrap, Client owned hardware for secure products and Security seal.

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

The integrity of any machinery or tooling used for production is not considered as part of the definition of an asset. However, the site has maintained procedures, measures and internal documentation to ensure the importance of this condition.

The site specific internal documentation and data that is relevant to maintain the confidentiality and integrity of an intended TOE is considered as asset. This comprises the site security concept and the associated security measures as well as keys and cryptographic tools for the encrypted exchange of data. These items are not explicitly listed in the list of assets below.

The integrity of any machines and hardware/software used for production, testing and initialization are not considered as an asset. However, appropriated measures are defined for the site to ensure this important condition. Therese items normally consist of standard hardware and software which are programmed or customized for their purpose at UTL only.

The equipment and tools used to store sensitive data related to initialization and / or COS upload are considered as assets.

- Wafer and packaged security ICs (like modules or other packages),
- Finished security product (like an IC with optional initialization),
- Reject and defect wafer dice, packaged security ICs and Security Products,
- Classified Product Specifications,
- Initialization data including initialization scripts and keys use for the initialization.

6 Threats

Threats refer to the potential attacks which could possibly threaten the confidentiality and integrity of the TOE. These threats could possible happen from incoming of materials (secured wafers, IC and dies), in production and in the shipment of secured products. These threats are described generally and are applicable to the site. Following are major threats which describe the potential attacks:

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the IT.

The intended TOE and the representation of parts of the intended TOE are vulnerable to attacks during development; assemble test and initialization including update of a COS.

The following threats are described in a general way; however, they are applicable to the site provided service and handling assets as describe in the upper sentence as above. The explanation below the threats shall allow addressing the security objectives according to the site-specific aspects.

T. Smart-Theft

In situation where the attacker plans to access the authorised area or restricted boundaries for the purpose of stealing secured items from the site. This attacker could use tools or equipment to break into the physical boundary of the company or building. Potential Physical theft could also happen during incoming of raw material, during in process of manufacturing production till shipment of the finish goods. Concerned assets include Clients Secured Wafers and ICs, Secure IC wafers which are rejected in the manufacturing process or intended for scrap, special transport protection like security seals that support the security of the internal shipment to the client.

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 used or rejected devices that can be used to further investigate the functionality of the device and search for further exploits.

The time spent by an attacker to prepare the attack and the flexibility of such an attack will provide big risk.

Potential attackers could be either existing employee of the company or external attackers whom are not existing employees. It will cause the company financial loss and loss of reputation as the goods are entrusted to the site by the client.

The site has implemented different levels of access control depending on the security restriction of the area. Some additional measures of the different level of access will include additional password entry or escorted by security personnel. Tools like security burglar alarms and CCTV cameras are also installed throughout the entire company to enhance the physical security of the company.

During production of the secure products there are risks of theft from employees. Zero Balancing of security products are observed in the production process. Tracking all pass and fail security parts at incoming, outgoing and during the production process steps on a list and ensuring that all the security wafers are accounted for zero balancing at shop floor control.

T. Rugged-Theft

In a situation where the attacker is experienced, plans to attack by accessing the permissible area or restricted boundaries for sensitive configuration items. Attacker could be paid for such stealing activities. Concerned assets include Client's Secure Wafers / ICs, finished products, special transport protection like security seal that support the security of the internal shipment to the client.

The risk for this attack could vary depending on the subject and the recognized value of the assets. These attackers could be prepared to take high risks for payment. They are considered to be sufficiently resourced to overcome the security measures. The target of the attack could be devices that can be re-sold or misused in an application context. These attackers are considered to have the highest attack potential.

These attackers could not completely be blocked by the physical, technical and procedural security measures. The site has special restricted location and access to highly secured area where such information are the most sensitive. Signed and Secured Keys are also used to transmit confidential or sensitive files with external parties to provide additional protection against such attacks.

T. Computer-Net

Data theft could happen when the attacker tried to access the network without authorization. The attacker could try to download or intercept confidential documents of the company/ clients' data (such as personalization data) for manipulation. In such cases, data theft through access of the company network or data servers could lead to loss of reputation of the company as well as the leak of confidentiality of clients' knowhow and intellectual property. This could eventually lead to a financial loss, compensation or legal case for the company. Concerned assets include Clients Testing Specifications, test programs and personalization data.

These attackers are considered to have high attack potential because they might have vast technical knowledge to perform such attack whereby the in-house system or software may not have sufficient capabilities to withstand such attacks.

Risk of Logical theft is reduced by the implementation of the security firewall to the external network. Limitations are set on websites, web applications and computer applications which are not essential for company use. Computer users also have individual accounts which require password authentication.

The site also houses dedicated servers and procedures in place handling Pre-personalization data which will enhance the security of the data received from the clients. The production network is also separated from the office network which the production network has no access to the internal network and has no access to internet to reduce the risk of any external attacks from hackers.

Used of SFTP server and SFTP Client system is for transfer of confidential sensitive data between UTAC and customer securely through data encryption. The SFTP Server is hosted in locked rack at secure UTAC Data Centre at UTL1 (With Dual Authentication). On request SFTP user ID and password will be generated and issued to specific customer to allow a secure access for each individual customer.

T. Unauthorised-Staff

Unauthorised entry into prohibited area such as store, warehouse, production area and personalization is restricted. Concerned assets include Clients Secured Wafers and ICs, Client's finished products, special transport protection like security seals that support the security of the internal shipment to the client. The site is segregated into various levels of restricted access and the access is only permitted to authorised personnel.

Only authorized personnel are allowed into the secure area to verify and giving the authority to authorize person needing area's owner and Security Manager for approval.

Subcontractors/ vendors, visitors or non-employee of the site will be subjected to record their particulars and escorted by an employee during the duration of their stay in the site and have restricted access to the site. The site has also internal procedure guiding the access of unauthorised employees entering the site.

T. Staff-Collusion

Threats from external attacker might have collaborated with existing employee to extract data, confidential information or material from the site. Collaboration of such nature could have been motivated by personal interest or extortion. Concerned assets include Clients Secured Wafers and ICs, Client's finished products, Secure IC wafers which are rejected in the manufacturing process or intended for scrap.

