Site Security Target Lite

Henghui Production Centre Zibo

Author	Reviewer	Approver
Ting WANG	Shengwu YU	Lin ZHU

Version Control

Version	Date	Description
0.1	28/01/2022	Initial version
0.2	28/11/2023	Updated according to SST

PUBLIC

Contents

PUBLIC

1 Document Information

1.1 Reference

Title: Site Security Target Lite Henghui Production Centre Zibo

Version: 0.2

Date: 28/11/2023

Company: HENGHUI Technology Corporation Limited

Name of the site: Henghui Production Centre Zibo

Product Type: Security IC

Assurance Requirements: ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, ALC_FLR.1

PUBLIC

2 站点安全目标介绍 SST Introduction

This Site Security Target refers to the following site:

Henghui Production Centre Zibo

This site performs security chips packaging activities.

本站点安全目标是指以下站点：

淄博恒汇生产中心。

该站点用于安全芯片封装生产。

2.1 现场标识 Identification of the Site

The site name is Henghui Production Centre Zibo (hereinafter referred to as “HPCZ”), which is located at:

No.187 Zhong Run Avenue,

Zibo High-new Technology Development Zone,

Zibo, Shandong, 255088, People’s Republic of China

站点名称为新恒汇电子股份有限公司（以下简称“HPCZ”），坐落于中国山东淄博高新区中润大道 187 号。

This location is a campus, which belongs to HENGHUI Technology Corporation Limited . (hereinafter referred as “HET”). This campus consists of several plants and buildings as below.

上述位置为站点所在的园区，该园区属于“新恒汇电子股份有限公司”（之后简称为 HET）。这个园区由下面的车间和建筑组成。

- **Plant #1:** This building is a production plant which provides the tape to Plant#4 for the assembly.

  1 号车间用于提供 4 号车间封装使用的载带。

- **Plant #2:** This building is a production plant which conducts the wafer back grinding, sawing, testing and eSIM packaging.

  2 号车间作为生产厂房，进行硅圆背部打磨、减划、eSIM 的封装和测试。

- **Plant #4:** This building is the production plant which provides assembly and test services for secure IC modules products such as smart card and similar devices. The warehouse of plant #4 is used for the storage of materials and finished products. It contains the packaging area and delivery/loading area that is used to receive, pack and deliver goods.

4 号车间作为生产厂房，提供例如智能卡和类似设备等安全芯片模块产品的封装和测试服务。4 号车间仓库用于存放材料和成品，包括用于收货、包装、发货的收发货区域以及包装区域。

- **Plant #5**: This building is a production plant which provides the lead frame to Plant#2 for the assembly.

  5 号车间用于提供 2 号车间封装使用的金属引线框架。

- **Warehouse Plant**: This building is used for the general stuff storage.

  仓库用于通用物件的储存。

- **Plant Server Building**: This building contains the electricity and water engineer room and the main network & server room. This main network & server room is located at the 2nd floor of the plant server building.

  车间配套机房建筑物包括水电气机房以及总机房。总机房位于车间配套机房的 2 楼。

- **Office Building**: This building is used for handling the daily office management affairs, such as the HR and financial stuff.

  办公楼建筑物用于处理日常办公管理事务，如人事以及财务事务等。

- **Canteen Building:** This building is constructed for the employee to have the meals.

  餐厅建筑用于员工就餐。

- **Dormitory Building:** This building is constructed for the employee to sleep and have a rest.

  宿舍建筑物用于员工休息和睡觉。

The scope of evaluation for the HPCZ site includes the following physical areas:

- Plant #2 workshop (Building 2): wafer back grinding, sawing, eSIM packaging and testing.
- Plant #4 workshop (Building 4): IC packaging for the product of smart card and similar devices.
- Plant #4 warehouse (Building 4): Reception, identification, registration and storage of materials. Warehousing and shipment of finished modules.
- Main network & server room (Plant server building): located at the 2nd floor of Plant Server Building.

HPCZ 站点的评估范围包括以下物理区域：

- 2#分厂车间：硅圆背部打磨、减划、eSIM 的封装和测试。
- 4#分厂车间：智能卡和类似设备等安全芯片模块产品的封装服务。

- 4#分厂仓库：对材料的接收、标识、入库登记以及储存，成品仓储以及发货。
- 总机房：网络设备及服务器等位于车间配套机房的 2 楼。

2.2 站点描述 Site Description

The campus is surrounded by a fence that is guard with surveillance and secured by security guards, restrictions and access controlled from main gate. Additionally, guard services, access control and surveillance restrict and control the access to HPCZ production plant. The site includes different rooms and areas that are located in different plants/buildings:

- Plant #2:
  - Security control room
  - eSIM product encapsulation production area (including production workshop, raw material storage area, wafer and frame storage area, internal packaging area, server room)
  - UPS equipment room
- Plant #4:
  - Security control room
  - Smart card and similar devices product encapsulation production area (including production workshop, raw material storage area, wafer and tape reel storage area, internal packaging area, server room)
  - Warehouse area (including external packaging area, raw material storage room, main material storage room, finished goods storage room, packaging material storage area, delivery/loading area)
- Plant server building:
  - Main network & server room

园区由装有监控设备的围墙包围，同时有安保人员进行监控，园区入口有门禁进行控制。此外，HPCZ 生产车间也部署了安保人员、门禁以及监控措施。站点包括位于不同车间/建筑的不同房间和区域：

- 2 号车间：
  - 安控室
  - eSIM 产品封装生产区域（包括生产车间、原材料存放区、硅圆框架存放区、内包装区、机房）
  - UPS 机房
- 4 号车间：
  - 安控室

  - 智能卡和类似设备产品封装生产区域（包括生产车间、原材料存放区、硅圆载带存放区、内包装区、机房）
  - 仓库区域（包括外包装间、原材料库、主材库、成品库、包材间、收发货区域）
- 总机房：
  - 网络设备及服务器机房

The following service and/or processes provided by HPCZ are in the scope of the evaluation process:

- Reception, identification, registration and storage of materials
- Wafer sawing
- Assembly into modules
- Quality control testing for incoming raw materials and each production process
- Electronic testing and visual inspection of finished modules
- Warehousing and shipment of finished modules
- Product security flaw collection, verification, correction and corrective action delivery
- Scrap recycle and return to customer

以下 HPCZ 提供的服务以及流程都包含在本次评估的范围内：

- 对材料的接收、标识、入库登记以及储存
- 硅圆减划
- 封装为模块
- 来料质检以及各工序质量检测
- 成品电性测试以及目检
- 成品仓储以及发货
- 产品安全漏洞的收集、验证、整改和整改措施的交付
- 废品回收返还至客户

The complete flow of the security IC modules for smart card product at the site is covered by the SST. In addition, the management of the security IC modules for smart card related processes and the site security are covered by the SST. The production flow of the security IC modules for smart cards starts from the delivery of parts for the product (incoming raw materials) up to the packaging phase, and then shipping the finished security IC modules for smart cards to the next production phase (external parties: clients). The clients of HET, e.g., an IC developer, or ICC (smart card) developer, send the wafer or sawn wafer to HPCZ for the chips packaging. Next, the packaged finished modules, which are the final products of this site, will be sent back to the clients.

智能卡产品的安全芯片加工流程都已在 SST 中进行了描述。此外，智能卡相关流程的安全芯片模块的管理以及站点的安全也都在 SST 中进行了描述。本站点进行的智能卡安全芯片模块

的生产流程起始于原材料的接收，然后封装，将成品包装发送至下一生产阶段（外部：客户）。HET 的客户如 IC 开发商、ICC 智能卡开发商，会将未减划或已减划的硅圆送至 HPCZ 进行芯片封装，封装完成的模块将作为站点的成品发回给客户。

The site life-cycle phase for the Security IC modules can be subjected (but not limited to) to the Protection Profile (1) Phase 4:

此站点安全 IC 模块的生命周期阶段基于(但不限于)以保护配置文件 (1):

- Life cycle phase 4: IC Packaging 生命周期第四阶段：IC 封装
  - Security IC packaging (and testing)安全芯片封装(以及测试)

3 一致性声明 Conformance Claim

The evaluation of this site is based on Common Criteria Version 3.1, Revision 5.

该评估基于通用标准第 3.1 版，修订版 5。

- Common Criteria for Information Technology Security Evaluation, Part1: Introduction and general model; Version 3.1, Revision 5, April 2017, (2)

  信息技术安全评估通用标准，第 1 部分：介绍和通用模型；第 3.1 版，第 5 版，2017 年 4 月， (2)

- Common Criteria for Information Technology Security Evaluation, Part3: Security assurance components; Version 3.1, Revision 5, April 2017, (3)

  信息技术安全评估的通用标准，第 3 部分：安全保证组件；第 3.1 版，第 5 版，2017 年 4 月， (3)

For the evaluation, the following methodology is used:

对于评估，将采用以下方法：

- Common Methodology for Information Technology Security Evaluation: Evaluation methodology. Version 3.1, Revision 5, April 2017, (4)

  信息技术安全评估的通用方法：评价方法。第 3.1 版，2017 年 4 月第 5 版， (4)

This Site Security Target (SST) is **CC Part 3 conformant**. This SST claims the EAL6 package augmented with ALC_FLR.1, which consists of the following CC assurance components:

本站点安全目标(SST)符合 CC 第 3 部分，本 SST 符合 EAL6 增加 ALC_FLR.1，其中包括以下 CC 保证组件:

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

The assurance components chosen for the SST are taken from the definition of the EAL6 package defined in (3), because EAL5+ and above are the levels usually applied for Smart Card and similar devices evaluations related with Protection Profile (1).

为 SST 选择的保证组件取自 (3)中定义的 EAL6 压缩包的定义，因为根据保护配置文件 EAL5+及以上是通常用于智能卡和类似设备评估的级别。

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

为了评估安全措施，假设攻击者具有很高的攻击潜力。这允许根据保证组件 AVA_VAN.5 使用本站点对产品进行评估。

Note:

The site does not provide services that are covered by ALC_TAT.3 as no development activities are carried out in the site.

该站点没有进行任何开发活动，因此不提供 ALC_TAT.3 所涵盖的服务。

The site does not provide contributions to ALC_DEL.1 as there are no delivery activities of the final TOE to the end user are carried out at the site.

该站点没有向最终客户交付产品，因此该站点不为 ALC_DEL.1 提供贡献。

PUBLIC

4 安全问题定义 Security Problem Definition

The Security Problem Definition comprises security problems derived from the threats of the assets handled at the site and security problems derived from the configuration management. The configuration management covers the integrity and confidentiality of the products and the security management of the site.

安全问题定义包括源于对站点处理的资产的威胁的安全问题和源于配置管理的安全问题。配置管理包括产品的完整性和站点的安全管理。

This Site Security Target is based on the life cycle defined in the Security IC Platform Protection Profile (1). The assets (Section 4.1), threats (Section 4.2) and Organizational Security Policies (OSP) (Section 4.3) defined in this document are derived from the life cycle defined in the Protection Profile (1).

本站点安全目标基于安全 IC 平台保护配置文件中定义的生命周期 (1)，本文档中定义的资产(第 4.1 节)、威胁(第 4.2 节)和组织安全策略(OSP)(第 4.3 节)源自该 PP 中定义的生命周期。

The Security Problem Definition comprises two major so-called security problems. The first set of security problems comprises all types of attacks regarding theft (e.g. samples) or disclosure (e.g. design data) or manipulation of assets. These security problems are described in terms of threats. The second set of security problems comprises the requirements for the configuration management (e.g. controlled modification) and the control of security measures (e.g., access control). These security problems are described by the Organizational Security Policies (OSPs).

安全问题定义包括两个所谓的主要安全问题。第一组安全问题包括关于盗窃（例如，样本）或泄露（例如，设计数据）或操纵资产的各种攻击。这些安全问题以威胁的形式来描述。第二组安全问题包括对配置管理(例如受控修改)和安全措施控制的需求（例如访问控制）。这些安全问题将根据组织安全策略（OSPs）来描述。

4.1 资产 Assets

The following sections describe the assets handled at the site.

以下部分描述了在站点上处理的资产。

The site has the internal documentation and data that are relevant to maintain the confidentiality and integrity of the intended TOE. This comprises site security concepts and the associated security measures as well as key and cryptographic tools for the encrypted change of data. These items are not explicitly listed in the list of assets below.

该站点拥有与维护预期 TOE 的机密性和完整性相关的内部文档和数据。这包括站点安全概念和相关的安全措施，以及用于加密数据更改的密钥和加密工具。这些项目并没有在下面的资产列表中明确列出。

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

items consist of commercially available hardware and software, which are programmed and customised by HPCZ.

用于生产和测试的任何机器或工具的完整性不被视为资产。然而，为确保这一重要条件，现站点制定了适当的措施。这些项目包括由 HPCZ 编制和定制的商用的硬件和软件。

4.1.1 IC 组件 IC Assembly

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

- Wafer, sawn wafer and unfinished products
- Finished products as modules or other packages
- Defective or rejected products.

与安全硅圆生产相关的资产如下:

- 硅圆，减划的硅圆和半成品
- 成品，如模块或其他封装形式
- 有缺陷或被拒收的产品

There can be further client specific assets like seals, special transport protection or similar items that support the security of the internal shipment to the client. They are handled in the same way as the other assets to prevent misuse, disclosure or lost.

可以还有其他客户特定资产，如印章、特殊运输保护或类似物品，以支持向客户内部运输的安全性。它们的处理方式与其他资产相同，以防止滥用、披露或丢失。

4.1.2 开发安全文档 Development Security Documentation

The development security documentation containing sensitive information is regarded as sensitive asset in terms of its integrity and confidentiality, which is classified as Confidential. However, development security documentation with the absence of sensitive information is considered as Internal.

包含敏感信息的开发安全文档在其完整性和机密性方面被视为敏感资产，并被分类为机密文件。但是，没有敏感信息的开发安全文档被视为内部文档。

4.1.3 生产数据 Production Data

Production data is the data being generated during the production process. It is considered as a sensitive information asset requiring the protection in accordance with the confidentiality and integrity of the intended TOE. Therefore, the production data is classified as Confidential.

生产过程中生成的数据称为生产数据。它被认为是一种需要根据其机密性和完整性进行保护的敏感信息资产。因此，生产数据被归类为机密文件。

4.2 风险 Threats

All threats endanger the integrity and confidentiality of the intended TOE and the representation of parts of the intended TOE. The intended TOE protects itself in life-cycle phase 7 (see (1)). However, during the production, testing and assembly of the intended TOE and the representation of parts of the intended TOE are vulnerable to the integrity and confidentiality attacks.

所有风险都会危及预期 TOE 的完整性和机密性以及预期 TOE 各部分的代表性。预期 TOE 在生命周期第 7 阶段自我保护（参见 (1)）。然而，在生产、测试和组装过程中，预期 TOE 和预期 TOE 零件很容易受到完整性和机密性攻击。

The following threats are described in a general way. However, they are applicable to the site that handles the assets listed in Section 4.1. All the threats described below shall be countered by the Security Objectives of the site.

以下是对风险的一般描述。但是，它们适用于提供处理上文第 4.1 节所列项目的服务的站点。以下风险的解释应支持映射到站点的安全目标。

T.Smart-Theft

An attacker tries to access security areas of the site for manipulation or theft of intended TOE (or its parts) during production. The attacker has sufficient time to investigate the site outside the controlled boundary. For the attack, the usage of standard equipment for burglary is considered. In addition, the attacker may be able to use specific working clothes of the site to hide the intention.

攻击者试图访问站点的敏感区域，以操作或盗窃预期的 TOE 部件。攻击者有足够的时间来调查受控边界外的站点。对于攻击，应考虑使用标准设备进行盗窃。此外，攻击者还可以使用现场的特定工作服来伪装意图。

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 unregistered or defective chips that can be used to further investigate the functionality of the chip and search for possible exploits. Such an attacker will have limited resources and a low financial budget to prepare the attack. However, the large amount of time that can be spent by such an attacker to prepare the attack will impose a notable risk.

这次攻击已经包括了与上一节中列出的各种资产有关的目标和方面。它应涵盖试图获得未注册或缺陷芯片的个性化范围，这些芯片可用于进一步调查芯片的功能并搜索可能的漏洞。这样的攻击者将拥有有限的资源和较低的财政预算来准备攻击。然而，这种攻击者为准备攻击所花费的时间以及这种攻击者的灵活性将带来显著的风险。

T.Rugged-Theft

An experienced thief with specialized equipment for burglary, who may be paid to perform the attack tries to access security areas and manipulate or steal intended TOE (or its parts) during production.

一个被雇佣的配备专业入室盗窃设备的经验丰富的小偷，可能进入敏感区域并在生产中操纵或盗窃预期的 TOE 零件。

Although this attack is applicable for each site, the risk may be different regarding the assets. These attackers may be prepared to take high risks for payment. They are sufficiently resourced to circumvent security measures and do not consider any damage of the affected company. The target of the attack may be products that can be sold or misused in an application context. This can comprise chips at a specific testing or personalization state for cloning or introduction of forged chips. Those attackers are considered to have the highest attack potential.

尽管这种攻击适用于每个站点，但关于资产的风险可能会有所不同。这些攻击者可能为了报酬承担高风险。他们有足够的资源来规避安全措施，并且不考虑受影响公司的任何损失。攻击的目标可能是在应用程序上下文中可能被销售或误用的产品。这可以包括用于克隆或引入伪造芯片的特定测试或个性化状态的芯片。这些攻击者被认为具有最高的攻击潜力。

Such attackers may not be completely defeated by the physical, technical and procedural security measures. Special security measures like storage of items in safes or secured rooms provide additional support against such attacks. Also, the unique registration of the products can support the protection if they can be disabled or blocked.

物理、技术和程序安全措施可能无法完全战胜这类攻击者。特殊措施，如将物品存放在保险箱或安全的房间中，为抵御此类攻击提供了额外的支持。此外，如果可以禁用或阻止产品，则产品的唯一注册可以支持保护。

T.Computer-Net

An attacker with substantial expertise, standard equipment, who may be paid to attempt to access the critical network segments remotely to get access to sensitive configuration data or items or modify security relevant production processes.

一个拥有大量专业知识和标准设备的黑客，他们可能会被收买，试图远程访问重要的网络段，以访问敏感的配置数据或项目，或修改与安全相关的生产过程。

T.Accidental-Change

An employee, contractor or student trainee may exchange products of different production lots or different clients during production by accident.

员工、承包商或实习学员在生产过程中可能因意外情况调换不同生产批次或不同客户的产品。

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

未经培训的员工、承包商或学员可能会不考虑可能产生的影响或问题就拿走产品或影响生产系统。这种威胁包括意外变化，例如由于学员的工作任务或承包商在开发、生产或测试区域内的维护任务。

Such accidental changes can include the modification of configurations for tools that may have an impact on the intended TOE, or misuse of the tools during production. Other examples may be production machine failures or mixed products during production among operators that are responsible for products of different clients or different products of the same client. This also includes the disposal of sensitive products using the simple “trash” procedure, and not the controlled secure handling of the defective sensitive products.

此类意外变化可能包括修改可能对预期 TOE 产生影响的工具配置，以及生产中错误使用工具。进一步的例子可能是机器故障或负责不同客户产品的操作员之间的错位，或者同一客户的不同产品在生产过程中混合。这还包括使用简单丢弃流程而不是可控安全的处理流程来处置敏感废品。

T.Unauthorized-Staff

Employees or subcontractors that are not authorized to get access to products or systems used for production get access to products or affect production systems, so that the confidentiality and/or the integrity of the product could be impaired. This can apply to any intended TOE (or its parts) in production.

未经授权的员工或分包商接触用于生产的产品或系统，接触产品或影响生产系统，使产品的保密性和/或完整性受到侵犯。这可以适用于生产中任何预期的 TOE 部件。

Also, other subcontractors like cleaning staff or maintenance staff for the building get limited access that may allow them to plan and conduct an attack. The secure handling of defective equipment and/or intended TOE (or its parts) must be considered.

此外，其他分包商，如清洁人员或维修人员有受限的访问权限，这可能使他们能够计划并发动攻击。必须考虑缺陷设备和/或预期 TOE 零件的安全处理。

T.Staff-Collusion

An attacker tries to get access to sensitive data or items stored or processed at the site. The attacker tries to get support from one or more employees through an attempted extortion or bribery.

攻击者试图访问该站点上存储或处理的敏感数据或项目。攻击者试图通过勒索或贿赂获得一名或多名员工的支持。

T.Attack-Transport

An attacker might try to get information or products during the external delivery to client. The target is to compromise confidential information or violate the integrity of the products during the stated external delivery process to allow a modification, cloning or the retrieval of confidential information after the intended TOE production.

攻击者可能试图在外部传递到客户端的过程中获取信息或产品。目标是在规定的外部交付过程中泄露机密信息或侵犯产品的完整性，以便在进一步的生产步骤后修改、克隆或检索机密信息。

4.3 组织安全策略 Organizational Security Policies

The following policies are introduced by the requirements of the assurance components. The chosen policies shall support the understanding of the production flow and the security measures of the site. All the OSPs described below shall be enforced by the Security Objectives of the site.

根据保证组件的要求，引入了以下策略。所选择的政策应支持对现场生产流程和安全措施的理解。以下描述的所有 OSP 都需要映射到站点安全目标。

The evaluation of the security documentation of the site is maintained by the configuration management system. This comprises all site procedures and policies regarding the intended TOE production, quality inspection, tests, assembly control flows and the security measures that are in the scope of evaluation.

安全文件的评估由配置管理系统维护。这包括评估范围内与 TOE 生产、质量检验、测试和封装控制流程以及安全措施有关的所有站点程序与政策。

P.Config-Items

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

配置管理系统应能够识别唯一地配置项目。它包括在现场创建、生成、开发、修改或使用的物品以及接收、转让和/或提供的物品的唯一标识。

The configuration management relies completely on the naming and identification of the received configuration items. The consistency with the expected identification is verified after receiving, and then each item is assigned with an internal unique identifier. This holds also for test programs and other items that are provided to the site for local use. For configuration items that are created, generated or developed at the site the naming and identification must be specified.

配置管理完全依赖于接收到的配置项的命名和标识。在收到后验证与预期标识的一致性，并为每个项目分配一个内部唯一标识。这也适用于提供给站点供本地使用的测试程序和其他项目。对于在现场创建、生成或开发的配置项，必须指定命名和标识。

P.Config-Control

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

设置新产品生产流程的程序以及允许更改产品初始设置的程序只能由授权人员使用。自动化系统应支持配置管理，并确保设置和变更的访问控制或交互式验收措施。生产过程的初始设置程序确保客户提供了足够的信息。

The product setup includes the following information: identification of the product, properties of the product when received at the site, properties of the product when internally moved in the same building, how the product is tested after assembly, any configuration of the processed item as part of the services provided by the site, which address is used for the internal transportation.

产品设置包括以下信息：产品的标识，产品在现场收到时的性质，产品在同一建筑物内部移动时的性质，产品在组装后如何进行测试，作为现场提供的服务一部分的加工物品的任何配置，用于内部运输的地址。

P.Config-Process

The services and/or processes provided by the site are stated in the configuration management plan. This plan comprises tools used for the development and production of the product, the management of flaws and optimizations of the process flow as well as the documentation that describes the services and/or processes provided by the site.

站点提供的服务和/或过程受控于配置管理计划。这包括用于产品开发和生产的工具、缺陷管理和流程优化，以及描述站点提供的服务和/或流程的文档。

The security documentation with the processes descriptions and the security measures of the site are maintained by a version control system. Control measures are in place to ensure that the defined procedures for the documentation and production management are followed. In most cases tools are used to support the processes at the site. This comprises e.g. scripts, programs or batch routines developed by the site and other 3rd party production data processing systems. This comprises also service levels and quality parameters.

包含流程描述和站点安全措施的文档处于版本控制之下。措施到位，以确保遵循定义的文档和生产管理流程。在大多数情况下，工具用于支持站点的制程。这包括例如由站点开发的脚本、程序或批处理例程和第三方生产数据处理系统。这也包括服务水平和质量参数。

P.Reception-Control

The inspection of incoming items performed at the site ensures that the received configuration items comply with the properties stated by the client. Furthermore, it is verified that the product can be identified, and a released production process is defined for the product. This aspect includes the check that all required information and data is available to process the items.

在现场对进料项目进行检查，确保收到的配置项目符合客户规定的属性。此外，还验证了产品的可识别性，并为产品定义了已发布的生产流程。这方面包括检查处理项目所需的所有信息和数据是否可用。

P.Accept-Product

The testing and quality control of the site ensures that the products released by the site comply with the specifications agreed with the client. The acceptance process is supported by automated means. Production records are generated during the acceptance process of the configuration items. Thereby, it is ensured that the properties of the product are ensured when the products are in release phase.

站点的测试和质量控制确保放行的产品符合与客户商定的规格。由自动化措施支持验收过程。对配置项的验收过程进行记录。因此，在产品处于发布阶段时，可以确保产品的特性得到保证。

P.Zero-Balance

The site ensures that all sensitive items (security relevant parts of the intended TOEs of different clients) are separated and traced on the chip basis. According to the released production process, the defective assets are sent back to the client.

该站点确保所有敏感项目（不同客户的预期 TOE 的安全相关部分）都在芯片基础上进行分离和跟踪。根据发布的生产流程，缺陷资产被送回客户。

This policy covers the packing and handover of products at the site after the applied production flow. All finished products are sent back to the clients that provided the items or sending the products to the specific locations requested by the clients. This is considered as an internal shipment to the client (not the end user).

本政策涵盖了加工后现场产品的包装和移交。所有成品都会退回给提供物品的客户，或发送到客户要求的特定位置。这被视为向客户（不是最终用户）的内部发货。

P.Product-Transport

Technical and organizational measures shall ensure the correct labelling of the product. A controlled external delivery to client (not the end user) shall be applied. The transport supports traceability up to the recipient. In case the product needs to be moved within the building, this will be considered as internal transportation.

技术和组织措施应确保产品标签的正确性。应采用受控的外部交付给客户（不是最终用户）。运输支持可追溯到接收者。如果产品在建筑内移动，这将被视为内部运输。

P.Organize-Product

The production process is applied as specified by the site's configuration management plan. If the production data includes sensitive items, appropriate security measures must be applied.

生产过程按照现场配置管理计划的规定进行。如果生产数据包括敏感项目，则必须采取适当措施。

P.Flaw-Remediation

A flaw remediation procedure must be in place to continually minimize potential flaw by tracking and handling reported security flaws across their life cycle.

必须有一个缺陷修复程序，通过跟踪和处理整个生命周期中报告的安全缺陷，不断减少潜在的缺陷。

4.4 假设 Assumptions

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received from the previous site. This is reflected by the assumptions that might be defined for the site, even though the assumptions lay outside of the evaluation scope. Therefore, any assumptions made are considered to be satisfied (i.e. true) during the evaluation. Assumptions provide a basis for an appropriate production process setup to ensure secure handling and storage of all configuration items related to the intended TOE production. The processing activities at the site rely on the assumptions related to the products, the data, the documentation and the transfer information/items provided by the client or the product supplier.

生产流程中的每个站点都必须依赖于前一个站点提供的先决条件。每个站点都必须依赖于从前一个站点接收到的信息。这反映在可能为站点定义的假设中，即使这些假设并不在评估范围内。因此，所有假设在评估中都会被认为是满足的。假设为恰当生产流程的制定奠定基础，确保与 TOE 生产相关的所有配置项的安全处理与保存。站点的处理依赖于以下与客户或产品供应商提供的产品、数据、文件和转让信息相关的假设。

A.Item-Identification

Each configuration item received by the site shall be appropriately labelled to ensure the correct identification of the configuration items received from the client.

站点接收的每个配置项都有适当的标签，以确保从客户接收到的配置项的正确识别。

A.Prod_Release

The client is responsible for the release of the products to be produced.

客户负责发布将要生产的产品。

A.Prod-Specification

The product developer must provide appropriate specifications and guidance for the assembly and testing of the product. This comprises configuration management plan for an appropriate assembly process as well as test requirements and test parameters for the development of the electronic tests or finished test programs appropriate for the final testing. The provided information includes the classification of the delivered items, documents and data.

产品开发者必须为产品的组装和测试提供适当的规格和指导。这包括适当装配过程的粘合计划，以及用于开发电性测试的测试要求和测试参数，或适用于最终测试的完成测试程序。提供的信息包括交付物品的分类、文件和数据。

A.External-Delivery

The recipient (Card issuer or Smart Card Production plant) of the product is identified by the address provided by the client. The address of the client is part of the product setup. Every recipient of the product is identified by the address provided by the client.

由客户提供产品接收者（发卡机构或智能卡生产工厂）的地址。客户的地址是产品设置的一部分。产品的每个收件人都由客户提供的地址标识。

A.Product-Integrity

The self-protecting features of the chip are fully operational, and it is not possible to influence the configuration or behavior of the chips based on insufficient operational condition or any commands sequences generated by an attacker or by accident.

芯片的自我保护特性是完全可行的，不可能基于不充分的操作条件或攻击者或意外产生的任何命令序列来影响芯片的配置和行为。

The developer assumes that the features used for testing of the chip (die) at the end of the life-cycle phase 3 and phase 4 (according to (1)) are disabled. The developer will be provided with the configuration of the product that will be used as the basis for the integrity protection during the internal transportation.

假设开发者在生命周期第 3 阶段和第 4 阶段（根据 (1)）结束时用于测试芯片特性已禁用。开发者将提供基于内部运输时保护基础的产品配置。

5 安全目标 Security Objectives

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

安全目标涉及物理、技术和组织安全措施、配置管理以及内部运输。

O.Security-Documentation

The security of the site is maintained according to the site's security documentation covering all physical and logical security measures.

根据现场安全文件维护现场安全，该文件涵盖了确保现场安全的所有物理和逻辑措施。

O.Physical-Access

The combination of physical partitioning between the different access control levels together with technical and organizational security measures allows a sufficient separation of employees to enforce the "need-to-know" principle for the production areas. The access control system shall limit the access to these areas including the identification and rejection of unauthorized people. The site enforces three levels (level 1 to level 3) of physical access control rights, which correspond to the controlled areas (level 1), security areas (level 2) and high-security areas (level 3) of the site. The access control measures ensure that only authorized employees and vendors can access such areas. Sensitive products are only handled in the production areas.

不同访问控制级别之间的物理分区与技术和组织安全措施相结合，使员工能够充分分离，以执行"需要知道"原则。访问控制应识别和拒绝未经授权人员进入这些限制区域。站点强制执行三级（1 级至 3 级）的物理访问控制权限，分别映射到站点的控制区域（1 级）、安全区域（2 级）和高安全区域（3 级）。访问控制措施确保只有授权员工和供应商才能进入该区域。敏感产品仅在生产区域处理。

O.Security-Control

Assigned personnel of the site or guards operate the systems for access control and surveillance and they respond to alarms. Technical security measures like video monitoring, motion sensors and similar kind of sensors support the enforcement of the physical access control. These personnel are also responsible for registering and ensuring escort of visitors, contractors and suppliers.

现场指定人员或警卫人员操作门禁控制和监控系统，并响应警报。视频控制、运动传感器和类似类型的传感器等技术安全措施支持访问控制的实施。这些人员还负责访客、承包商和供应商的登记和陪同。

O.Alarm-Response

The technical and organizational security measures ensure that an alarm is activated (detection layer) before an unauthorized person gets access to any sensitive configuration items (asset). After the alarm has been triggered, the unauthorized person must be hold back by other security measures (stop layer). The reaction time of the employees or security guards must be short enough to prevent the attack.

技术和组织安全措施确保在未经授权的人员访问任何敏感配置项(资产)之前产生警报（侦测层）。触发警报后，必须通过其他的安全措施阻止未被授权的人员。员工或警卫人员在足够短的时间内响应以防止攻击成功。

O.Internal-Monitor

The site performs security management meetings annually. The security management meetings are used to review security incidences, to verify that the security measures are correctly configured, and to reconsider the assessment of risks and security measures. Furthermore, an internal audit is performed every year to control the application of the security measures. Sensitive processes maybe controlled within a shorter period to ensure the sufficient level of protection.