While the site conducts yearly security training and security talks for the employees, they have to also sign the confidentiality agreement during their term of employment with the site. Procedures such as limited access and document controlled access on production data and clients' sensitive data are also available at site. Handling of material or product at site using the 4 eyes principal is also implemented to reduce the tendency of such attacks.

T. Accidental-Change

Employee, trainee, freight forwarder could have also make mistakes in executing their tasks and therefore resulting in the wrong mix of the different shipment at collection, mixing the wrong lot or batch of raw materials of products in production or even loading wrong personalization data by mistake. Concerned assets include Clients Secured Wafers and ICs and Client's finished products.

We have measures in place to prevent accidental changes in high risk area prone to accidental change such as incoming shipment identification, outgoing shipment collection, in production process during issuing of materials.

T. Attack-Transport

Potential attackers might be planning to get products or confidential data during shipment of the product. Their aim on the attack is to get sensitive information for unauthorised activities, such as replicating sensitive product devices or data, reselling of security devices or getting sensitive information. Concerned assets include Clients Secured Wafers and ICs, Client's finished products, Secure IC wafers which are rejected in the manufacturing process or intended for scrap, specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. These specific assets are handled the same way as other assets to prevent misuse, disclosure or lost.

Incoming and outgoing shipment of raw material and finished goods/ products to clients are controlled via a restricted channel whereby access is dedicated to only logistics personnel and all transactions of materials are performed between the freight forwarders and logistics personnel are also recorded. Procedure and controls for Freight Forwarders (for incoming and outgoing shipments) are also in place. Collection for the finished goods is also identified with unique numbers whereby it's only made known to the freight forwarder who are collecting the goods.

Internal transportation of TOE is also monitored under the production process security element.

7 Organizational Security Policies (OSPs)

The security policies devised are based on the requirement of the assurance components of ALC for the assurance level EAL 6. The policy in place supports the entire process of the site as described (under section 2.1) and serves as security measures under the Security Assurance requirement (SAR). In addition, scheduled internal security audit and maintenance schedule of security equipment shall ensure the correct and continuous operation of the site's security.

The documentation of the site under evaluation is under configuration management. This comprises all procedures regarding the production flow and the security measures that are in the scope of the evaluation. Guidelines outlining the Security policy of the Site are mapped as follow.

P. Config-Items

The configuration management system shall be able to uniquely identify configuration items. This includes the unique identification of the items that are created, generated, developed or used at the site.

All products and item codes are guided by the site's configuration system which uses unique item code for different client, Bill of material (BOM) and products. The site also uses a Work in Progress (WIP) and Zero balancing system for production and item traceability. Procedure of the client's creation and new product introduction (NPI) are also in place to ensure that the information of the clients, material configuration and process specifications of the product are defined. The documentation (Physical copy) of this clients' assembly build diagram and specifications are controlled documents released only for production. Limited access to these documentations (electronic copy) is also stored in the server, available only to authorised engineering personnel.

Procedures on the creation of the Bill of material guiding the unique item code for all raw materials (including security products) and client's codes. The entire production system is also guided by the SAP system which control information of the entire process from incoming to production and shipment.

The naming and the identification of these configured items are specified during the entire production process.

P. Config-Control

The procedures governing setting up the production process for new product and the procedure that allows changes of the initial setup for a new product shall only be perform by authorised personnel.

The new product setup includes the following information: identification of the product, properties of the product, itemized level (BOM/ raw material) and properties of the product when internal transfers take place, how the product is tested after assembly, address used for the shipment and other configuration of the processed product. All these setups are also managed via the SAP system and governed by procedure on item master part creation.

Configured items will be tied to the client's approval documents before releasing it for mass production. Program name will be defined based on the client's name and configuration name. There are internal procedures and work instructions to ensure the traceability of clients' inventory and is further governed by the SAP system.

P. Config-Process

Services and processes provided by the site are controlled in the configuration management plan. This comprises tools used for assembly of the product like the process control plan will govern how the process is run and what are the tools and assembly equipment used in the production of the module. This clearly explains in detail the manufacturing processes and quality of the modules at the site.

The documentation with the process description and the security measures of the site are under version control. Measures are in place to ensure that the evaluated status complies.

P. Reception-Control

Procedures on receiving of products, outgoing shipments to clients and internal material flow are followed to ensure that security is not compromise. Inspection of incoming materials is also done on site to ensure that the received configuration items comply with the properties stated by the clients.

Traceability of the materials and products are monitored via SAP system. Information of freight forwarders are also recorded to ensure traceability and accountability. All incoming shipments have a dedicated incoming reception channel for the transfers of goods (including security material) to ensure security.

P. Accept-Product

The quality control of the site ensures that the released products comply with the specification agreed with the clients. The quality control plan depicts the process, control and measures in place for the acceptance process of the configuration items. Therefore, the properties of the product are ensured when shipped.

P. Zero-Balance

Site ensures that all sensitive items (on the intended TOE from clients) are separated and traced by devices basis. Procedure on Zero balancing is practiced ensuring that all scrap materials are accounted for at each different manufacturing process. Security products are traced and recorded to ensure traceability. At the end of the production process where functional or defective assets are consolidated, they are ether destroyed or send back to the clients (dependent on the production setup).

The policy on Zero balancing covers the handling of products at each production flow of the site.

All finished products are returned to the clients that has provided the site with the products.

This is considered as internal shipment routing back to the clients.

P. Transport-Prep

Procedures and measures are ensured for the correct labelling of the product. Products are labelled according to the specification determine by the clients and are verified before shipment to the clients. Products are packed per specification indicated by the clients. Controls are in place when the forwarder indicated by the client before the handover of the security products. Traceability of the outgoing materials and security products are monitored. Information of freight forwarders are also recorded to ensure traceability and accountability. All outgoing and internal shipments have a dedicated outgoing shipment channel for the transfers of goods (including configuration products) to ensure security

P. Data-Transfer

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 etc) is also encrypted to ensure security before sending out to clients through email.

P. Secure-Scrap

Storage of the functional or defective Scrap materials are securely maintained with authorised access. Secured scrap products must be destroyed securely with registered vendors or are returned to the clients (according to the production setup).

8 Assumptions

Each site operating in a production flow must reply on preconditions provided by the previous site. Each site has to reply on the information received by the previous site/client. This is reflected by the assumptions defined below for the interface with UTL1.