该站点每年举行一次安全管理会议。安全管理会议用于审查安全事件，验证是否正确部署安全措施，并重新考虑对风险和安全措施的评估。此外，每年都会进行一次内部审计，以控制安全措施的应用情况。可以在较短时间内控制敏感过程，以确保有足够的保护。

O.Maintain-Security

Technical security measures are maintained regularly to ensure correct operation and uninterrupted operation. The logging information of the sensitive systems is checked regularly. This comprises the access control system to ensure that only authorized employees have access to sensitive areas as well as computer/network systems to ensure that they are configured as required to ensure the protection of the developer network and computer systems.

为确保正确操作和不被中断的操作，需定期维护技术安全措施。定期检查敏感系统的日志记录情况。这包括确保只有授权员工才能访问敏感区域的访问控制系统，以及确保根据需要配置计算机/网络系统以确保对网络和计算机系统的保护。

O.Logical-Access

Access to the production operation machines and related production systems are restricted to authorize employees that work in the related area or that are involved in the configuration tasks or the production operations. Every user of an IT system has its own user account and password. Authentication of the users is enforced by all computer systems.

对生产机器操作和相关系统的访问仅限于授权在相关区域工作或涉及配置任务或生产系统的员工。IT 系统的每个用户都有自己的帐户和密码。所有计算机系统都强制要求用户进行身份验证。

O.Logical-Operation

All network segments and the computer systems are kept up to date (software/hardware updates/upgrades, security patches and virus protection). The backup of sensitive data and security relevant logs is applied and protected according to the classification of the original data.

所有网段和计算机系统都保持更新（软件/硬件更新/升级、安全补丁和病毒防护）。根据原始数据的分类，备份敏感数据和安全相关日志。

O.Config-Items

The site has configuration management systems that assign a unique internal identifier to each product/item to uniquely identify configuration items and allow their trackability and traceability. In addition, the internal security procedures and guidance documentation are covered by the configuration management systems.

该站点有配置管理系统，该系统为每个产品分配一个唯一的内部标识，以唯一地标识配置项，并允许对他们的可追踪性。此外，配置管理系统涵盖了内部安全程序和指南文件。

O.Config-Control

The site applies a release procedure for the setup of the production process for each new product. In addition, the site has a process to classify and introduce changes for services and/or processes of released products. A designated team/employee is responsible for integration of new products or changes into the configuration management system.

站点为每个新产品的生产流程设置应用发布程序。此外，该站点有一个对已发布产品的服务和/或流程进行分类和引入变更的流程。指定的团队/员工负责将新产品或变更整合到配置管理系统中。

O.Config-Process

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

站点使用配置管理计划控制其服务和/或过程。配置管理由用于产品生产的工具和程序、用于缺陷管理和工艺流程优化的工具和程序以及用于描述站点提供的服务和/或过程的文档控制。

O.Acceptance-Test

The site ships the outgoing configuration items that fulfil the specified properties. Parameter checks, electronic and/or visual checks and inspection, and quality tests as specified by the clients are performed to ensure the release product is compliant with the client specifications. The test results are logged to support tracing and the identification of systematic failures.

站点提供满足指定属性的配置项。执行客户指定的参数检查、功能和/或目视检查和测试，以确保符合规格。记录测试结果，以便追溯以及识别系统故障。

O.Staff-Engagement

All employees who have access to the intended TOE (or its parts), and who can move TOE (or its parts) out of the production areas are thoroughly checked for the security violations and must sign a non-disclosure agreement. Furthermore, all employees in the production areas are trained and qualified for their job.

所有能够接触到预期 TOE 零件并能够将产品零件移出生产区域的员工都要接受安全问题检查，并且必须签署保密协议。此外，所有生产区域的员工都接受过培训，并具备胜任工作的资格。

O.Zero-Balance

The site ensures that all sensitive products (intended TOE of different clients) are separated and traced on a chip basis. Automated control and/or two employee's acknowledgement is applied for during shipment of the functional chips. The defective chips will be sent back to the client. All the production stages of sensitive products are automatically managed through the configuration systems, the quantity of the intended TOE and defective products are recorded in the configuration system to ensure that all the sensitive materials/parts are under control.

该站点确保所有敏感产品（不同客户的预期 TOE）在芯片基础上进行分离和跟踪。在移交功能性芯片时需自动控制和/或两个员工的确认。缺陷芯片将退还给客户。敏感产品的所有生产阶段都通过配置系统自动管理，预期 TOE 和缺陷产品的数量记录在配置系统中，并确保所有敏感材料都处于充分的控制之下。

O.Reception-Control

Upon reception of the incoming products (raw materials), an immediate inspection is performed. The inspection of physical products is done according to the internal requirements. It comprises the surface checks of raw materials, quantity of products checks, the identification and assignment of the product to a related internal production process. For security checks, the integrity and authenticity of the incoming products are verified upon reception.

在收到产品（原材料）后，就会立即进行进货检查。实物产品的检验是根据内部标准进行的。它包括原材料的外观、收到的产品数量、产品的识别和分配到相关的内部生产过程。为了安全起见，产品完整性和真实性在接收时进行验证。

O.External-Delivery

The sender of a physical configuration item is identified by the assigned client address on the shipment form. The sender of an electronic configuration item (e.g., initialization data, response data) can be identified in different ways (e.g., certificates, public keys). The specific way is defined in the procedure of external delivery to client (not final intended TOE user). The external delivery procedure is applied to all sensitive configuration data or items. The recipient of shipment can only be changed by a controlled process and authorization is required. The packaging (if any) is also part of the defined process and applied as agreed with the client. The approved couriers supports the tracking of sensitive configuration data or items during external delivery. For every configuration data or item, the integrity and authenticity security measures are defined (if necessary) to protect the product against manipulation/alteration/forging.

物理配置项的发件人根据发货单上客户端指定的地址标识。电子配置项目（例如初始化数据、响应数据）的发送者可以通过不同的方式识别。具体的方式在外部交付给客户（非最终目标 TOE 用户）的过程中定义。外部传递过程适用于所有敏感的配置数据或项目。装运的收件人只能通过一个受控的流程进行更改。包装（如有）也是定义过程的一部分，并按照客户的约定进行作业。在外部传递期间，代运人支持对敏感配置数据或项目的跟踪。对于每个配置数据或项目，都定义了防止操作/修改/篡改的完整性和真实性安全措施（如有必要）。

O.Transfer-Data

Sensitive electronic configuration items (data or documents in electronic form) are protected by applying cryptographic algorithms to ensure confidentiality and/or integrity (whatever is required) during internal transportation and external delivery to/from client (not the end user). In case asymmetric cryptographic algorithms are applied, the associated cryptographic keys must be assigned to individuals to ensure that only authorized employees are able to extract the sensitive electronic configuration items. Alternatively, the symmetric key or password-based exchanges methods might be used (e.g. symmetric key encrypted files, password protected archives). In the latter case, it has to be ensured that only authorized users have access to the symmetric cryptographic keys or passwords. The cryptographic keys and/or passwords are exchanged/stored based on the defined security measures, and they are sufficiently protected.

敏感的电子配置项目（电子形式的数据或文件）通过应用加密算法进行保护，以确保在内部运输和外部交付给客户（不是最终的 TOE 用户）期间的机密性和/或完整性（无论需要什么）。在应用非对称加密算法的情况下，必须将相关的加密密钥分配给个人，以确保只有授权员工才能提取敏感的电子配置项目。或者，可以使用对称密钥或基于密码的交换方法（例如，对称密钥加密文件、密码加密档案）。在后一种情况下，必须确保只有授权用户才能访问加密密钥或密码。

O.Control-Scrap

The site has security measures in place to destroy sensitive documentation/items/media and securely erase electronic data media, so that the data cannot be used in any meaningful way to impair confidentiality of the TOE. The defective and rejected products (scraps) are collected and returned back to the client.

该站点已采取安全措施销毁敏感文件/项/媒介，并安全擦除电子媒体，使其数据无法再通过任何方式使用来影响 TOE 机密性。收集有缺陷和被拒绝的产品并将其退还给客户。

O.Flaw-Remediation

This site has defined a written procedure and appointed responsible to collect, track and handle any reported security flaw to achieve a goal that reported security flaw being handled, potential security flaw being prevented and corrective actions being delivered to the intended TOE receiver.

本站点已制定书面程序，并指定专人负责收集、跟踪和处理任何已报告的安全漏洞，以达到已报告的安全漏洞正在处理的目标，防止潜在的安全漏洞，并将纠正措施传递给预期的 TOE 接收器。

5.1 安全目标基本原理 Security Objectives Rationale

The following table provides the rationale for the Security Objectives tracing showing that all the Threats and/or OSPs are effectively addressed by the Security Objectives.

下表为安全目标基本原理，显示了安全目标涵盖了所有威胁和 OSP。

5.1.1 安全目标映射 Mapping of Security Objectives

Threats and OSP 威胁和 OSP	Security Objective 安全目标	Note 注释
T.Smart-Theft 智能盗窃	O.Security-Documentation 安全文档 O.Physical-Access 物理访问 O.Security-Control 安全控制 O.Alarm-Response 预警响应 O.Internal-Monitor 内部监控 O.Maintain-Security 安全维护	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threat. 结构、技术和组织措施相结合，可检测未经授权的访问，并允许对任何威胁做出适当反应。
T.Rugged-Theft	O.Security-Documentation 安全文档 O.Physical-Access 物理访问 O.Security-Control 安全控制 O.Alarm-Response 预警响应 O.Internal-Monitor 内部监控	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats. 结构、技术和组织措施相结合，可检测未经授权的访问，并允许对任何威胁做出适当反应。

	O.Maintain-Security 安全维护	
T.Computer-Net 计算机网络	O.Security-Documentation 安全文档 O.Logical-Access 逻辑访问 O.Logical-Operation 逻辑操作 O.Internal-Monitor 内部监控 O.Maintain-Security 安全维护 O.Staff-Engagement 员工参与	Physical and logical access control limits the access to sensitive data to authorized persons. In addition, organizational measures prevent uncontrolled access to products or product related items. 物理和逻辑访问控制限制授权人员访问敏感数据。此外，组织措施防止对产品或产品相关项目的不受控制的访问。
T.Accidental-Change 意外变更	O.Logical-Access 逻辑访问 O.Physical-Access 物理访问 O.Config-Items 配置项目 O.Staff-Engagement 员工参与 O.Config-Process 配置过程 O.Zero-Balance 零平衡 O.Acceptance-Test 验收测试	The automated measures and the control and verification procedures avoid accidental changes of sensitive items. 自动化措施以及控制和验证程序避免了敏感物品的意外变化。
T.Unauthorized-Staff 未经授权的员工	O.Logical-Access 逻辑访问 O.Physical-Access 物理访问 O.Security-Control 安全控制 O.Logical-Operation 逻辑控制 O.Internal-Monitor 内部监控 O.Maintain-Security 安全维护 O.Security-Documentation 安全文档 O.Alarm-Response 预警响应 O.Zero-Balance 零平衡 O.Staff-Engagement 员工参与 O.Control-Scrap 报废控制	The application of internal security measures combined with the hiring policies that restrict hiring to trustworthy employees prevent unauthorized access to the sensitive data or items. 将内部安全措施与限制雇佣可靠员工的招聘政策相结合，以防止未经授权访问敏感数据或项目。

T.Staff-Collusion 员工串通	O.Security-Documentation 安全文档 O.Staff-Engagement 员工参与 O.Internal-Monitor 内部监控 O.Maintain-Security 安全维护 O.Transfer-Data 数据传输 O.Control-Scrap 报废控制	The applied security measures on sensitive data during internal transportation and external delivery prevent modification or disclosure of any sensitive data during transport. The applied security measures on physical items during internal transportation and external delivery allow detection of attempted attacks. 在内部运输和外部运输过程中对敏感数据采取的安全措施，防止在运输过程中对敏感数据进行修改或披露。在内部运输和外部交付过程中，对实物采取了安全措施，可以检测到企图发动的袭击。
T.Attack-Transport 运输攻击	O.External-Delivery 外部交付 O.Transfer-Data 数据传输	The combination of structural, technical and organizational measures detects unauthorized access and allow for appropriate response on any threats. 结构性、技术性和组织性措施的结合可以检测到未经授权的访问，并允许对任何威胁作出适当的反应。
P.Accept-Product 产品接收	O.Acceptance-Test 验收测试 O.Config-Control 配置控制 O.Config-Process 配置设置	On request of the client release tests are performed. 根据客户端的要求，执行批准测试。
P.Config-Control 配置控制	O.Config-Control 配置控制 O.Config-Items 配置项目 O.Config-Process 配置过程 O.Reception-Control 接收控制 O.Logical-Access 逻辑访问	The scope of the configuration control comprises the production process. 配置控制的范围包括生产过程。
P.Config-Items 配置项目	O.Config-Items 配置项目 O.Reception-Control 接收控制	All relevant items are covered by the control. 所有相关项目均纳入控制范围。
P.Config-Process 配置过程	O.Config-Process 配置过程	The scope of the configuration control comprises the production process. 配置控制的范围包括生产过程。
P.Organize-Product 组织产品	O.Config-Process 配置过程 O.Config-Control 配置控制 O.Logical-Access 逻辑访问 O.Logical-Operation	The application of the production processes is supported by technical and organizational means. 生产过程的应用得到了技术和组织手段的支持。

	逻辑操作	
P.Product-Transport 产品运输	O.External-Delivery 外部交付 O.Transfer-Data 数据传输 O.Config-Items 配置项目	The controlled shipment and delivery procedures ensure correct shipment and delivery of items. 受控的装运和交付程序确保物品的正确装运和交付。
P.Reception-Control 接收控制	O.Reception-Control 接收控制	The incoming control on physical items ensures that only authentic items of correct quantity are accepted. 对实物的接收控制确保只接受正确数量的正品。 The incoming control on integrity and availability of items ensures that only authentic and qualified items are accepted. 对物品的完整性和可用性的输入控制确保只有真实和合格的物品被接受。
P.Zero-Balance 零平衡	O.Zero-Balance 零平衡 O.Control-Scrap 报废控制 O.Internal-Monitor 内部监控 O.Staff-Engagement 员工参与	The handling of correct and defective items ensures that no unexpected missing items or left-over items occur. 正确和有缺陷的物品的处理确保不会出现意外的物品丢失或遗留。
P.Flaw-Remediation 缺陷修复	O.Flaw-Remediation 缺陷修复	Reported security flaw will be handled according to the written procedure of flaw remediation so that reported security flaw will be collected, tracked and handled in a concerted way. 报告的安全缺陷将按照缺陷修复的书面程序进行处理，以便对报告的安全缺陷进行协同收集、跟踪和处理。

TABLE 1 MAPPING OF SECURITY OBJECTIVES

The following table provides the tracing from the Security Objectives to the Threats and/or Organizational Security Policies (OSPs).

下表显示了安全目标与威胁和/或组织安全策略（OSPs）之间的映射。

	O.Acceptance-Test	O.Alarm-Response	O.Config-Control	O.Config-Items	O.Config-Process	O.Control-Scrap	O.External-Delivery	O.Internal-Monitor	O.Logical-Access	O.Logical-Operation	O.Maintain-Security	O.Physical-Access	O.Reception-Control	O.Security-Control	O.Security-Documentation	O.Staff-Engagement	O.Transfer-Data	O.Zero-Balance	O.Flaw-Remdediation
P.Accept-Product	X		X		X														
P.Config-Control			X	X	X				X				X						
P.Config-Items				X									X						

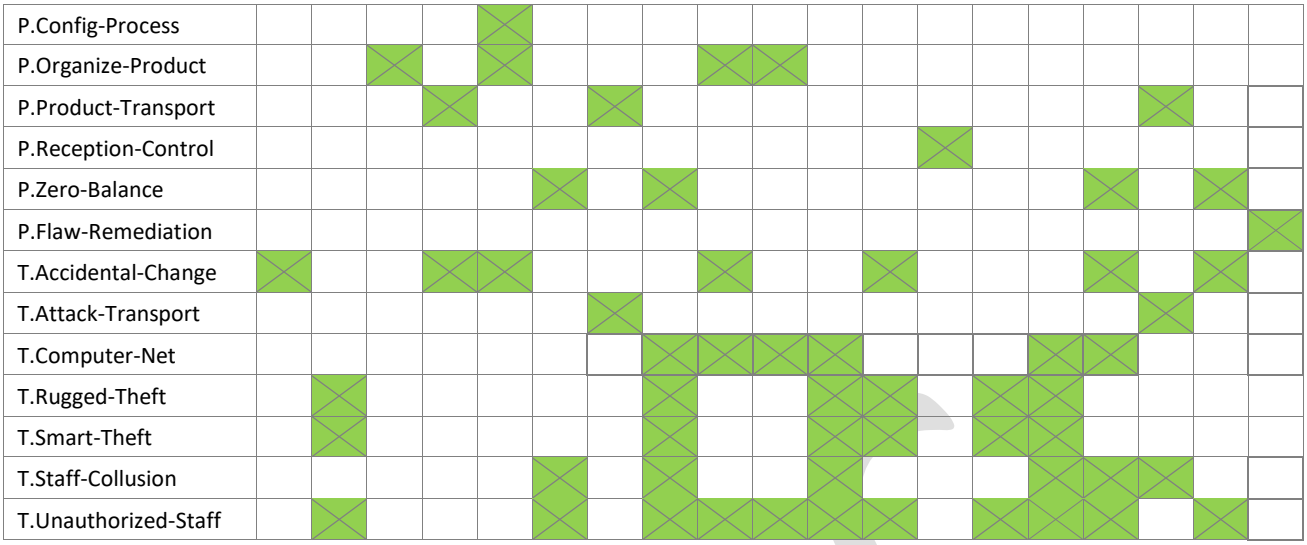

Table **2 MAPPING BETWEEN** policies/threads covering objectives

5.1.2 安全目标映射的论证 Justification of Security Objectives mapping

T.Accidental-Change

Objectives O.Logical-Access and O.Physical-Access protect the sensitive items defined by O.Config-Items from an unauthorized physical and logical access.

逻辑访问和物理访问保护配置项中定义的敏感项，免受未经授权的物理和逻辑访问。

O.Staff-Engagement ensures that staff with access to sensitive items are well trained and trustworthy and follow the CM plan defined by O.Config-Process.

员工参与确保以任何方式与敏感资产互动的员工都经过良好培训（配置流程）且值得信赖，并通过零平衡的目标防止任何资产在客户之间错误泄露。

O.Zero-Balance ensures correctness of shipment and traceability of the release products for each client.

零平衡确保每个客户的成品运输的正确性和可追溯性。

Before shipment, O.Acceptance-Test guarantees that the release products meet the required criteria imposed by the client.

在交付资产之前，验收测试保证交付符合客户要求的标准。

T.Attack-Transport

The security measures defined by O.External-Delivery ensure that an attacker cannot get access to sensitive physical or electronic data or items during internal or external shipment. For electronic items, the threat is further countered by the security measures defined by O.Transfer-Data.

外部交付定义的安全措施确保攻击者无法在内部或外部运输期间访问敏感的物理或电子数据或物品。对于电子项目，由数据传输定义的安全措施支持。

Therefore the combination of O.External-Delivery and O.Transfer-Data is sufficient to cover T.Attack-Transport.

因此，外部交付和数据传输的组合足以覆盖运输攻击。

T.Computer-Net

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

安全文档规定了站点的所有安全措施，因此是站点对抗所有资产攻击的基础。

The logical security measures defined by O.Logical-Access prevent an attacker from unauthorized remote access to sensitive data. The measures defined by O.Logical-Operation ensure that the IT systems are kept up-to-date and ensure backups integrity, availability, and confidentiality.

逻辑访问定义的逻辑安全措施可防止攻击者对敏感数据进行未经授权的远程访问。逻辑操作定义的措施确保 IT 系统保持最新状态，从而确保逻辑访问定义的安全措施持续提供足够的安全级别。这得到了内部监控和维护安全的支持。

O.Internal-Monitor ensures the periodic review of suitability/adequacy of the current protection mechanisms and their correct implementation and operation.

内部监控确保定期审查当前安全机制与其正确实施执行的适宜性和充分性。

O.Maintain-Security requires the security checks to ensure the integrity and availability of the security mechanisms.

安全维护要求对安全机制进行检查确保其完整性和可行性。

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills to maintain the integrity and confidentiality of the TOE (or its parts) by the correct operation of the security measures/procedures established at the site.

员工参与定义的措施确保接触敏感物品的员工具备必要的技能，通过正确实施安全措施/程序维护 TOE 或其组件的完整性和机密性。

Therefore the combination of O.Security-Documentation, O.Logical-Access, O.Logical-Operation, O.Internal-Monitor, O.Maintain-Security and O.Staff-Engagement are sufficient to cover T.Computer-Net.

因此，安全文档、逻辑访问、逻辑操作、内部监控、维护安全和工作人员参与的结合足以覆盖计算机网络。

T.Smart-Theft and T.Rugged-Theft

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to the assets of the site.

安全文档规定了站点的所有安全措施，因此是站点对抗所有资产攻击的基础。

The site is protected with the measures defined by O.Physical-Access preventing the unauthorized access to the developer facilities. Procedures and measures defined by O.Security-Control ensures the correct operation of access control mechanisms supporting the physical security.

现场采用物理访问规定的措施进行保护，防止入侵者进入设施。安全控制规定的程序和措施确保支持物理安全机制的正确运行。

O.Internal-Monitor ensures the periodic review of suitability/adequacy of the current protection mechanisms and their correct implementation and operation.

内部监控规定了对当前保护机制的适用性及其正确实施和执行的定期审查，安全维护规定了确保安全机制完整性的检查。

O.Maintain-Security requires the security checks to ensure the integrity and availability of the security mechanisms.

安全维护要求对安全机制进行检查确保其完整性和可行性。

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have a sufficient amount of time to succeed the attack without being noticed by the security protection supporting forces. The facilities resistance time must exceed the reaction time of the security forces.

警报响应确保在发生入侵时，在不触发缓解攻击的响应下，入侵者将没有时间完成攻击。Therefore the combination of O.Security-Documentation, O.Physical-Access, O.Security-Control, O.Alarm-Response, O.Internal-Monitor and O.Maintain-Security are sufficient to cover T.Smart-Theft and T.Rugged-Theft.

因此，安全文档、物理访问、安全控制、报警响应、内部监控和安全维护的结合足以涵盖智能盗窃

T.Staff-Collusion

O.Security-Documentation specifies all security measures of the site and is therefore the very basis to counter all attacks to protect the assets of the site.

安全文档规定了站点的所有安全措施，因此是站点对抗所有资产攻击的基础。

The measures defined by O.Staff-Engagement ensure that staff with access to sensitive items has the required skills to ensure integrity and confidentiality of the items, and to understand the risks and liabilities of supporting an external/internal attacker or acting as an attacker.

员工参与定义的措施确保接触敏感物品的员工具备必要的技能，通过正确实施安全措施/程序维护 TOE 或其组件的完整性和机密性。

It is ensured that the required security level of the site is maintained at all times by the security measures defined in O.Internal-Monitor and O.Maintain-Security including background checks during the hiring process and security procedures for the terminated employees (e.g., deactivation of the user accounts, the user access rights revocation). 通过内部监控和安全维护中规定的安全措施，

包括雇佣人员期间的背景调查和被解雇员工的离职程序（如账户停用），确保现场的安全级别始终保持不变。

O.Transfer-Data ensures the integrity and confidentiality of sensitive data during transfer.

数据传输确保了敏感数据传输过程中的安全性。

The security measures defined by O.Control-Scrap ensure that an attacker cannot get access to sensitive data from the scrap.

废料控制定义的安全措施可确保攻击者在站点不再需要敏感数据时无法访问这些数据。

Therefore the combination of O.Security-Documentation, O.Internal-Monitor, O.Maintain-Security, O.Staff-Engagement, O.Transfer-Data and O.Control-Scrap are sufficient to cover T.Staff-Collusion.

因此，安全文件、内部监控、安全维护、员工参与、数据传输和报废控制的结合足以涵盖工作人员串通。

T.Unauthorized-Staff

By measures defined by O.Logical-Access and O.Physical-Access, unauthorized staff cannot access any sensitive assets. The threat is further countered by the additional physical and logical security measures defined by O.Security-Control, O.Logical-Operation and O.Internal-Monitor and O.Maintain-Security.

根据逻辑访问和物理访问定义的措施，未经授权的员工不能访问任何资产。措施通过定义的安全控制、逻辑操作和内部监控措施保持有效，同时通过安全维护定期评估其有效性。

O.Security-Documentation specifies all security measures of the site, and therefore, is the very basis to counter all attacks to protect the assets of the site.

安全文档规定了站点的所有安全措施，因此是站点对抗所有资产攻击的基础。

O.Alarm-Response ensures that in the event of an intrusion, the intruder will not have a sufficient amount of time to succeed the attack without being noticed by the security protection supporting forces. The facilities resistance time must exceed the reaction time of the security forces.

警报响应确保在发生入侵事件时，入侵者在不被安保措施发现的情况下也没有足够的时间成功实施攻击，设施的抵御时间长于安保人员的响应时间。

Staff attempting to deliberately or by mistake access the sensitive assets for which no authorization is granted, will be detected and prevented by the security measures defined by O.Internal-Monitor, and O.Zero-Balance. O.Staff-Engagement requires staff to be vigilant and repot any abnormal behaviors or situations.

员工试图(有意或无意)访问未授权的资产，内部监控将在访问之前检测到，或通过零平衡定义的措施阻止。其他工作人员的合作可能是必要的，并由工作人员参与来执行。

Rejected assets will be collected before leaving the facilities where the access is controlled and returned to the client, by measures defined in O.Control-Scrap.

通过废料控制中定义的措施被拒收的资产在离开受控设施前收集并且返还给客户端。

P.Accept-Product

O.Acceptance-Test directly enforces the policy for which the products are released only when quality criteria defined by the client is satisfied.

通过验收测试定义的目标直接强制执行只有在满足客户定义的标准时才发布产品的政策。

O.Config-Control and O.Config-Process contribute to the product quality acceptance framework necessary to enforce the policy.

配置控制和配置过程都有助于实现策略所需的验收准则。

P.Config-Control

Objective O.Config-Control directly enforces the policy as all the production processes are explicitly tailored for each client. O.Config-Items, O.Config-Process, O.Reception-Control and O.Logical-Access define the additional security measures and procedures to enforce the policy.

配置控制直接执行目标政策，因为所有的流程都是为此目的明确定制的。配置控制的实施由定义为满足配置项、配置过程、接收控制和逻辑访问的措施和程序支持。

P.Config-Items

Objective O.Config-Items directly enforces the policy as all the configuration items are explicitly tailored for each client. O.Reception-Control defines the additional security procedures to enforce the policy.

配置项直接执行策略，因为所有的过程都是为此目的明确定制的。配置项的执行是由满足接收控制的程序支持的。

P.Config-Process

O.Config-Process directly enforces the policy as it defines all the security procedures and measures (CM plan) used during the production process.

所有服务定义、程序和内部相关文件均由 CM 系统管理，并遵循 CM 管理计划。

P.Organize-Product

O.Config-Process ensures that a configuration management plan is in place.

配置过程确保配置管理计划到位。

O.Config-Control ensures that the configuration management plan is applied and followed during the production process.

配置控制确保生产过程中应用及遵循配置管理计划。

O.Logical-Access and O.Logical-Operation provide the necessary security measures to protect sensitive items from an unauthorized access or modifications.

逻辑访问和逻辑操作为阻止对敏感项目的未授权访问或修改提供了必要的安全措施。

P.Product-Transport

O.External-Delivery ensures a secure external transportation of the release products. O.Transfer-Data ensures secure transfer of sensitive electronic data items. O.Config-Items ensures the correct labelling of the product.

产品运输直接由外部发货的外部交付和敏感电子配置项目的传输数据强制执行。配置项目支持这种强制执行以确保标签正确。

P.Reception-Control

O.Reception-Control ensures that the reception procedures for the secure products are applied and followed.

为满足接收控制而定义的程序直接执行接收控制政策。

P.Zero-Balance

O.Zero-Balance and O.Control-Scrap ensure that no sensitive items loss occurring during production and shipment. Besides, O.Internal-Monitor and O.Staff-Engagement further contribute to the policy enforcement by defining additional security measures and procedures for the access control and staff awareness.

零平衡是通过零平衡和废料控制来执行的，它确保不会发生意外的丢失或遗留物品。此外，内部监督和员工参与也有助于这一政策。

P.Flaw-Remediation

O.Flaw-Remediation ensures that a formal security flaw handling procedure is in place.

缺陷修复是由修复缺陷来实现的，以确保有正式的安全缺陷处理程序。

PUBLIC

6 扩展保证组件定义 Extended Assurance Components Definition

No extended components are defined in this Site Security Target.

在此站点安全目标中没有定义任何扩展组件。

PUBLIC

7 安全保障要求 Security Assurance Requirements

The Security Assurance Requirements (SAR) for this Site Security Target are derived from the ALC (Life-cycle support) assurance class as follows:

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

本 SST 中的安全保证要求（SAR）来源于 ALC（生命周期支持）的保证类别：

- ALC_CMC.5 (CM 能力)
- ALC_CMS.5 (CM 范围)
- ALC_DVS.2 (开发安全)
- ALC_LCD.1 (生命周期定义)
- ALC_FLR.1 (缺陷修复)

The ALC-SARs listed above are described in CC Part 3 (3) and fulfil Minimum Site Requirements (5).

以上列出的 ALC-SARs 在 CC Part 3 中描述并满足最低站点要求 (5)。

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

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

ALC_CMS.5: None

ALC_DVS.2: None

ALC_LCD.1: None

ALC_FLR.1: None

上述保证要求的相关关系如下：

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

ALC_CMS.5: 无

ALC_DVS.2: 无

ALC_LCD.1：无

ALC_FLR.1：无

The dependency ALC_CMS.1 is satisfied by inclusion of the hierarchically higher assurance component ALC_CMS.5.

The dependency ALC_LCD.1 is partially fulfilled because the site does not cover the whole life cycle of the TOE development. For this site, only the Phase 4 (IC Packaging) (1) are relevant.

7.1 应用说明和改进 Application Notes and Refinements

7.1.1 CM 功能概述 Overview regarding CM capabilities (ALC_CMC)

A production control system is employed to guarantee the traceability and completeness of different production charges or lots. The chip lots, production serial number, client part ID, production quantity, defective products quantity, operators, production progress, serial number of production machines, working time of operators, usage of raw materials, etc. is tracked by this system. Appropriate administration procedures are implemented for managing wafers, dice and/or packaged products, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It is ensured, that wafers, dice or assembled chip removed from the production stage that are not functional will be delivered to the client instead of destruction.

采用生产控制系统，保证不同生产指令或批次的可追溯性和完整性。该系统对芯片批号、生产序列号、客户零件 ID、生产数量、次品数量、操作人员、生产进度、生产机器序列号、操作人员工作时间、原材料使用情况等进行跟踪。实施适当的管理程序来管理从生产过程中移除的晶圆、晶片和/或包装产品，以验证和控制预定义的质量标准和生产参数。确保从生产阶段移除的不能正常工作的晶圆、晶片或组装芯片将被交付给客户，而不是销毁。

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

用于评估站点的程序和描述的配置控制和已定义的变更过程是强制性的。控制过程必须包括对评估的生产过程以及现场安全措施有影响的所有程序。

The life-cycle described in (1) is a complex production process. Only parts of this production process are normally provided at a specific site. In such a case the control of the product during such a production process must include sufficient verification steps to ensure the specified and expected result. Test procedures, verification procedures and the associated expected results must be under configuration management for these cases.

(1)中描述的生命周期是一个复杂的生产过程。通常只有部分生产过程在特定的地点提供。在这种情况下，在这种生产过程中对产品的控制必须包括足够的验证步骤，以确保规定和预期的结果。对于这些情况，测试程序、验证程序和相关预期结果必须处于配置管理之下。

The configuration items for the considered product type are listed in section 4.1. The CM documentation of the site must be able to maintain the items listed for the relevant life-cycle step and the CM system must be able to track the configuration items.

所顾及的产品类型的配置项请参见 4.1。现场的 CM 文档必须能够维护相关生命周期步骤中列出的项目，并且 CM 系统必须能够跟踪配置项目。

A CM system has to be employed to guarantee the traceability and completeness of different production charges or lots. Appropriate administration procedures have to be provided in order to maintain the integrity and confidentiality of the configuration items.