A. Item-Identification

Each Configuration item received by the site is appropriately labelled to ensure the identification of the configuration item

A. Product-Spec

The product developer must provide appropriate specifications and guidance for the assembly of the product. This comprises bond plans for an appropriate assembly process The provided information includes the classification of the delivered item and data.

A. Internal-Shipment

The recipient (Client) of the product is identified by the address of the client site. The address of the client is part of the product setup. The client defined the requirements for packing of the security products in case the standard procedure of UTL1 is not applicable.

A. Product-Integrity

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

The assumptions are outside the sphere of influence of UTL1. They are needed to provide the basis for an appropriate production process, to assign the product and destruction of all configuration items related to the intended TOE.

9 Security Objectives (AST_OBJ)

The site's security objectives and measures shall conform to the EAL 6. These measures defined the physical, data, organizational security measures, and logistical security of the site.

- 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
- O. Config-Process
- O. Accept-Product
- O. Staff-Engagement
- O. Zero-Balance
- O. Reception-Control
- O. Internal-Shipment
- O. Data-Transfer
- O. Control-Scrap

O. Physical-Access

Different Security access supports the different level of access control level of different authorised staff entering the facility. The area of access of the authorised staff is subjected to the basis of each individual's job scope and enforcing the "need to know" principle. The access control supports the limitation for the access to sensitive area including the identification and rejection of unauthorised entry.

The site enforces up access control depending on the area of access. The access control measures and mapping ensure that only authorised staff and accompanied visitors can access restricted areas. Any visitors who are accompanied must also be authorised to visit the restricted area by a formal security application, approved by authorised personnel. All Security products are handled in restricted areas only.

O. Security-Control

The site has defined the responsibilities of each different personnel responsible for the security of the site. Measures, response and controls on the operation of the system for access control and surveillance are also defined. Technical security equipment such as video control, CCTV, sensors will also support the enforcement of the access control. All staff is responsible for registering the visitors, get authorised approval for entry to each area and should ensure to escort the visitors.

O. Alarm-Response

The technical and organizational security measures ensure that an alarm is generated before an unauthorised person gets access to any sensitive configuration item (asset). After the alarm is triggered, the unauthorised person still has to overcome further security measures. The reaction time of the employee or security personnel is short enough to prevent a successful attack.

O. Internal-Monitor

The site performs security management meeting once every year. The security management meetings are used to review security incidences, to verify that the maintenance measures are applied and to reconsider the assessment of risks and security measures. An internal audit is also conducted yearly to control the application and seek further improvement of the security measures defined.

O. Maintain- Security

Technical security measures are maintained regularly to ensure correct and accurate operations. Access control system to ensure that only authorised employee have access to sensitive area as well as computer/ network system 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. The internal network is also separated into the production network and the administration network. Additional specific networks for production and configuration are physically separated from any internal network to enforce access control. Access to the production network and internal network is also restricted to authorised employees that are working in the related area or that are involved in the configuration tasks or the production system. Every authorised user of an IT system has its own user account and password managed by the authorised IT administrator. An authentication user account and password is enforced by all computer systems.

O. Logical-Operations

The network segments and computer systems are kept up to date software updates, security patches, virus protection, and spyware protection). The backup of sensitive data and security relevant logs is applied accordingly 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 and is assigned to each different client.

O. Config-Control

The site has a procedure for the setup of the production process for each new product- From the release of a new configuration of the product to the production of the product. The site has also integrated a process of change management whereby process to introduce changes to the product or processes is enforced. Only authorised personnel can access the changes in the system. The configuration management system which is automated supports the entire production control.

O. Config-Process

The site controls its services and processes using a configuration management plan. The configuration management is controlled by tools and procedures for the assembly of the products, for the management of optimizing the documentation and process flow managed by the site.

O. Accept-Product

The site delivers configuration items that fulfil the specified properties. Specification checks, Machine Parameters, Functional and visual control checks are performed to ensure that the products are compliant to the specifications defined. Activity logs are stored and maintained in the database to support the tracing and identification in case of any systematic failures.

O. Staff-Engagement

All employees have to sign a non-disclosure agreement upon their employment with the site. Authorised staffs who are engaged to move, transfer and have contact with the security configuration items have to be trained and qualified based on the security procedures, on handling of the products. Briefing session with employees on basic security procedures of the company is done for every new employee joining the site and yearly sessions are also conducted to facilitate and enforce the importance of security within the site.

O. Zero-Balance

Tracing of the security product is essential, and the site has to ensure that each device of the client are tracked separately and are accounted for each functional and defective device at every production step. Devices are tracked until when they are shipped or destructed as determined by clients.

O. Reception-Control

Upon receipt of products an 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- Shipment

The internal shipment procedure is applied to the configuration item. The recipient of a physical configuration item is identified by the assigned clients address. The internal shipment procedure is applied to the configuration site. The packaging is part of the defined process and applied as agreed with the client. The forwarder supports the tracing of configuration items during the internal shipment.

O. Data-Transfer

Sensitive electronic configuration items (data or documents in electronic form) are protected with cryptographic algorithms (PGP Keys) to ensure confidentiality and integrity. The associated keys must be assigned to individuals to ensure that only authorised employees are able to extract the sensitive electronic configuration item. The keys are exchanged based on secured measures and they are sufficiently protected.

O. Control-Scrap

The site has measures to destruct sensitive configuration items. Rejected or defective devices are either destructed by authorised vendors or are returned to the clients.

10 Security Objective Rationale

The Site Security Target includes a Security Objectives Rationale with two parts. The first part includes a tracing which shows how the threat 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.

Notice that the Assumptions defined in this site security target (see section 8) 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.

Table 10a : Mapping of Security Objectives

Threats and OSP	Security Objectives	Rationale
T. Smart Theft	O. Physical- Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security	The combination of structural technical and organizational measures detects unauthorized access and allow for appropriate response on the 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.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	The combination of structural, technical and organizational measures detects unauthorized access and allows for appropriate response on the threat. O.Physical-Access ensures that the 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.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. Maintain-Security O. Logical-Access O. Logical-Operations O. Staff-Engagement	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.