必须采用 CM 系统来保证不同生产指令或批次的可追溯性和完整性。必须提供适当的管理程序，以保持配置项的完整性和机密性。

7.1.2 CM 范围概述 Overview regarding CM Scope (ALC_CMS)

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

站点认证过程的配置列表的范围仅限于与声明的生命周期 SAR 和在站点处理的配置项的 SAR 相关的文档。

Process control data, test data and related procedures and programs can be in the scope of the configuration management.

在配置管理的范围可以包含过程控制数据、测试数据和相关程序和程序。

7.1.3 开发安全概述 Overview regarding Development Security (ALC_DVS)

The CC assurance components of family ALC_DVS refer to the “development environment”, 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.

ALC_DVS 系列的 CC 保证组件指的是“开发环境”、“TOE”或“TOE 设计和实施”。ALC_DVS.2 部分“安全措施的充分性”要求提供安全措施适用性的额外证据。

The intended TOE Manufacturer must ensure that the development and production of the intended TOE is secure so that no information is unintentionally made available for the operational phase of the intended TOE. The confidentiality and integrity of design information, test data and configuration data must be guaranteed, access to any kind of samples (client’s specific samples or open samples) development tools and other material must be restricted to authorized persons only, and scrap must be controlled and returned.

TOE 制造商必须确保 TOE 的开发和生产是安全的，这样就不会无意中为 TOE 的运行阶段提供任何信息。必须保证设计信息、测试数据和配置数据的机密性和完整性，任何类型的样品（客户的特定样品或开放样品）开发工具和其他材料的访问必须仅限于授权人员，并且必须控制和退回废料。

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

基于这些要求，现场的物理安全性和逻辑安全性是评估的重点。除了单纯实施安全措施外，还必须考虑对安全措施的控制和维护。

If the transfer of configuration items between two lanes involved in the production flow is included in the scope of the evaluation (life-cycle covered by the product evaluation) this is considered as internal transportation. In general, the security requirements for confidentiality and integrity are the same but it must clearly distinguish to ensure the correct subject of the evaluation.

如果生产过程中涉及评估范围内（产品评估所涵盖的生命周期）两条线路之间的配置项目转移，则被认定为内部转运。一般来说，保密性和完整性的安全要求是相同的，但必须明确区分，以确保正确的评估主体。

7.1.4 生命周期定义概述 Overview regarding Life-Cycle Definition (ALC_LCD)

The site is not equal to the entire development environment. Therefore, the ALC_LCD criteria are interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site. The PP (1) provides a life-cycle description there, specific life-cycles steps can be assigned to the tasks at site. This may comprise a change of the life-cycle state if e.g. testing or initialization is performed at the site or not.

该站点并不等于整个开发环境。因此，ALC_LCD 标准的解释方式是，只需评估现场范围内的生命周期阶段。PP (1)提供了生命周期描述，可以在现场为任务分配特定的生命周期步骤。这可能包括改变生命周期状态，例如是否在现场进行测试或初始化。

The PP (1) does not include any refinements for ALC_LCD. The products are assembled and delivered to the client. The defective products are also returned to the client.

PP (1)不包括对 ALC_LCD 的任何改进。产品组装完成后交付给客户。不合格的产品也被退回给客户。

For this site, only the phase 3 'IC Packaging' is relevant.

本站点只有“IC 封装”阶段与生命周期是相关的。

7.1.5 缺陷修复概述 Overview regarding Flaw Remediation (ALC_FLR)

Since this site is a production site and the finished good is not in a status that can be delivered to the end user of intended TOE. Therefore, the flaw remediation procedure mentioned across this SST is focus on the service provided to the finished good receiver, normally it is the client who sends the sawn wafer or wafer to this site. The intent of the flaw remediation procedure is to collect security flaw reported by client or reported internally and handle it with predefined way.

由于该站点是生产站点，并且成品不处于可以交付给最终意向 TOE 用户的状态。因此，本 SST 中提到的缺陷修复程序是针对成品接收方提供的服务，通常是客户将已减划和未减划的晶圆发送到该站点。缺陷修复程序的目的是收集客户报告或内部报告的安全缺陷，并以预定义的方式进行处理。

7.2 安全保障原理 Security Assurance Rationale

The security assurance requirements rationale maps the content elements of the selected assurance components of (3) to the security objectives defined in this Site Security Target.

The site has a process in place to ensure an appropriate and consistent identification of the products.

安全保证需求基本原理将 (3)中选定的保证组件的内容元素映射到本站点安全目标中定义的安全目标。

现场有一个流程，以确保对产品进行适当和一致的标识。

Application Note for ALC requirements in terms of Site Certification:[1]

1. In the scope of Site Certification, the term “TOE” shall be understood as an “intermediate product”, “incomplete product”, or “non-final TOE” since the TOE itself is not the subject of evaluation. The term “product” can be used interchangeably with the term “TOE” depending on the context relevance.
2. Since the TOE is not directly in the focus of Site Certification, certain TOE requirements (SARs) cannot be applied to the site in the way they are written. Therefore, such SARs will be refined in this document as follows:
    a. ~~exclusion of some parts of the requirement which are not applicable to site~~,[2]
    b. *inclusion of some parts into the requirement which are applicable to site*,[3] and
    c. new requirement which is applicable to site.[4]

7.2.1 ALC_CMC.5 的基本原理 Rationale for ALC_CMC.5

SAR	Security Objective	Rationale
ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling. CM 文件应表明具备确保适当和一致的标签的过程。	O.Config-Items 配置项目	All products assembled at HPCZ get a unique production serial number generated by a database as defined by O.Config-Items, which is linked to the client part ID. 所有在 HPCZ 组装的产品都得到一个唯一的生产序列号，该序列号由配置项目定义的数据库生成，该数据库链接到客户端部件 ID。
ALC_CMC.5.2C The CM documentation shall describe the method used to uniquely identify the configuration items. CM 文档应描述用于唯一标识配置项的方法。	O.Reception-Control 接收控制 O.Config-Items 配置项目 O.Config-Control 配置控制 O.Config-Process	Incoming inspection are based on O.Reception-Control product identification that ensures associated labelling. 进料检验是基于接收控制确保相关标签的产品标识。 Labelling is mapped to the internal identification as defined by O.Config-Items. This ensures the unique identification of security products.

[1] Application Note shall be applied to the whole document, whenever suitable in the specified context.
[2] ~~Strikethrough~~
[3] *Italic*
[4] Underline

	配置过程	标签映射到配置项定义的内部标识。这确保了安全产品的唯一标识。 O.Config-Control ensures that each client part ID is released based on a defined process. This includes changes that are related to a client part ID. The configurations can only be done by authorized person. 配置控制确保每个客户端部件 ID 都是根据定义的过程发布的。这包括与客户端部件 ID 相关的更改。配置只能由授权人员完成。 O.Config-Process provides a configured and controlled production process. 配置过程提供了一个配置的和受控的生产过程。
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. 配置管理文件应证明验收过程提供了对所有配置项变更的充分和适当的评审	O.Config-Process 配置过程 O.Config-Control 配置控制	O.Config-Process and O.Config-Control ensure that only authorized staff can apply changes based on a defined process. This comprises changes related to process flows, procedures and items of clients. Teams are defined to assess and release changes. 配置过程确保只有授权人员才能应用更改。这包括与客户的流程、程序和项目相关的变更。定义了团队来评估和发布变更。
ALC_CMC.5.4C The CM system shall uniquely identify all configuration items. CM 系统所有配置项应具备唯一标识。	O.Reception-Control 接收控制 O.Config-Items 配置项目 O.Config-Control 配置控制 O.Config-Process 配置过程	O.Reception-Control includes the incoming labelling and the mapping to internal identifications. 接收控制包括输入标签和到内部标识的映射。 O.Config-Items includes the internal unique identification of all items that belongs to a client part ID. 配置项包括属于客户端部件 ID 的所有项的内部唯一标识 O.Config-Control ensures the ID assignment of all configuration items is supported by automated tracking systems. 配置控制确保了自动跟踪系统支持的所有配置项之间的分配 O.Config-Process provides a configured and controlled production process. 配置过程提供了一个配置的和受控的生产过程。

ALC_CMC.5.5C The CM system shall provide automated measures such that only authorized changes are made to the configuration items. CM 系统应提供自动化措施，以便只对配置项目进行经授权的更改	O.Config-Control 配置控制 O.Config-Process 配置过程 O.Logical-Access 逻辑访问 O.Logical-Operation 逻辑操作	According to O.Config-Control an automated system is in place to map the configuration items to a unique job number. 根据配置控制，一个自动系统将配置项映射到一个唯一的作业号 Changes can only be applied by authorized personal as described by O.Config-Process. 变更只能由.配置流程所述的授权人员应用。 O.Logical-Access and O.Logical-Operation support the control by limiting the access and ensuring the correct operations for all tasks to the authorized staff. 通过限制访问并确保授权人员对所有任务的正确操作来支持控制逻辑访问和逻辑操作。
ALC_CMC.5.6C The CM system shall support the production of the TOE by automated means. CM 系统应支持通过自动化方式进行的产品生产。	O.Config-Control 配置控制 O.Zero-Balance 零平衡 O.Acceptance-Test 验收测试	O.Config-Control comprises an automated system that ensures the unique mapping between configuration items and the tracking of the different production steps. 配置控制包括一个自动化系统，以确保配置项之间的唯一映射和跟踪不同的生产步骤。 O.Zero-Balance ensures that the number of produces modules complies with the sum of the delivered modules and the scrap modules. 零平衡确保生产模块的数量符合交付模块和报废模块的总和。 O.Acceptance-Test ensures the released product meet the requirements imposed by client. 验收测试，确保发布的产品满足客户规定的要求。
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. CM 系统应确保负责接受配置项目的人不是开发配置项目的人。	O.Config-Process 配置过程 O.Reception-Control 接收控制	The management of the production environment and the different steps is assigned to different teams as described by O.Config-Process. 生产环境和不同步骤的管理分配给不同的团队，如配置过程. O.Reception-Control includes the incoming labelling and the mapping to internal identifications. 接收控制包括输入标签和到内部标识的映射。

PUBLIC

ALC_CMC.5.8C The CM system shall *clearly* identify the configuration items that comprise the TSF. CM 系统应识别组成 TSF 的配置项。	O.Reception-Control 接收控制 O.Config-Items 配置项目 O.Config-Control 配置管理 O.Config-Process 配置过程	Since there is no specific TOE in the main focus of the site certification. Evaluator should only select such kind of configuration items which are in the scope of the certified site like CM tools/documentation or development tools for example, which is nearly the same as ALC_CMC.5.4C. 由于站点认证没有特定的 TOE。评估人员应仅选择认证站点范围内的此类配置项目，例如 CM 工具/文档或开发工具，这与 ALC_CMC.5.4C 几乎相同。 O.Reception-Control includes the incoming labelling and the mapping to internal identifications. 接收控制包括输入标签和到内部标识的映射。 O.Config-Items includes the internal unique identification of all items that belongs to a client part ID. 配置项目包括属于客户端部件 ID 的所有项目的内部唯一标识。 O.Config-Control ensures the ID assignment of all configuration items is supported by automated tracking systems. 配置控制确保自动跟踪系统支持的所有配置项之间的分配。 O.Config-Process provides a configured and controlled production process. 配置过程提供了一个配置的和受控的生产过程。
ALC_CMC.5.9C The CM system shall support the audit of all changes to the TOE by automated means, including the originator, date, and time in the audit trail. CM 系统应支持通过自动化的方式对配置项的所有变更进行审核，包括审核跟踪中的发起者、日期和时间。	O.Config-Control 配置控制	The automated production control covered by O.Config-Control comprises the logging of all production steps and thereby includes the required audit trail including the originator. 配置控制涵盖的自动化生产控制包括所有生产步骤的日志记录，从而包括所需的审计跟踪，包括发起人。
ALC_CMC.5.10C	O.Config-Control 配置控制	O.Reception-Control comprises the control of the incoming configuration items.

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. CM 系统应提供一种自动的方法来识别受给定变更影响的所有其他配置项目	O.Config-Items 配置项 O.Config-Process 配置过程 O.Reception-Control 接收控制	接收控制包括对传入的配置项的控制。 O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. 配置项和配置控制涵盖了客户配置项目的独特标记和管理。 O.Config-Process ensures that only controlled changes are applied. 配置过程确保只应用受控的更改。
ALC_CMC.5.11C The CM system shall be able to identify the version of the implementation representation from which the TOE is generated. CM 系统应能够识别出产品产生的所有生产相关数据。	O.Reception-Control 接收控制 O.Config-Items 配置项目 O.Config-Control 配置管理 O.Config-Process 配置过程	O.Reception-Control comprises the control of the incoming configuration items. 接收控制包括对传入的配置项的控制。 O.Config-Items and O.Config-Control cover the unique labelling and management of the client configuration items. 配置项和配置控制涵盖了客户配置项目的独特标记和管理。 O.Config-Process ensures that only controlled changes are applied. 配置过程确保只应用受控的更改。
ALC_CMC.5.12C The CM documentation shall include a CM plan. 配置管理文件应包括配置管理计划。	O.Config-Control 配置控制 O.Config-Process 配置过程	According to O.Config-Control, the setup of each client part ID includes an associated CM plan including the release. 根据配置控制，每个客户端部件 ID 的设置包括包括发布的相关 CM 计划。 O.Config-Process ensures the reliability of the processes and tools based on dedicated CM plans. 配置过程确保了基于专用 CM 计划的流程和工具的可靠性。
ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE. CM 计划应描述 CM 系统如何用于开发产品。	O.Config-Control 配置控制 O.Config-Process 配置过程	O.Config-Control describes the management of the client part IDs at the site. 配置控制描述了在站点上对客户端部件 ID 的管理。 According to O.Config-Process, the CM plans describe the services provided by the site. 根据配置过程，CM 计划描述了站点提供的服务。

ALC_CMC.5.14C The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE. 配置管理计划应描述用于接受已修改或新创建的配置项作为产品一部分的过程。	O.Reception-Control 接收控制 O.Config-Items 配置项目 O.Config-Process 配置过程	O.Reception-Control supports the identification of configuration items at HPCZ. 接收控制支持识别 HPCZ 的配置项目。 O.Config-Items ensures the unique identification of each product is supported by the client part ID. 配置项确保在 HPCZ 测试的每个产品都能通过客户的零件 ID 进行独特的识别。 O.Config-Process ensures the automated control of released products. 配置过程确保对已发布产品的自动控制。
ALC_CMC.5.15C The evidence shall demonstrate that all configuration items *have been and* are being maintained under the CM system. 证据应证明所有配置项目都在 CM 系统下得到维护。	O.Reception-Control 接收控制 O.Config-Control 配置控制 O.Config-Process 配置过程 O.Zero-Balance 零平衡	The objectives O.Reception-Control, O.Config-Control, O.Config-Process ensure that only released client part IDs are produced. 目标接收控制，配置控制，配置过程确保只产生已释放的客户端部件 id。 This is supported by O.Zero-Balance ensuring the tracing of all security products. 这是由零平衡所支持的，以确保对所有安全产品的跟踪。
ALC_CMC.5.16C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan. 证据应证明所有配置项目都在 CM 系统下得到维护。	O.Config-Control 配置控制 O.Config-Process 配置过程 O.Acceptance-Test 验收测试 O.External-Delivery 外部运输 O.Zero-Balance 零平衡	O.Config-Control includes a release procedure as evidence. 配置控制包括作为证据的发布程序。 O.Config-Process ensures the compliance of the process. 配置过程确保遵守了这个程序。 O.Acceptance-Test comprises the control of all finished products ID. Since the finished products are returned to the client according to O.External-Delivery at least the labelling is controlled by the client. 验收测试包括控制所有成品部件的 ID。由于成品是根据外部交货返回给客户的，所以客户至少控制标签。 O.Zero-Balance ensures that the number of produced modules complies with the sum of the delivered modules and the scrap modules.

		零平衡确保生产模块的数量符合交付的模块和报废模块的总和。

TABLE 3 RATIONALE FOR ALC_CMC.5

7.2.2 ALC_CMS.5 的基本原理 Rationale for ALC_CMS.5

SAR	Security Objective	Rationale
ALC_CMS.5.1C The configuration list includes 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 *production* tools and related information. 配置清单应包括以下内容：~~TOE 本身、~~SARs 要求的评估证据、~~TOE 组成部分、实现表示、安全缺陷报告和解决状态以及、~~生产工具和相关信息。	O.Config-Items 配置项 O.Config-Control 配置控制 O.Config-Process 配置过程	Since the process is subject of the evaluation, the TOE itself, the parts that comprise the TOE, the implementation representation, security flaw reports and resolution status are not applicable for a site evaluation. 由于该过程是评估的主题，因此 TOE 本身、组成 TOE 的部分、实现表示、安全缺陷报告和解决状态不适用于站点评估。 O.Config-Items ensure unique part IDs including a list of all items and processes for this part. 配置-项目确保唯一的零件 ID，包括该零件的所有项目和流程的列表。 O.Config-Control describes the release process for each client part ID. 配置控制描述了每个客户端部件 ID 的发布过程。 O.Config-Process defined the configuration control including part IDs. Procedures and processes. 配置过程定义了包括零件 ID 在内的配置控制、程序和流程。
ALC_CMS.5.2C The configuration list shall uniquely identify the configuration items. 配置列表应唯一地识别配置项目。	O.Config-Items 配置项 O.Config-Control 配置控制 O.Config-Process 配置过程 O.Reception-Control 接收控制 O.External-Delivery 外部交付	Items, products and processes are uniquely identified by the database system according to O.Config-Items. 项目、产品和过程由数据库系统根据配置项目进行唯一标识。 Within the production process the unique identification is supported by automated tools according to O.Config-Control and O.Config-Process. 在生产过程中，根据配置控制和配置过程，通过自动化工具支持独特的标识。 The identification of received products is defined by O.Reception-Control.

		接收产品的识别由接收控制系统定义。 The labelling and preparation for the transport is defined by O.External-Delivery. 标签和运输的准备工作由外部交付定义。
ALC_CMS.5.3C The configuration list shall show that a process is in place to ensure that the developer for each configuration item is indicated. 对于每个产品相关的配置项目，配置清单应注明该项目的开发人员。	O.Config-Items 配置项目	HPCZ does not involve subcontractors for the test of security products. According to O.Config-Items all configuration items for secure products are identified. HPCZ 不涉及进行安全产品测试的分包商。根据配置项目-可识别所有安全产品的配置项目。

TABLE 4 RATIONALE FOR ALC_CMS.5

7.2.3 ALC_DVS.2 的基本原理 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 *and provide evidence that these security measures are followed during the development and maintenance of the TOE*. 开发安全文件应描述所有物理的、程序的、人员的和其他的安全措施，这些措施对于保护产品设计的保密性和完整性以及在其开发环境中的实现是必要的，并提供证明TOE开发与维护遵循这些安全措施。	O.Physical-Access 物理访问 O.Security-Control 安全控制 O.Alarm-Response 报警响应 O.Logical-Access 逻辑访问 O.Logical-Operation 逻辑操作 O.Staff-Engagement 员工参与 O.Maintain-Security 安全维护 O.Control-Scrap 报废控制 O.External-Delivery 外部交付 O.Security-Documentation 安全文档 O.Transfer-Data 数据传输	The physical protection is provided by O.Physical-Access, supported by O.Security-Control, O.Alarm-Response, and O.Maintain-Security. 物理保护是由物理访问提供的，由安全控制、报警响应和维护安全支持。 The logical protection of data and the configuration management is provided by O.Logical-Access and O.Logical-Operation. 数据的逻辑保护和配置管理是由 "逻辑访问 "和 "逻辑操作 "提供的。 The personnel security measures are provided by O.Staff-Engagement. 人员安全措施由员工参与提供。 Any scrap that may support an attacker is controlled according to O.Control-Scrap. 任何可能支持入侵者的废料都要根据废料控制进行控制。 Secure physical delivery between different sites is controlled by O.External-Delivery. 不同站点之间的安全物理交付由外部交付控制。 O.Security-Documentation ensures the security related documentation control. 安全文档确保与安全相关的文档控制。 O.Transfer-Data is intended to secure the data transmission. 数据传输旨在确保数据传输的安全。

		The evaluator should get evidence that the security measures stated in the development documentation are followed can be achieved while performing a site visit which is handled by ALC_DVS.2.2E. 评估人员应获得证据，说明在执行由 ALC_DVS.2.2E 处理的现场访问时，遵循开发文档中所述的安全措施。
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. 开发安全文件应证明安全措施提供了必要的保护，以保持TOE的保密性和完整性。	O.Physical-Access 物理访问 O.Security-Control 安全控制 O.Alarm-Response 报警响应 O.Logical-Access 逻辑访问 O.Logical-Operation 逻辑操作 O.Staff-Engagement 员工参与 O.Control-Scrap 报废控制 O.Internal-Monitor 内部监控 O.Zero-Balance 零平衡 O.Acceptance-Test 验收测试 O.Reception-Control 接收控制 O.Maintain-Security 安全维护 O.Security-Documentation 安全文档 O.Transfer-Data 数据传输 O.External-Delivery 外部交付	The security measures described above under ALC_DVS.2.1C are commonly regarded as effective protection if they are correctly implemented and enforced. The security measure defined by O.Acceptance-Test, O.Reception-Control and O.Zero-Balance guarantees that certain procedures are followed to control the incoming and outgoing of configuration items. O.Internal-Monitor ensures the periodic review of suitability/adequacy of the current protection mechanisms and their correct implementation and operation. The associated control and continuous justification are subject of the objectives as there is not necessarily an intended TOE evaluation running the evidence needed may be taken previous TOE/product developments. 上述 ALC_DVS.2.1C 项下的安全措施如果得到正确实施和执行，通常被视为有效的保护。关联控制和持续的论证是目标的主体，因为不一定有预期的 TOE 评估，运行所需的证据可能是之前的 TOE/产品开发。

TABLE 5 RATIONALE FOR ALC_DVS.2

7.2.4 ALC_LCD.1 的基本原理 Rationale for ALC_LCD.1

SAR	Security Objective	Rationale
ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE. 生命周期定义文件应描述用于开发和维护 TOE 的模式。	O.Config-Control 配置控制 O.Config-Process 配置程序	The process used for identification and manufacturing are covered by O.Config-Control and O.Config-Process. 用于识别和制造的过程包含在配置控制和配置过程中。
ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE. 生命周期模型应提供对产品开发和维护的必要的控制。	O.Acceptance-Test 验收测试 O.Config-Process 配置过程 O.Zero-Balance 零平衡	The site does not perform development tasks. The applied production process is controlled by automated means according to O.Config-Process, the finished products are tested according to O.Acceptance-Test and all security products are traced by automated means according to O.Zero-Balance, and/or the four-eye principle (where applicable) is applied. 该站点不执行开发任务。应用的生产过程按配置过程进行控制，完成的客户部件按验收测试进行测试，所有安全产品按零平衡进行跟踪。

TABLE 6 RATIONALE FOR ALC_LCD.1

7.2.5 ALC_FLR.1 的基本原理 Rationale for ALC_FLR.1

SAR	Security Objective	Rationale
ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. 缺陷修复程序文件应描述用于跟踪 TOE 的每个版本中所有报告的安全缺陷的程序。	O.Flaw-Remediation 缺陷修复	The procedures are established by O.Flaw-Remediation. 这些程序是由缺陷修复制定的。
ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each	O.Flaw-Remediation 缺陷修复	The description of the nature, effect of each security flaw, as well as the status of finding a correction to that flaw can be fulfilled by the establishment of O.Flaw-Remediation.

security flaw be provided, as well as the status of finding a correction to that flaw. 缺陷补救程序应要求提供对每个安全缺陷的性质和影响的描述，以及对该缺陷进行纠正的情况		对每个安全缺陷的性质、效果的描述，以及发现纠正该缺陷的状态，可以通过建立缺-修复来实现。
ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. 缺陷补救程序应要求针对每个安全缺陷确定纠正措施。	O.Flaw-Remediation 缺陷修复	Corrective actions can be identified by the establishment of O.Flaw-Remediation. 可以通过建立缺陷修复来确定纠正措施。
ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. 缺陷修复程序文件应描述用于向 TOE 用户提供提供缺陷信息、纠正和指导纠正行动的方法。	O.Flaw-Remediation 缺陷修复	O.Flaw-Remediation established the procedures describing methods to provide flaw information, corrections and guidance. 缺陷修复确立了描述提供缺陷信息、纠正和指导方法的程序。

TABLE 7 RATIONALE FOR ALC_FLR.1

8 站点规范摘要 Site Summary Specification

8.1 站点所需的先决条件 Preconditions Required by the Site

The main precondition for the design specifications, data preparation and the modules production is a released process technology between the wafer fab and the final client. This comprises the definition of the design specifications as well as parameters and limits for the wafer fabrication. The design specifications are used for the product classification and production process setup.

设计数据准备和模块生产的主要先决条件是晶圆厂和最终客户之间发布的工艺技术。这包括定义需求规格以及生产的晶圆的参数和限制。需求规范独立于产品分类，并固定用于特定的生产过程。

This section provides background information on the assumptions. These assumptions impose the additional requirements on the clients and HPCZ regarding the production process, information and deliverables which are needed to enable the correct product production and delivery under the conditions described in this Site Security Target.

A.Item-Identification: The production configuration items must be properly labelled before delivery to HPCZ to allow the correct identification of the received items.

生产配置项必须在发给 HPCZ 之前进行标记，从而实现签收项的正确识别。

A.Prod_Release: The client provides the sawn wafers or wafers that need to be produced by HPCZ.

客户提供需要加工的已减划或未减划的硅圆给 HPCZ。

A.Prod-Specification: HPCZ provides assembly services for smart cards IC and eSIM IC. The sawn wafers, wafers and lead frames are acceptable as input for the assembly lines. Defective dies on the wafer will be marked by inking or wafer mapping. The finished products (IC packages) shall be labelled before delivery to the client to allow the correct product identification.

HPCZ 为智能 IC 卡和 eSIM IC 提供组装服务。未减划和已减划的硅圆和引线框架可作为装配线的输入。晶片上的缺陷芯片可以通过油墨或比对图进行标记。包装和硅圆在交付给客户之前必须贴上标签，以便进行产品识别。

A.External-Delivery: If specific requirements are needed for the shipment of the final products, the related instructions and cargo/security items, e.g., anti-tampering labels/tapes/boxes, shall be provided by the client.

如果对成品的运输有特殊要求，客户必须提供相关的规格和运输/安全项目，如防篡改标签/胶带/箱子。

A.Product-Integrity: HPCZ will conduct the finished modules testing after the assembly, using electronic tests as well as open and short measurements based on the test parameters, and design specifications provided by the client.

HPCZ 将在组装后使用简单的电性测试进行成品测试，基于客户提供的测试参数、设计规格的开路和短路测试。

8.2 站点的服务 Services of the Site

Reception, identification, registration and storage of materials: It includes raw materials, wafers, sawn wafers, unfinished modules and finished modules. The materials received by HPCZ will be labelled with a unique client part ID (client parts). This part ID is linked to the chips that are assembled in the modules.

对材料的接收、标识、入库登记以及储存：包括原材料、未减划和已减划的硅圆、半成品与成品。HPCZ 收到的材料将标有唯一的客户部件 ID（客户部件）。此零件 ID 与模块中组装的芯片相关联。

Wafer sawing: The received wafers are labelled with client part ID that will keep unchanged across the wafer sawing process.

硅圆减划：接收到的具有客户部件 ID 的硅圆，在整个硅圆减划过程中其保持 ID 不变。

Assembly into modules: The processes for assembly, testing and acceptance are set up at HPCZ according to the specifications (e.g. bond plan, module specification, test specification and packing requirements) provided by the client. Die bond and wire bound is performed in the production area. For the release product, a sample lot is produced at the site.

封装为模块：HPCZ 根据客户提供的规范（如焊接计划、模块规格、测试规范和包装要求）制定组装、测试和验收流程。在生产区进行贴片和焊线。站点进行批量生产以发布样品。

Quality control testing for the incoming raw materials and each production process: There is a quality control procedure used to inspect the incoming materials and the modules under production at each step of the production process.

来料质检以及各工序质量检测：在每个生产过程中，都有质量控制程序用于检验来料和产品。

Electronic testing and visual inspection of finished modules: The complete production specific flow includes an electronic testing of each product as part of the acceptance process. The electronic testing program is performed by HPCZ following the test specifications and electrical parameters provided by the client. The testing program is integrated in the test environment of HPCZ. No sensitive information or data should be included in the tests.

成品电性测试以及目检：作为验收过程的一部分，完整的产品流程包括每个产品的电性测试。HPCZ 根据测试规范和客户提供的电气参数/限值制定电信测试程序。该测试项目被整合到 HPCZ 的测试环境中。在这些测试中不应该包括任何敏感信息。

Warehousing and shipment of finished modules: HPCZ has a standard procedure for packing of finished modules and preparation for shipment using protective materials. If special packing requirements are provided by the client, they are included in the process setup. The client is informed if products are ready for shipment because the transportation time and cost must be planed and covered by the client. The client will be provided with the information such as the shipment details and the express tracking number that are used for the shipment package identification and verification at the reception on the client side.

成品仓储以及发货：HPCZ 有一个关于成品包装和装运准备的标准程序。如果客户提供了特殊的包装要求将被包含在过程设置中。如果产品准备好运输，客户会收到通知，因为运输时间成本必须由客户组织。基于提醒目的，客户将获得诸如发货细节和快递单号等信息，用于在接收产品时进行验证。

Product security flaw collection, verification, correction and corrective action delivery: The intent of the flaw remediation procedure is to collect security flaw reported by client or reported internally and handle it with predefined way.

产品安全漏洞的收集、验证、整改和整改措施的交付：缺陷修复程序的目的是收集客户报告的或内部报告的安全缺陷，并以预定义的方式进行处理。

Scrap recycle and return to customer: Both the defective or rejected products and chips are returned to the client.

废品存储以及其他安全处理：有缺陷或被拒绝的产品和芯片都会返回给客户。

8.3 目标理论依据 Objectives Rationale

The following rationale provides a justification that shows that all threats and organizational security policies are effectively addressed by the security objectives.

The following table shows security objectives cover which threats and OSPs.

以下理由说明，所有的威胁和组织安全政策都是由安全目标有效解决的。下表显示了哪些安全目标涵盖了哪些威胁和 OSPs。

Security Objective	Threats and OSPs
O.Acceptance-Test 验收测试	P.Accept-Product, T.Accidental-Change 接收产品，意外变更
O.Alarm-Response 报警响应	T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff Rugged-Theft, Smart-Theft，未经授权的员工
O.Config-Control 配置控制	P.Config-Control, P.Organize-Product, P.Accept-Product 配置控制，产品组织，产品接收
O.Config-Items 配置项	P.Config-Control, P.Config-Items, P.Product-Transport, T.Accidental-Change 配置控制，配置项，产品运输，意外变更
O.Config-Process 配置过程	P.Accept-Product, P.Config-Control, P.Config-Process, P.Organize-Product, T.Accidental-Change 产品接收，配置控制，配置过程，产品组织，意外变更
O.Control-Scrap 报废控制	P.Zero-Balance, T.Staff-Collusion, T.Unauthorized-Staff 零平衡，员工勾结，未经授权的员工
O.External-Delivery 外部交付	P.Product-Transport, T.Attack-Transport 产品运输，运输攻击
O.Internal-Monitor 内部监控	P.Zero-Balance, T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorized-Staff

	零平衡，计算机网络，Rugged-Theft, Smart-Theft，员工勾结，未经授权的员工
O.Logical-Access 逻辑访问	P.Config-Control, P.Organize-Product, T.Accidental-Change, T.Computer-Net, T.Unauthorized-Staff 配置控制，产品组织，意外变更，计算机网络，未经授权的员工
O.Logical-Operation 逻辑操作	P.Organize-Product, T.Computer-Net, T.Unauthorized-Staff 产品组织，计算机网络，未经授权的员工
O.Maintain-Security 安全维护	T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unauthorized-Staff 计算机网络，Rugged-Theft, Smart-Theft，未经授权的员工
O.Physical-Access 物理访问	T.Accidental-Change, T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff 意外变更，Rugged-Theft, Smart-Theft，未经授权的员工
O.Reception-Control 接收控制	P.Config-Control, P.Config-Items, P.Reception-Control 配置控制，配置项，接收控制
O.Security-Control 安全控制	T.Rugged-Theft, T.Smart-Theft, T.Unauthorized-Staff Rugged-Theft, Smart-Theft，未经授权的员工
O.Security-Documentation 安全文档	T.Computer-Net, T.Rugged-Theft, T.Smart-Theft, T.Staff-Collusion, T.Unautorised-Staff 计算机网络，Rugged-Theft, Smart-Theft，员工勾结，未经授权的员工
O.Staff-Engagement 员工参与	P.Zero-Balance, T.Accidental-Change, T.Computer-Net, T.Staff-Collusion, T.Unauthorized-Staff 零平衡，意外变更，计算机网络，员工勾结，未经授权的员工
O.Transfer-Data 数据传输	P.Product-Transport, T.Attack-Transport, T.Staff-Collusion 产品运输，运输攻击，员工勾结
O.Zero-Balance 零平衡	P.Zero-Balance, T.Accidental-Change, T.Unauthorized-Staff 零平衡，意外变更，未经授权的员工
O.Flaw-Remediation 漏洞修复	P.Flaw-Remediation 漏洞修复

TABLE 7 OBJECTIVES RATIONALE

O.Security-Documentation

The security of the site is maintained according to the site's security documentation covering all physical and logical measures to ensure the security of the site.