Threats and OSP	Security Objectives	Rationale
		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.Maintain-Security ensures that the above is managed and maintained. Together, these objectives will therefore counter T. Computer-Net.
T. Accident-Change	O. Logical-Access O. Config-Control O. Config-Process O. Accept-Product O. Staff-Engagement O. Zero-Balance	Automated measures and control procedures allow preventing accidental changes on sensitive items. O.Logical-Access ensures that the networks are protected with Firewall to prevent external or internal unauthorized access and that machines are measures (such as Login and password) to restrict access to. 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.Accept-Product to ensure that the products to be returned to the clients are compliant with their specifications. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all items are traced and accounted for. Together, these objectives will therefore counter T. Accident-Change
T. Unauthorised Staff	O. Physical-Access O. Security-Control O. Alarm-Response O. Internal-Monitor O. Maintain-Security O. Logical-Access O. Staff-Engagement O. Zero-Balance O. Control-Scrap O. Logical-Operation O. Config-Control	Physical and Logical access control prohibits access to assets. Secure destruction of scrap limits the amount of assets. 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.

Threats and OSP	Security Objectives	Rationale
		O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party. 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.Config-Control ensures that sites procedures for manufacturing are known and followed for the manufacturing operation. 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. Staff Collusion	O. Internal-Monitor O. Maintain-Security O. Staff-Engagement O. Zero-Balance O. Control-Scrap O. Data-Transfer	The Application of internal security measures combined with the hiring policies that restrict to trustworthy employees limits unauthorized access to assets. O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party. O. Data-Transfer ensures the integrity of the secure delivery of data. O.Internal-Monitor and O.Maintain-Security ensure that the above is managed and maintained. Together, these objectives will therefore counter T. Staff Collusion
T. Attack-Transport	O. Internal-Shipment O. Data-Transfer	The shipment method and the organizational measures ensure that integrity change and shipped objects are detected and appropriately responded upon. O.Internal-Shipment ensures the traceability and security of products during shipment. O. Data-Transfer ensures the integrity of the secure delivery of data. Together, these objectives will therefore counter T. Attack-Transport.
P. Config-Items	O. Reception-Control O. Config-Items	The Security Objective directly enforces the OSP. O.Reception-Control ensure an immediate identification of the product upon reception and confirm the received quantity O.Config-Item ensures that all configuration items for secure products are identified. Together, these objectives will therefore counter P. Config-Items

Threats and OSP	Security Objectives	Rationale
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-Item 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.
P. Config Process	O. Config-Process	The Security Objective directly enforces the OSP.
P. Reception-Control	O. Reception-Control	The Security Objective directly enforces the OSP.
P. Accept-Product	O. Config-Control O. Config-Process O. Accept-Product	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.Accept-Product to ensure that the products to be returned to the clients are compliant with their specifications. Together, these objectives will therefore counter P. Accept-Product.
P. Zero-Balance	O. Staff-Engagement O. Zero-Balance O. Control-Scrap O. Internal-Monitor	All assets are traced internally until their possible destruction (O. Zero-Balance, O. Control-Scrap) by trained and authorized people (O. Staff-Engagement) to enforce the OSP O.Staff-Engagement ensures that all staff is aware of its responsibilities (signing NDAs, and being trained). O.Zero-Balance ensures that all items are traced and accounted for. O.Control-Scrap ensures that scrap material cannot be accessed by an authorized party. O.Internal-Monitor ensures that the above is managed and maintained. Together, these objectives will therefore counter P. Zero-Balance

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

11 Extended Assurance Components Definition (AST_ECD)

No extended components are currently defined in this Site Security Target.

12 Security Assurance Requirement (AST_REQ)

Clients using this site Security Target require an evaluation against evaluation assurance level EAL 6. In many cases, this evaluation assurance level is appropriate with the Security Assurance Requirement ALC_DVS.2. This Security Assurance Requirement (SAR) is often requested in the Security IC Platform Protection Profile.

The Security Assurance Requirements (SAR) are from the class ALC (LIFE-CYCLE SUPPORT) as defined:

- CM Capabilities (ALC_CMC.5)
- CM SCOPE (ALC_CMS.5)
- Development Security (ALC_DVS.2)
- Life-Cycle Definition (ALC_LCD.1)

The Security Assurance Requirements listed above fulfil the requirements of [7] because hierarchically higher components than the defined minimum site requirement: ALC_CMC.3, ALC_CMS.3, ALC_DVS.1, which are used in the SST.

12.1 Application Notes and Refinements

The description of the site certification process 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 terms "TOE" is not applicable in the SST the associated process for the handling of products (or "intended TOEs") are in the focus and described in this Site Security Target. These processes are subject of the evaluation of the site.

12.1.1 Overview and Refinements regarding CM Capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production lot. The number of wafers, dice and/ or packaged products (e.g. modules) is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dice and/ or packaged modules, which are being removed from the production-process in order to verify and to control pre-defined quality standards and production parameters. It is ensured, the wafers, dice or assembled devices removed from the production stage (i) are returned to the production stage from where they were removed or (ii) are securely stored and destroyed.

According to 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 are defined for ALC_CMC.5. Since this Site Security Target claims ALC_CMC.5 only relevant content elements are adapted.

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 the site security measures.

The life cycle described is a complex production process which sufficient verification steps to ensure the specified and expected results are used during the control of the product. Assembly procedures, verification procedures and associated expected results must be under configuration management.

The configuration items for the considered product type are listed in section 5. 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.

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

12.1.2 Overview and refinement regarding CM Scope (ALC_CMS)

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 handles at the site.

In the particular case of a security ICs, the scope of the configuration management can include a number of configuration items. The configuration items already defined in section 5 that are considered as TOE implementation representation" include:

- Security Wafers, ICs/ dies.
- Security Modules (Finished Products) and other forms of module packages.
- Security Dice and modules which are rejected in the manufacturing process or intended for scrap.

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

12.1.3 Overview and refinements regarding Delivery Procedures (ALC_DEL)

The CC assurance components of the family ALC_DEL (Delivery) refer to the external delivery of (i) the TOE for parts of it (ii) to the consumer or consumer's site (Composite TOE Manufacturer), The CC assurance components ALC_DEL.1 requires procedures and technical measures to maintain the confidentiality and integrity of the product. The means to detect modifications and prevent any compromise of the initialization Data and/ or Configuration Data may include supplements of the Security IC Embedded Software.