These security measures are necessary to prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unautorized-Staff and T.Staff-Collusion.

站点的安全是根据站点的安全文件来维护的，该文件涵盖了确保站点安全的所有物理和逻辑措施。

这些安全措施对于防止 Smart-Theft、Rugged-Theft、计算机网络、未经授权的工作人员和工作人员混淆等威胁是必要的。

O.Physical-Access

The production site is operated by HPCZ. The site is separated into different security levels. The production site is monitored by security staff on duty and surveillance cameras at production times.

The building can only be entered presenting a company badge or visitor's badge to the card readers at the entrance. All employees and visitors have to wear their badges visible at any time.

生产现场由 HPCZ 运营。该站点分为不同的安全级别。生产现场由值班安保人员和生产时的监控摄像头进行监控。

只有向入口处的读卡器出示公司证件或访客证件才能进入大楼。所有员工和访客都必须佩戴随时可见的证件。

The access to the production area is secured by full height turnstile with card readers. Access to the production area requires special permissions. It is ensured by policy that either no staff is present in the production area or at least two staff members are present in the production area. Since production area is 24/7 in operation, this area is never empty of personnel. For delivery of production materials and goods into and from the production area, special entrance systems are used which ensures that only materials can get into the production area or out from the production area, but no person can enter or exit the area via this system.

进入生产区的通道由带有读卡器的全高闸机保护起来。进入生产区需要特殊许可。通过政策确保生产区域没有员工，或者至少有两名员工在生产区域。由于生产区是 7*24，所以这个区域从来没有无人员的情况。为了将生产材料和货物送入和送出生产区，使用了特殊的入口系统，确保只有材料可以进入生产区或从生产区出来，但没有人可以通过该系统进入或离开该区。

All access doors to high secure areas are monitored by surveillance cameras at all times. The outer area of the building is monitored by surveillance cameras. Emergency exits are also monitored by surveillance cameras.

All access attempts at any entrance of all locations named above will be recorded by the security staff.

所有通往高安全区的入口都由监控摄像头监控。大楼的外部区域由监控摄像头进行监控。紧急出口也会通过监控摄像头进行监控。在上述所有地点的任何入口的所有访问尝试都将由保安人员记录。

Smart Card Products which are not in the process of production are stored in a specially secured area (warehouse). The warehouse, which is the primary storage location, is inside the production area. Access to the warehouse is controlled by card readers and special permissions for this area. It is ensured by technical means that at least 2 people are present in the area or no one is present in this area.

不在生产过程中的智能卡产品被储存在一个特别安全的区域（仓库）。仓库是主要的储存地点，位于生产区内部。进入仓库是由读卡器和该区域的特殊权限控制的。通过技术手段确保该区域至少有 2 人在场或无人在场。

These measures prevent access to sensitive areas for any unauthorized person and therefore prevent the threats T.Smart-Theft, T.Rugged-Theft, T.Unauthorized-Staff and T.Accidental-Change.

这些措施防止了任何未经授权的人进入敏感区域，因此也防止了 Smart-Theft, Rugged-Theft、未经授权的工作人员和意外变更的威胁。

O.Security-Control

Trained security staff is in charge of operating all security related systems. This especially holds granting access rights, etc. Visitors are escorted by the security staff or collected by company internal staff from the security staff.

受过培训的安保人员负责操作所有与安保相关的系统。这尤其包括授予访问权等。访客由安保人员护送，或由公司内部人员从安保人员那里接走。

Therefore the threats T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff are addressed by management of the security related systems like the access control system.

因此，Smart-Theft、Rugged-Theft 和未经授权的员工的威胁是通过管理门禁系统等安全相关系统来解决。

O.Alarm-Response

Several alarm and detection sensors are installed to provide a warning system for entering the premises by T.Smart-Theft, T.Rugged-Theft and T.Unauthorized-Staff. Security staff will start to investigate any alarm immediately.

安装了多个报警和探测传感器，为 Smart-Theft、Rugged-Thef 和未经授权的人员进入楼宇提供警告系统。接到警报后，安保人员将立即展开调查。

O.Internal-Monitor

The security manager performs meetings with all security staff on a regular basis. During this meeting, security procedures are reviewed, and corrective actions are initiated (if necessary). In case security

related incident occurred since the last security meeting, they will be addressed. In addition, internal audits are performed on a regular basis to ensure the application of the security measures.

安保经理定期与所有安保人员举行会议。在会议期间，审查安全程序，并启动纠正措施（如有必要）。如果自上次安全会议以来发生了与安全相关的事件，将对其进行处理。此外，还定期进行内部审计，以确保安全措施的实施。

The monitoring and protection of the IT system (including network) is handled by the IT department under supervision of the security manager.

IT 系统（包括网络）的监控和保护由 IT 部门在安全经理的监督下进行。

These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff, T.Staff-Collusion and promote the enforcement of P.Zero-Balance.

这些措施防止了 Smart-Theft、Rugged-Theft、计算机网络、未经授权的员工、员工勾结，并促进了零平衡的实施。

O.Maintain-Security

All security related alarm and detection systems are checked on a regular basis. Logs for building access or site access as well as access to especially secured areas are stored and checked on a regular basis. Network security is monitored permanently by the IT department.

These measures prevent T.Smart-Theft, T.Rugged-Theft, T.Computer-Net, T.Unauthorized-Staff, T.Staff-Collusion.

定期检查所有与安全相关的报警和检测系统。建筑物出入或现场出入以及进入特别安全区域的日志都会定期存储和检查。网络安全由 IT 部门永久监控。

这些措施可以防止 Smart-Theft, Rugged-Thef，计算机网，未经授权的工作人员，工作人员的勾结。

O.Logical-Access

The IT network is logically separated from the outside world by a firewall which ensures that only authorized connections from and to the IT network are possible. The firewall secures the communication between external network with internal network and at the same time manages the internal communication by implementing logical network segmentation.

IT 网络通过防火墙与外部世界进行逻辑隔离，确保只有经过授权的 IT 网络连接才能进行。防火墙确保外部网络与内部网络之间的通信安全，同时通过实施逻辑网络分段来管理内部通信。

Each user has an individual account. To access data on the company's network every user has to authenticate himself by login name and password. Multiple successive failed authentication attempts lead to a blocked account. The number of retries depend on the authentication method.

每个用户都有一个单独的账户。要访问公司网络上的数据，每个用户都必须通过登录名和密码来验证自己。多次连续失败的认证尝试会导致账户被封锁。重试的次数取决于认证方法。

Access rights to all network resources are set according to a need-to-know or need-to-have basis, respectively. Access rights of users who do not need access to a network share any longer (e.g. change of jobs) are revoked. In particular, all accounts of employees who leave the company are deactivated.

对所有网络资源的访问权分别按照需要知道或需要拥有的原则来设置。不再需要访问网络共享的用户（如工作变动）的访问权被撤销。特别是离职员工的所有账户都被停用。

The production network is additionally separated from the rest of HPCZ internal network.

These measures prevent T.Computer-Net, T.Accidental-Change and T.Unauthorized-Staff and support the OSPs P.Config-Control and P.Organize-Product.

生产网络还与 HPCZ 内部的其他部分网络分开。

这些措施可以防止计算机网络、意外变更和未经授权的工作人员，并支持 OSP 的配置控制和组织产品。

O.Logical-Operation

Virus protection and patch management for operating systems and applications shall ensure the correct operation of the systems and prevent the systems from malfunction. They ensure that protective measures of the IT workplaces are up-to-date (virus definitions, security patches of operating system, security patches of programs, etc.). In addition, regular backups are applied to prevent loss of data. Backup media are securely stored protected against unauthorized modification and disclosure.

操作系统和应用程序的病毒保护和补丁管理应确保系统的正确运行，防止系统出现故障。他们确保 IT 工作场所的保护措施是最新的（病毒定义、操作系统的安全补丁、程序的安全补丁等）。此外，还应用定期备份以防止数据丢失。备份介质被安全地存储，防止未经授权的修改和披露。

These measures prevent T.Computer-Net and T.Unauthorized-Staff and support the OSP P.Organize-Product.

这些措施防止了计算机网络和未经授权的工作人员，并支持 OSP 产品组织。

O.Config-Items

All configuration items are identified by a unique version number by the configuration management system. By this method, different products can be identified. By this the threat T.Accidental-Change is countered and the OSPs P.Config-Items, P.Config-Control and P.Product-Transport are addressed.

所有配置项都由配置管理系统的唯一版本号进行标识。通过这种方法，可以识别出不同的产品。通过这种方式，可以抵御 "意外变更 "的威胁，并解决 OSP 的配置项目、配置控制和产品运输问题。

O.Config-Control

The application of released procedures for the setup of the production process for each product and the controlled introduction of changes ensures a production according to clients' specifications.

Procedures for setting up the production process as well as changes to the initial setup are done only by authorized personnel. The production process is supported by automated systems. By this the OSPs P.Organize-Product, P.Accept-Product and P.Config-Control are addressed.

应用已发布的程序来设置每种产品的生产流程，并控制变更的引入，确保生产符合客户的规范。设置生产流程的程序以及对初始设置的更改只能由授权人员完成。生产过程由自动化系统支持。通过此操作，解决了 OSP 组织产品、接受产品和配置控制问题。

O.Config-Process

Configuration items are stored in the configuration management system according to the site's configuration management plan. By this the OSPs P.Accept-Product, P.Config-Control, P.Config-Process and P.Organize-Product are addressed. Because an authorized configuration process is defined, T.Accidental-Change can be addressed in terms of less potential flaw caused by unauthorized operation process.

配置项目根据现场的配置管理计划存储在配置管理系统中。由此，OSP 的产品接受、配置控制、配置过程和产品组织得到了解决。由于定义了授权的配置过程，意外变更可以通过减少未授权操作过程造成的潜在缺陷来解决。

O.Acceptance-Test

On request of the client release tests are performed for the corresponding products. By this the threat T.Accidental-Change is countered and the OSP P.Accept-Product is addressed.

根据客户的要求，将对相应的产品进行发布测试。通过这种方式，应对了意外变更的威胁，并解决了 OSP 接受产品的问题。

O.Staff-Engagement

All employees working at the site and having access to sensitive information or data have to sign a non-disclosure agreement to provide legal liability to protect sensitive information against disclosure. In addition, all employees are trained regarding security to support the security awareness. All employees have to pass a security check before they are hired. These measures prevent T.Accidental-Change, T.Computer-Net, T.Unauthorized-Staff and T.Staff-Collusion. Staff engagement can also facilitate the enforce of OSP P.Zero-Balance.

所有在现场工作并能接触到敏感信息或数据的员工都必须签署一份保密协议，以提供保护敏感信息不被披露的法律责任。此外，所有员工都要接受安全方面的培训，以支持安全意识。所有员工在被雇用前都必须通过安全检查。这些措施可以防止意外变更、计算机网络、未经授权的工作人员和工作人员的混淆。工作人员的参与也可以促进 OSP 零平衡的执行。

O.Zero-Balance

Automated means and/or the application of a 4-eye-principle ensures a continuous tracking of Smart Card Products during the whole production process. By this the OSP P.Zero-Balance is addressed and in addition, the threat T.Accidental-Change and T.Unauthorized-Staff are covered.

自动化手段和/或四眼原则的应用确保了在整个生产过程中对智能卡产品的持续跟踪。通过这种方式来解决 OSP 零平衡的问题，此外还包括意外改变和未经授权的工作人员的威胁。

O.Reception-Control

Upon reception of the incoming materials relevant to production from a different site, the inspection is performed to check the quality of received materials. Identification is performed to assign the internal unique ID to the incoming materials. By this the OSPs P.Config-Control, P.Config-Items and P.Reception-Control are addressed.

在从另一个站点接收到与生产相关的来料后，检查验证接收材料的质量。为来料分配内部唯一的 ID 进行识别。由此，OSP 的配置控制、配置项目和接收控制得到解决。

O.External-Delivery

Security relevant physical items are externally delivered either by security transport (e.g. sealed boxes), in person by company's internal staff or collected by the client or the consumer as long as the security functions of the item are not sufficient to protect itself. Security relevant electronic items are externally shipped using secure communication measures. This might be signed and/or encrypted emails or similar (e.g. SSL secured web portals). This prevents T.Attack-Transport and covers P.Product-Transport.

只要物品的安全功能不足以保护自身，与安全相关的实物可以通过安全运输工具（如密封箱）、公司内部员工亲自或由客户或消费者收集从外部交付。与安全相关的电子物品使用安全通信措施对外运输。这可能是经过签名和/或加密的电子邮件或类似内容（例如 SSL 安全的门户站点）。这可以防止攻击运输，也包括产品运输。

O.Transfer-Data

Sensitive electronic configuration items are protected against modification and/or disclosure by cryptographic means during transfer. Either symmetric means, asymmetric means or password protection are applied (as appropriate). Cryptographic keys and password used for secure communication are sufficiently protected against unauthorized access and disclosure. This prevents T.Staff-Collusion, T.Attack-Transport and covers P.Product-Transport.

在传输过程中，通过加密手段保护敏感电子配置项不受修改和/或披露。采用对称方式、非对称方式或密码保护（视情况而定）。用于安全通信的加密密钥和密码得到充分保护，不会被未经授权的访问和披露。这可以防止员工串通、攻击运输，还包括产品运输。

O.Control-Scrap

At this site, sensitive documentation is destroyed and electronic media is erased.

Scrap (Smart Card modules) is securely sent back to the client in order to avoid any material could be accessible from the personnel in the company. By this, no employee could get uncontrolled access to scrap which might be helpful to support an attack. This prevents T.Unauthorized-Staff, T.Staff-Collusion and covers P.Zero-Balance.

在这个站点，敏感文件被销毁，电子媒体被删除。废料（智能卡模块）被安全地送回客户，以避免公司人员可以获得任何材料。通过这种方式，没有员工可以不受控制地获得可能有助于支持攻击的废料。这可以防止未经授权的员工，员工串通，并覆盖零平衡。

O.Flaw-Remediation

The written procedure and appointed responsible for collecting, tracking and handling any reported security flaw can ensure P.Flaw-Remediation is covered.

负责收集、跟踪和处理任何报告的安全缺陷的书面程序可以确保涵盖缺陷修复。

8.4 SAR 基本原理 SAR Rationale

The Security Assurance Requirements rationale does not explicitly address the developer action elements defined in (3) because they are implicitly included in the content elements. This comprises the provision of the documentation to support the evaluation and the preparation for the site visit. In addition, this includes that the procedures are applied as written and explained in the documentation.

安全保证要求的基本原理没有明确说明 (3)中定义的开发人员行动元素，因为它们隐含地包含在内容元素中。这包括提供文件以支持评估和现场考察的准备工作。此外，这包括以书面形式应用程序，并在文件中进行解释。

8.4.1 ALC_CMC

The security assurance requirements of the assurance component "ALC_CMC.5" are suitable to support the production of complex products due to the formalized acceptance process and the automated production support. This comprises the identification of all configuration items and the automated control and tracking within an industrialized production process. The requirement for authorized changes and separate roles for operation and release support the integrity and confidentiality required for the products. Therefore, this assurance level meets the requirements for the configuration management.