In the particular case of a security IC more "material and information" then the TOE itself (which by definition includes the necessary guidance) is exchanged with clients. Since the TOE can be externally delivered after different life cycle phases, the Site Security Target must consider the data that is exchanged by the sites either as part of the product or separate as input for further production steps.

Since the assurance component ALC_DEL.1 is only applicable to the external delivery to the consumer, the Internal shipment is covered by ALC_DVS.

12.1.4 Overview and refinements regarding Development Security (ALC_DVS)

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

The TOE Manufacturer must ensure that the development and production of the TOE is secure so that no information is unintentionally made available for the operational phase of the TOE. The confidentiality and integrity of design information, configuration data must be guaranteed, access to any kind of samples (Clients specific samples) development tools and other material must be restricted to authorised persons only, scrap must be controlled and destroyed.

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

12.1.5 Overview and refinements regarding life Cycle Definition (ALC_LCD)

The site does 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 Protection Profile (BSI-PP-0084) [provides a life-cycle description there specify life-cycle steps can be assigned to the tasks at site. This may comprise a change of life-cycle state if e.g. initialization is performed at the site or not.

The Protection Profile (BSI-PP-0084) 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 are assembled and the functional devices are returned to the clients. The defective devices are scrapped or also returned to the client.

12.1.6 Overview and Refinements regarding Tool and Techniques (ALC_TAT)

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

Neither source code of the intended TOE is handled nor is any task performed at the site that must be considered accordingly to ALC_TAT.

13 Security Rationale (SAR)

The Security Assurance rationale maps the content elements of the selected assurance components to the security objectives defined in this Site Security Target. The refinements described above are considered.

The site has a process in place to ensure an appropriate and consistent identification of the products. If the site already receives configuration items, the process is based on the assumption that the received configuration items are appropriately labelled and identified.

The dependencies for the assurance requirements are as follow

a. ALC_CMC.5 : ALC_CMS.1, ALC_DVS.2, ALC_LCD.1
b. ALC_CMS.5 : None
c. ALC_DVS.2 : None
d. ALC_LCD.1 : None

One dependency is not (completely) fulfilled:

- ALC_LCD.1 is only partially fulfilled as the site does not represent the entire development environment. This is in-line with and further explained in [7] 5.1 'Application Notes for ALC_CMC'

Table 13a: Rationale for ALC_CMC.5 [Mapping]

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	Wafers are labeled by a unique part ID. Automatic tools are used to set-up the wafers in a new production item. The products get a unique client part ID automatically generated by the system tools based 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 to O. Reception-Control ensures product identification and the associated labeling. This labeling is mapped to the internal identification as defined by O. Config-Items. This ensures the unique identification of security products. O. Config-Control ensures that each client part ID is setup and released based on a defined process. This comprises also changes related to a client part ID.The configurations can only be done by 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 review of changes to all configuration items.	O. Config-items O. Config-control	O. Config-Items comprise the internal unique identification of all items that belong to a client part ID. Each product is setup according to O. Config-Control comprising all necessary items.
ALC_CMC.5.4C: 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 comprise the internal unique identification of all items that belong to a client part ID. Each product is setup according to O. Config-Control comprising all necessary items.
ALC_CMC.5.5C: 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. Config-Control assigns the setup including processes and items for the production of each client part ID. O. Config-Process comprises the control of the production processes. O. Logical-Access 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. Config-Control O. Zero-Balance O. Accept-Product	O. Config-Process comprises the automated management of the production processes. O. Config-Control assigns the setup including processes and items for the production of each client part ID.

SAR	Security Objective	Rationale
		O. Zero-Balance ensures the accountability of all security products during production. O. Accept-Product provides an automated mechanical testing of the product quality and supports the tracing.
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 different roles are assigned to difference teams. The members of each team are response to released differences step of the production and final good (Secure rejects) are differences. 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.
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 that belong to a client's part ID. O.Config-Control describes the management of the clients 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. Accept-Product O. Config-Control O. Config-Process	O.Config-Items comprise the internal unique identification of all items that belong to a client part ID. O.Config-Control describes the management of the client part IDs at the site the production 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.Accept-Product provides an automated mechanical 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 client 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. Reception-Control O. Logical-Access O. Config-Control O. Config-Process	O.Reception-Control comprises the incoming labelling and the mapping to internal identifications.

SAR	Security Objective	Rationale
	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 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-Control O. Config-Process	O.Config-Control describes the management of the client part IDs at the site. According to O.Config- Process the CM plans describe the services provided by the site.
ALC_CMC.5.13C: 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 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-Control O. Config-Process	O.Reception-Control supports the identification of configuration items at UTL. O.Config-Items ensure the unique identification of each product produces at UTL 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.

SAR	Security Objective	Rationale
ALC_CMC.5.15C: The evidence shall demonstrate that all configuration items are being maintained under the CM system.	O. Reception-Control O. Config-Control O. Config-Process O. Zero-Balance O. Internal-Shipment	The objectives: O. Reception-Control, O. Config-Control, O. Config-Process ensure that only released client part IDs are produced. This is supported by O. Zero-Balance ensuring the tracing of all security products. O. Internal-Shipment includes the packing requirements, the reports, logs and notifications including the required evidence.
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 13b: Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
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 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 ID's 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-Shipment	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 labelling and preparation for the transport is defined by O. Internal- Shipment.
ALC_CMS.5.3C: For each configuration item, the configuration list shall indicate the developer of the item.	O. Config-Items	UTL does not involve subcontractors for the production of IC product. According to O. Config-Items all configuration items for secure products are identified.

Table 13c: Rationale for ALC_DVS.2

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 TOE design and implementation in its development environment.	O. Physical-Access O. Security-Control O. Alarm-Response O. Logical-Access O. Logical-Operation O. Staff-Engagement O. Data-Transfer O. Control-Scrap	The physical protection is provided by: O. Physical-Access, supported by O. Security-Control, O. Alarm- Response. The logical protection of data and the configuration management is provided by O. Logical-Access and O. Logical- Operation. The personnel security measures are provided by O. Staff- Engagement. Any scrap that may support an attacker is controlled according to O. Control-Scrap.
ALC_DVS.2.2C: The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.	O. Internal-Monitor O. Logical-Operation O. Maintain-Security O. Zero-Balance O. Accept-Product O. Data-Transfer	The associated control and continuous justification is subject of the objectives O. Internal-Monitor, O. Logical- Operation and O. Maintain-Security. All devices including functional and non - functional are traced according to O. Zero-Balance. O. Accept-Product supports the integrity control by mechanical testing of the finished products.
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. Zero-Balance O. Accept-Product O. Data-Transfer	The associated control and continuous justification is subject of the objectives O. Internal-Monitor, O. Logical- Operation and O. Maintain-Security. All devices including functional and non - functional are traced according to O. Zero-Balance. O. Accept-Product supports the integrity control by mechanical testing of the finished products.

Table 13d: Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
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. Accept-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. The finished client parts are tested according O. Accept-Product. All security products are traced according O. Zero-Balance.

Since this SST references the PP [9], the life-cycle module used in this PP includes also the processes provided by this site. Therefore, the life-cycle module described in the PP [9] is considered to be applicable for this site.

The performed production steps do not involve source code, design tools, compilers or other tools used to build the security product (intended TOE). Therefore, the site does not use or maintain tools according to the definition of ALC_TAT.3. However, the component is included here to support the reuse of the evaluation results and to enable the justification of the evaluators regarding ALC_TAT.3. The site always returns the security products back to the client that provided the security products for the assembly. There is no delivery of security products directly to the client regarding the next life cycle step. Therefore, the transport of security products is always considered as internal transport.

14 Site Summary Specification (AST_SSS)

14.1 Preconditions Required by the Site

UTL provides manufacturing and assembly services for smartcards and identity modules. Sawn wafers are expected as input for the assembly lines. Defect devices on the wafer can be marked by inking or by electronic wafer map files. The packaging and the wafers must be labelled to allow for production product identification. The production at UTL is released after the client accepts the initial samples lot produced. Therefore, each client is responsible for the verification of his products based on the samples lot provided by the site. If specific requirement is needed for the transport of the finished products, the related specifications and other packaging items e.g. security seals are provided by the client. The client is responsible for delivery and transfer of the products. This comprises the selection of the forwarder and the provision of data for the verification of the transport arrangements.

The site maintains a Security Management System that covers the SAR ALC_CMS.5 and contributes also to cover the SAR ALC_CMC.5. The site also maintains the security to protect the assets they are in charge that covers the SAR ALC_DVS.2.

The site is not equal to the entire development environment. Therefore, the SAR ALC_LCD.1 is interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site.

Security related products such as modules (packaged Security ICs) come with clearly defined and fitting interfaces for the production at UTAC, these products are uniquely identifiable

The information required for the assembly of the ICs such as specification, assembly guidance, and production requirements.

Shipping process, including the shipping address and the packing requirements for the shipment, needs to be specified by the client. This also includes the procedure for selecting the forwarder.

UTAC can provide the optional service of module packaging in case the client delivers the security ICs and wafers.

The information required for the assembly and packaging of module such as:

a. The wafer map files with electronic defect marking,

b. The bond plans and assembly requirement (if they are different from the testing requirements for that chip).

Note : that the site can also handle wafer where the defect dice are marked with ink dots.

14.2 Services of the Site

Each product setup at the site gets a unique client part ID (Client consigned parts). This part ID is linked with the secure device that is assembled in the product.

The processes for assembly and product acceptance are setup at the site according to the specifications (E.g. Bonding diagrams, modules specification and packaging requirements, if applicable) provided by the client. For the release, a samples lot is produced at the site.

The site has a standard procedure for packing of finished products and preparation of shipment. If special packaging requirements are provided by the client, they are included in the process setup. The client is alerted if products are ready for transport because the transport will be arranged by the client. Base on the alert, the client provides the pickup information on the forwarder that is used for the verification of the forwarder before the handover of the products.

Defective or rejected products are either returned to the client or destructed according to the defined secure destruction process. The client must decide during the product setup whether the reject devices and defective dies on the wafer have to be returned or must be destroyed by UTL.

The UTL IC Manufacturing services can be detailed as follow:

a Receiving Material
- Receipt the information of incoming shipment from Importer Staff, Clients custom, Material providers.
- Receive the cargo shipment by consider address which was mentioned declare on document (Commercial Invoice, Customs Entry Form, HAWB and/or B/L and PO)

b Die Bank room
- Die Wafer storage and Contribution

c Production Control
- Management the security lots
- Define Manufacturing flow and guideline for process traveller.
- To management the loading schedule to planed meet on target with on time delivery performance.

d Pre-Assembly
- Preparing die and wafer before sending to Assembly process.

e Assembly
- Generate the Secure Standard Procedure of product to production line

f Product Engineer / Test Engineering
- Product development and after sales technical support who handle test program development,
- Sustaining and support activates for the security products.

14.3 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 plant 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. This considers the manpower per shift as well as the operational needs regarding the receipt and delivery of goods. The physical, technical and organizational security measures ensure a separation of the site into four security levels. The access control ensures that only registered and authorised 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.

The site implements a "need to know" principle by separation measures using a combination of physical partitioning together with technical and organizational security measure. The access control measure supports the enforcement of the separation and the "need to know" principle. The handling of assets is restricted to separates security areas. By the combination of these measures the threat. T. Smart – Theft, T. Rugged – Theft and T. Unauthorised – staff can be prevented.

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. Unauthorised-Staff and P. Config-Control are 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.

The site using dedicated personnel for guard services. These personnel is responsible for operation of the access control systems, for the enforcement of the access control, for the surveillance of the technical alarm sensors and the responses to incident and for the escort of visitors.

This addresses the threats T. Smart-Theft and 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. Unauthorised-Staff and the OSP O. Secure-Scrap are addressed.

O. Alarm-Response

During working hours the security officer will monitor the alarm system. The alarm system is connected to a control centre 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. Unauthorised-Staff. In case of an access attempt to an asset by an unauthorised person site has an alarm system in place. After the alarm is triggered the unauthorised person still has to overcome further security measure.

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). Upon introduction of a new process, a formal review and release for mass production is made before being generally introduced.

The established security measures of the site are regularly reviewed by security management meeting and internal audits.

This help to prevent the threats: T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff, T.Staff-Collusion 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 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 the threats 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.

An appropriate separate between the different working environment (office of developer and production with secure area) including the access control ensure access to only authorised people.
The network separation, the development network of the site is located in a dedicated secure area. This network is connected only to dedicated trustworthy systems.

The individual accounts are addressing T. Computer-Net. All configurations are stored in the database of the ERP system. Supported by O. Config-Items this addresses the threats T. Accident-Change and T. Unauthorised-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 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. Unauthorised-Staff. O. Config-Control Procedures arrange for a formal release of specifications based in 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 and major changes and the relevant interactions and releases with clients if required. The ERP requires personalized access controlled by passwords. Each user has access rights limited to the needs of his function. Thereby only authorised changes are possible.

O. Config-Items

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

This is addressing the OSP P.Config-Items, P.Config- Control.

O. Config-Process

The release configuration information including production and acceptance specifications is automatically copied to every work order.

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

O. Config –Control

Procedure arrange for a formal release of configuration documents, Specification and test program for the setup and test and/or assembly process flow. The information is also stored in the configuration database. The Engineering Change Notice [ECN] and Process Change Notice [PCN] both procedures are in place to classify and introduces the changes. The Procedure also defines the separated between minor and major changes and the relevant interactions and releases with clients if required. Each user has access rights limited to the need of this functions, thus , only authorized change are possible

This is addressing the threats T.Unauthorised-Staff, T.Accident-Change and the OSP P.Config-Control, P.Accept-Product.

O. Accept-Product

Acceptance mechanical tests are introduced and released based on the client approval. The tools, specifications and procedures for these tests are controlled by the means of O. Config-Items and O. Config-Control. Acceptance mechanical test results are logged and linked to a work order in the ERP system.

This addresses the threat T. Accident-Change and the OSP P. Accept-Product.

O. Staff-Engagement

All employees are interviewed before hiring. They must sign and NDA and a code of conduct for the use of computers before they start to work in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of security products. The security objectives O. Physical-Access, O. Logical-Access and O. Config-Items support the engagement of the staff.

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

O. Zero-Balance

Products are uniquely identified throughout the whole process. The amount of functional and non-functional dies on a wafer and for a production order is known. Scrap and rejects are following the good products thru the whole production process. At every process step the registration of good and rejected products is recorded and updated. This security objective is supported by O. Physical-Access, O. Config-Items and O. Staff-Engagement.

This security objective is supported by O.Physical-Access, O.Config-Control and O.Staff-Engagement.
This addresses the threats T.Accident-Change, T.Unauthorised-Staff, T.Staff-Collusion and the OSP P.Zero-Balance, P.Secure-Scrap.

O. Reception-Control

At reception, each configuration item including security products are identified by the shipping documents, packaging label and information in the ERP system based on shipments alerts from the client and supported by O. Config-Items. If a product cannot be identified, it is put on hold in a secured storage. Inspection at reception is counting the number of boxes and checking the integrity of security seal 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-Shipment

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

The threat T.Attack-Transport and the OSP P.Transport-Prep are addressed.

O. Data-Transfer

Sensitive electronic information is stored and transferred encrypted using PGP procedures. Supported by O. Logical-Access and O. Staff-Engagement

This addresses the threats T. Staff-Collusion and T. Attack-Transport a well as the OSP P. Transport-Prep and P. Data-Transfer.

O. Control-Scrap

Scrap is identified and handled in the same way as functional devices. They are stored internally in a secured location. The scrap is either returned to the client using the same packaging requirements as for functional products or its destructed in a controlled and documented way. 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 s supervised and documented process.

Supported by O. Physical-Access and O. Staff-Engagement, this addresses the threats T. Unauthorised-Staff and T. Staff-Collusion and the OSP P. Zero-Balance and P. Secure-Scrap.

14.4 Security Assurance Requirements Rationale

The Security Assurance Rationale is given in section 12. This rationale addresses all content elements and thereby also implicitly all the developer action elements defined in [3]. Therefore, the following Security Assurance rationale provides the justification for the selected Security Assurance Requirements. In general, the selected Security Assurance Requirements fulfil the needs derived from the Protection Profile [9]. Because they are compliant with the Evaluation Assurance Level EAL6 derived dependencies are fulfilled or justified when not wholly covered.

ALC_CMC.5

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 authorised changes support the integrity and confidentiality required for the products. 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 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 production, assembly of the product can be used by potential attackers. Therefore, the handling and storage 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 and production.

ALC_LCD.1

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 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_DEL.1

The assurance family "Delivery" is not applicable because the products are returned to the client and this is considered as an internal delivery.

ALC_TAT.3

The assurance family "Tools and Techniques" is not applicable because the tools used for the production process do not influence the behaviour of the product. Therefore, they are not considered under ALC_TAT.

14.5 Assurance Measure Rationale

O. Physical-Access

UTAC (UTL) is surrounded by a fence and controlled with motioned by CCTV. The Access to sensitive areas is granted by full height turnstiles. The enabling of the alarm system and the additional external control are managed according to the running operation at the site. This considers the manpower per shift as well as the operational need regarding the receipt and delivery of goods.

The physical, technical and organization security measures ensure a separation of the site into third layers. The access control ensures that only registered and authorised persons can accesses sensitive areas.

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

During working hours, the Security Officer will monitor the site and surveillance system during hole working day, non - daily working day. The alarm system is used to monitor the site.

The CCTV System is daily monitor with playback retrieved verify. Access System, Intrusion and Burglar System are monitored and verified by security manger periodically.

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

During working hours, the Security Officer monitors the alarm system which combines from various security features such as: CCTV system, Access system, Intrusion System, Burglar System. They are connected to a control centre that is running 24/7.

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

Regular security management meetings are implementing to analyse 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 reviews in general management security review meeting. (min 1 per year) Upon introduction of a new process, a formal review and release for mass production is made before being generally introduced. The required security methods and measures are implemented and maintained. Effectiveness of all measure is verified regularly through internal audits which are conducted at lead once a year. Therese audits, security meetings and reviews of results and changes are suitable to check the impended security measures.

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 requires that evidence justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

O. Maintain-Security

The security relevant systems enforcing of supporting O. Physical – Access, O. Security Control and O. Logical Access are checked regularly by Security Officer, in case of maintenance this is done by Security Technical with Supplier. In addition, the configuration is updated as required by authorised Security Specialist (for the access control system). Log files are also checked for technical problems and specific maintenance request.

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 requires that evidence justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

O. Logical-Access

The internal network is separated from internet by a firewall. The internal network is further separated into sub-networks by internal firewalls. These firewalls allow only authorised information exchange between the internal sub-networks. Each user is logged into the system with his personalized user ID. Access to the corresponding networks is restricted to authorised users working on the related area. The objective is supported by the checks of the logging regarding security relevant event.

ALC_CMC.5.4C: Requires that the CM system provides automated measures so that only authorised 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 responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.11C requires that he CM system be able to identify the version of the implementation representation from which the TOE is generated.

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.

O. Logical-Operation

All logical protection measures are maintained and updated as required, as least once a month. Critical items such as virus scanner / back-up data are update daily. This is sufficiently protected and is only accessible for the administration.

ALC_CMC.5.7C requires that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.11C requires that the CM system be able to identify the version of the implementation representation from which the TOE is generated.

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_DV.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_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.

O. Config-Items

ALC_CMC.5.1C requires a documented process ensuring an appropriate and consistent labelling of the products. A method used to uniquely identify the configuration items is required by ALC_CMC.5.2C. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. In addition, ALC_CMC.5.4C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.8C requires that the CM system identifies the configuration items that comprise the TSF. 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_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 fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that the developer of each TSF relevant configuration item is indicated in the configuration list.

The objective meets the set of Security Assurance Requirements.

O. Config-Control

Procedures arrange for a formal release of configuration documents, specifications and test programs for the setup of the test and / or assembly process flow. The information is also stored in the configuration database. The Engineer Change Notice (ECN) and Process Change Notice (PCN) procedures are in place to classify and introduce changes. The procedures also define the separation between minor and major changes and the relevant interactions and releases with clients if required. Each user has access rights limited to the need of these functions, thus, only authorised changes are possible.

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorised changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the TOE by automated means. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. 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_CMC.5.10C requires the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system be able to identify the version of the implementation representation from which the TOE is generated. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the TOE. ALC_CMC.5.15C requests evidence demonstrating 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 fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

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

The objective meats the set of Security Assurance Requirements

O. Config-Process

The release configuration information including production and acceptance specification is automatically linked to every work order. The test program is automatically loaded to the tester through barcode scanning of the secure lot process traveller (PT) according to the configuration information of the work order.

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 authorised changes is made to the configuration items as required by ALC_CMC.5.5C. ALC_CMC.5.6C requires that the CM system supports the production by automated means. ALC_CMC.5.8C requires that the CM system shall identify the configuration items that comprise the TSF. 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_CMC.5.10C requires the CM system provides an automated means to identify all other configuration items that are affected by the change of a given configuration item. ALC_CMC.5.11C requires that the CM system be able to identify the version of the implementation representation from which the TOE is 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 TOE. ALC_CMC.5.15C requests evidence showing 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 fulfilment of the SARs, development tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

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

The objective meets the set of Security Assurance Requirements.

O. Accept-Product

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

All employees are interviewed before hiring. They must sign on NDA by personal and the Code of Conduct for the user of computers before they started working in the company. The formal training and qualification includes security relevant subjects and the principles of handling and storage of the security product under "S" sticker on badge and on MES (CTIS) via certify program.

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 fulfils this combination of Security Assurance Requirements is able to meet the security objective.

O. Zero-Balance

The amount of functional and non-functional dies on a wafer and for a production order is known: Scrap and reject (dies on wafer / single units) At every process steps the registration of Good / Reject products is record and upload into MES.

ALC_CMC.5.6C requires that the CM system supports the production of the TOE by automated means. ALC_CMC.5.15C requires evidence demonstrating that all configuration items 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_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 this objective is suitable to meet the Security Assurance Requirement.

O. Reception-Control

ALC_CMC.5.2C requires a CM documentation process ensuring an appropriate and consistent labelling of the product. And describes the method used to uniquely identify the configuration items. ALC_CMC.5.4C: requires a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires that the person responsible for accepting a configuration item into CM is not the person who developed it. ALC_CMC.5.11C requires that the CM system be able to identify the version of the implementation representation from which the TOE is generated. 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_CMS.5.2C: addresses the same requirement as ALC_CMC.5.4C.

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

O. Internal-Shipment

The recipient of a production lot is linked to the work order in the MES (Active L) system and can only be modified by authorised users. Packing procedure are documented in the product configuration. This includes specific requirement of the client.

ALC_CMC.5.15C requests evidence showing that all configuration items are being maintained under the CM system. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C.

There by this objective is suitable to meeting the Security Assurance Requirement.

O. Data-Transfer

The confidential data transfer from / to the site occurs only in encrypted format (using PGP). The cryptography keys are stored in a protected server. SFTP server and client is also use for confidential data transfer and SFTP transfer path is encrypted. The server is located inside the IT secure room in the strong building in the company.

ALC_DVS.2.1C : The requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidential and integrity of the intended TOE design and implementation in its production environment including initialization and software upload and prevent misuse of non-conform security ICs. Thereby this objective is suitable to meet the Security Assurance Requirement. ALC_DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the TOE. ALC_DVS.3 requires that evidence justifies that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

There by this objective is suitable to meeting the Security Assurance Requirement.

O. Control-Scrap

ALC_DVS.2.1C : The requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidential and integrity of the intended TOE design and implementation in its production environment including initialization and software upload and prevent misuse of non-conform security ICs. Thereby this objective is suitable to meet the Security Assurance Requirement.

Scrap is identified and handled in the same way as functional devices. Scrap is stored internally in the secure location and destructed in a supervisor and document process (at least DIN 66399, security class 3), or returned to the client.

15 Definition & List of Abbreviations

15.1 Definition

Client: The site providing the Site Security Target may operate as a subcontractor of the TOE developer / 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 "customer" and "consumer" are only used in the sense of CC.

Client wafer map: The wafer map defined and coming from the client.

Wafer map: The electrical map data generated by the tester after chip probed.

15.2 List of Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
IC	Integrated Circuit
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
MES	Manufacturing Execution System
NPI	New Product Introduction
NPQ	New Product Qualification
PP	Protection Profile
SAP	Name of Software used for Enterprise Resource Planning
SAR	Security Assurance Requirement
SST	Site Security Target
ST	Security Target
TOE	Target of Evaluation