由于正式的验收流程和自动化的生产支持，保证组件“ALC_CMC.5”的安全保证要求适用于支持复杂产品的生产。这包括所有配置项目的识别以及工业化生产过程中的自动控制和跟踪。对授权更改的要求以及操作和发布的独立角色支持产品所需的完整性和保密性。因此，该保证级别满足了配置管理的要求。

8.4.2 ALC_CMS

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

所选择的保证体系 "CM 范围 "的 ALC_CMS.5 保证级别支持对生产和测试环境的控制。这包括与产品有关的文件和数据，以及配置管理和现场安全措施的文件。由于现场认证过程的重点是基于没有具体的 TOE 的过程，这些安全保证要求被认为是合适的。

8.4.3 ALC_DVS

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 handle at the site during production, assembly and testing of the product can be used by potential attackers for the development of attacks. Therefore, the handling and storage of these items must be sufficiently protected. Further on the Protection Profile (1) requires this protection for sites involved in the life-cycle of Security ICs development and production.

由于假定潜在攻击者具有很高的攻击潜力，因此需要选择保证系列“开发安全”的 ALC_DVS.2 保证级别。在产品的生产、组装和测试过程中，现场的配置项和信息处理可能被潜在的攻击者用于开发攻击。因此，这些物品的处理和储存必须得到充分的保护。此外，保护概要 (1)要求对涉及安全 IC 开发和生产生命周期的站点进行这种保护。

8.4.4 ALC_LCD

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.

所选择的保证系列“生命周期定义”的保证等级 ALC_LCD.1 适用于支持受控开发和生产过程。这包括这些过程的文件和配置管理程序。由于该站点只为所述的安全集成电路的开发和生产的生命周期提供了有限的支持，因此重点只限于该站点。

8.4.5 ALC_FLR

The chosen assurance level ALC_FLR.1 of the assurance family “Flaw Remediation” is suitable to support the flaw remediation procedures. This comprises the reported security flaws can be collected, tracked and handled with a predefined written procedure. The defined written procedure and the appointed responsible can potentially support preservation of the integrity and confidentiality of the products. Therefore, this assurance level meets the requirements for flaw remediation.

“缺陷修复”保证系列中选择的保证级别 ALC_FLR.1 适用于支持缺陷修复程序。这包括可以通过预定义的书面程序收集、跟踪和处理报告的安全缺陷。所定义的书面程序和指定的责任人可能有助于保护产品的完整性和机密性。因此，该保证级别满足缺陷修复的要求。

8.5 保证措施原理 Assurance Measure Rationale

O.Acceptance-Test

ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.16C ensure the CM system is operated as being required so as to contribute the fulfillment of O.Acceptance-Test.

ALC_CMC.5.6C 要求 CM 系统支持通过自动化手段生产预期的 TOE。ALC_CMC.5.16C 需要证据应证明 CM 系统的运作符合 CM 计划。

ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the intended TOE during the transfer between sites. ALC_LCD.1.2C ensure the life-cycle model defined can contribute to the fulfillment of O.Acceptance-Test.

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

ALC_DVS.2.2C 要求采取安全措施，以保护站点之间传输过程中预期 TOE 的机密性和完整性。ALC_LCD.1.2C 确保定义的生命周期模型有助于完成验收测试。

因此，该目标适合满足安全保证要求。

O.Alarm-Response

ALC_DVS.2.1C requires that the developer shall describe all the physical, personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation including the initialization in its development and production environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C requires the justification of necessary level of protection is provided. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DVS.2.1C 要求开发人员应说明包括开发和生产环境中的初始化保护预期 TOE 设计和实施的机密性和完整性所需的所有物理、人员、程序和其他安全措施，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS.2.2C 要求提供必要保护等级的理由。因此，该目标有助于满足安全保证的要求。

O.Config-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.3C requires an adequate and appropriate review of changes to all configuration items. ALC_CMC.5.4C and ALC_CMC.5.8C requires a unique identification of all configuration items by the CM system. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.6C requires the CM system to support the production of the intended TOE by automated means. ALC_CMC.5.9C requires the support of audit information for all changes to the intended TOE by automated means including the originator, date and time. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that all the production related data used to generate

the modules can be identified. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describes how the CM system is used for the development of the intended TOE. ALC_CMC.5.15C requests evidence demonstrating that all configuration items have been and are being maintained under the CM system. ALC_CMC.5.16C requires evidence of CM system being operated in accordance with the CM plan. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, production 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 listed here.

ALC_CMC.5.2C 提供 CM 文档，描述用于标识唯一配置项的方法。ALC_CMC.5.3C 要求对所有配置项的更改进行充分和适当的审查。ALC_CMC.5.4C and ALC_CMC.5.8C 要求 CM 系统对所有配置项目进行唯一的识别。ALC_CMC.5.5C 要求 CM 系统提供自动措施，以便只对配置项目进行授权更改。ALC_CMC.5.6C 要求 CM 系统支持通过自动化手段生产预期的 TOE。ALC_CMC.5.9C 要求通过自动化的方式对预期 TOE 的所有变更提供审计信息的支持，包括发起人、日期和时间。ALC_CMC.5.10C 要求系统自动识别受配置项更改影响的所有配置项。ALC_CMC.5.11C 要求能够识别用于生成模块的所有生产相关数据。ALC_CMC.5.12C 要求提供包括 CM 计划的 CM 文件。ALC_CMC.5.13C 要求 CM 计划描述 CM 系统如何用于开发预定的 TOE。ALC_CMC.5.15C 要求提供证据证明所有配置项目都在 CM 系统下得到维护。ALC_CMC.5.16C 要求在 CM 系统下维护配置项的证据。ALC_CMS.5.1C 包括 SARs 的评估证据、生产工具和相关信息。ALC_CMS.5.2C 满足了与 ALC_CMC.5.4C 相同的要求。此外，ALC_LCD.1.1C 要求生命周期定义文件描述用于开发和维护产品的模型。该目标为这里列出的一套安全保证要求提供了依据。

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. In addition, ALC_CMC.5.4C and ALC_CMC.5.8C requires that the CM system uniquely identifies all configuration items. ALC_CMC.5.10C requires an automated means is provided to identify affected configuration items by the change of a given configuration item. ALC_CMC.5.11C requires that all the production related data used to generate the intended TOE can be identified. ALC_CMC.5.14C requires a procedure is in place to accept modified or newly created configuration items. The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, production tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_CMS.5.3C requires that developer of each configuration item shall be indicated.

The objective meets the set of Security Assurance Requirements.

ALC_CMC.5.1C 要求有一个文件化的过程，以确保产品的标签适当且一致。ALC_CMC.5.2C 要求使用一种用于唯一识别配置项的方法。此外，ALC_CMC.5.4C 和 ALC_CMC.5.8C 要求 CM 系统唯一地识别所有配置项目。ALC_CMC.5.10C 要求系统自动识别受配置项更改影响的所有配置项。

ALC_CMC.5.11C 要求能够识别用于生成模块的所有生产相关数据。ALC_CMC.5.14C 要求有一个程序来接受修改或新创建的配置项。ALC_CMS.5.1C 要求的配置清单应包括实现 SAR 的评估证据、生产工具和相关信息。ALC_CMS.5.2C 提出了与 ALC_CMC.5.4C 相同的要求。ALC_CMS.53C 要求指出每个配置项的开发人员。该目标满足一组安全保证要求。

O.Config-Process

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. ALC_CMC.5.4C requires configuration items shall be uniquely identified. ALC_CMC.5.5C requires that the CM system provides automated measures so that only authorized changes are made to the configuration items. ALC_CMC.5.7C requires that the person or team accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.8C requires CM system shall identify configuration items comprising the TSF. ALC_CMC.5.10C requires that the system automatically identifies all configuration items that are affected by a change given to a configuration item. ALC_CMC.5.11C requires that all the production related data used at the site can be identified. ALC_CMC.5.12C requires a CM documentation that includes a CM plan. ALC_CMC.5.13C requires that the CM plan describe how the CM system is used for the development of the intended TOE. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requires evidence that configuration items have been and being maintained under the CM system. ALC_CMC.5.16C requires evidence of CM system being operated in accordance with the CM plan.

ALC_CMC.5.2C 需要一种用于标识唯一配置项的方法。ALC_CMC.5.3C 要求对所有配置项的更改进行充分和适当的审查。ALC_CMC.5.4C 要求对配置项目进行唯一标识。ALC_CMC.5.5C 要求 CM 系统提供自动措施，以便对配置项目只进行授权更改。ALC_CMC.5.7C 要求在 CM 系统中接受配置项目的人或团队不是开发它的人。ALC_CMC.5.8C 要求 CM 系统应识别包含 TSF 的配置项。ALC_CMC.5.10C 要求系统自动识别受给配置项的更改影响的所有配置项。ALC_CMC.5.11C 要求能够识别在现场使用的所有与生产相关的数据。ALC_CMC.5.12C 要求提供包括 CM 计划的 CM 文件。ALC_CMC.5.13C 要求 CM 计划描述 CM 系统如何用于开发预定的 TOE。ALC_CMC.5.14C 要求用于接受修改或新创建的配置项目作为预期 TOE 的一部分的程序的描述。ALC_CMC.5.15C 要求有证据证明配置项在 CM 管理系统下得到维护。ALC_CMC.5.16C 需要证据应证明 CM 系统的运作符合 CM 计划。

The configuration list required by ALC_CMS.5.1C shall include the evaluation evidence for the fulfilment of the SARs, production tools and related information. ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C and ALC_CMC.5.8C. 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 intended TOE. The objective meets the set of Security Assurance Requirements.

ALC_CMS.5.1C 要求的配置清单应包括实现 SARs 的评估证据、生产工具和相关信息。ALC_CMS.5.2C 满足与 ALC_CMC.5.4C 和 ALC_CMC.58C 相同的要求。ALC_LCD.1.1C 要求生命周期定义文档描述用于开发和维护产品的模型。该目标符合一套安全保证要求。

O.Control-Scrap

ALC_DVS.2.1C requires that all the physical, procedural, personnel, and other security measures that are implemented to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective is suitable to meet the Security Assurance Requirement.

ALC_DVS.2.1C 要求实施物理、程序、人员和其他安全措施，以保护预期 TOE 设计和实施的机密性和完整性。ALC_DVS.2.2C 证明了这些安全措施是足够的。因此，该目标适用于满足安全保证的要求。

O.External-Delivery

ALC_CMC.5.16C requires evidence of CM system being operated in accordance with the CM plan. ALC_CMS.5.2C requires the configuration list to uniquely identify the configuration items. ALC_DVS.2.1C and ALC_DVS.2.2C require all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment and provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_CMC.5.16C 需要证据应证明 CM 系统的运作符合 CM 计划。ALC_CMS.5.2C 要求配置列表应标识唯一地配置项。ALC_DVS.2.1C 和 ALC_DVS.2.2C 要求开发安全文件应描述在开发环境中保护产品设计和实施的机密性和完整性所需的所有物理、程序、人员和其他安全措施，并提供证据证明 TOE 的开发与维护遵循这些安全措施。

O.Internal-Monitor

ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DVS.2.2C 要求开发安全文件应证明安全措施提供了必要的保护级别，以保持预期 TOE 的机密性和完整性。因此，这一目标有助于满足安全保证要求。

O.Logical-Access

ALC_DVS.2.1C requires that the developer shall describe all the physical, personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design, implementation and in its development and production environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C justify the security measures are sufficient. ALC_CMC.5.5C requires that the CM

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

ALC_DVS.2.1C 要求开发人员应说明所有必要的物理、人员、程序和其他安全措施，以保护预期 TOE 设计、实施及其开发和生产环境的机密性和完整性，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS.2.2C 证明安全措施足够。ALC_CMC.5.5C 要求构型管理系统提供自动化措施，以便仅对配置项进行授权的更改。因此，这一目标有助于满足安全保证要求。

O.Logical-Operation

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

ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

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

ALC_DVS.2.1C 要求开发人员应说明所有必要的人员、程序和其他安全措施，以保护预期 TOE 设计、实施及其开发和生产环境的机密性和完整性，并提供证据证明 TOE 的开发和维护遵循这些安全措施。因此，该目标有助于满足安全保证的要求。ALC_DVS.2.2C 要求开发安全文件应证明安全措施提供了必要的保护级别，以保持预期 TOE 的机密性和完整性。因此，该目标适用于满足安全保证的要求。ALC_CMC.5.5C 要求 CM 系统提供自动化措施，以便只对配置项进行授权的更改。因此，该目标有助于满足安全保证的要求。

O.Maintain-Security

ALC_DVS.2.2C requires the implemented security measures to be sufficient to protect the confidentiality and integrity of the intended TOE. ALC_DVS.2.1C requires that the developer shall describe all the physical, personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development and production environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DVS.2.2C 要求开发安全文件应证明安全措施提供了必要的保护级别，以保持预期 TOE 的机密性和完整性。ALC_DVS.2.1C 要求开发人员应说明在其开发和生产环境中保护预期 TOE 设计和实施的机密性和完整性所需的所有物理、人员、程序和其他安全措施，并提供证据证明 TOE 的开发和维护遵循这些安全措施。因此，该目标有助于满足安全保证的要求。

O.Physical-Access

ALC_DVS.2.1C requires that the developer shall describe all physical security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DVS.2.1C 要求开发人员描述所有必要的物理安全措施，以保护其开发环境中预期 TOE 设计和实施的机密性和完整性，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS.2.2C 证明安全措施足够。因此，这一目标有助于满足安全保证的要求。

O.Reception-Control

ALC_CMC.5.2C requires a CM documentation that describes the method used to uniquely identify the configuration items. ALC_CMC.5.4C and ALC_CMC.5.8C require a unique identification of all configuration items by the CM system. ALC_CMC.5.7C requires that the person accepting the configuration item in the CM system is not the person who developed it. ALC_CMC.5.10C requires an automated means is provided to identify affected configuration items by the change of a given configuration item. ALC_CMC.5.11C requires that all the production related data used to generate the modules can be identified. ALC_CMC.5.14C requires the description of the procedures used to accept modified or newly created configuration items as part of the intended TOE. ALC_CMC.5.15C requires the evidence demonstrating that all configuration items have been and are being maintained under the CM system.

ALC_CMC.5.2C 需要一个 CM 文档，其中描述了用于标识唯一配置项的方法。ALC_CMC.5.4C 和 ALC_CMC.5.8C 要求 CM 系统对所有配置项的唯一标识。ALC_CMC.5.7C 要求在 CM 系统中接受配置项的人不是开发它的人。ALC_CMC.5.10C 要求提供一种自动通过更改给定配置项来识别受影响的配置项的方法。ALC_CMC.5.11C 要求能够识别用于生成模块的所有生产相关数据。ALC_CMC.5.14C 要求用于接受修改或新创建的配置项目作为预期 TOE 的一部分的程序的描述。ALC_CMC.5.15C 要求提供证据，证明所有配置项都在 CM 管理系统下进行维护。

ALC_CMS.5.2C addresses the same requirement as ALC_CMC.5.4C. ALC_DVS.2.2C requires security measures to protect the confidentiality and integrity of the intended TOE during the transfer between sites. Thereby this objective is suitable to meet the Security Assurance Requirement.

ALC_CMS.5.2C 满足了与 ALC_CMC.5.4C 相同的要求。ALC_DVS.2.2C 要求采取安全措施，以保护站点之间传输期间预期 TOE 的机密性和完整性。因此，该目标适合满足安全保证要求。

O.Security-Control

ALC_DVS.2.1C requires that the developer shall describe all personnel, procedural and other security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development and production environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C justify the security measures are sufficient. Thereby this objective contributes to meet the Security Assurance Requirement.

ALC_DVS.2.1C 要求开发人员应说明在其开发和生产环境中保护预期 TOE 设计和实施的机密性和完整性所需的所有人员、程序和其他安全措施，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS.2.2C 证明安全措施足够。因此，这一目标有助于满足安全保证要求。

O.Security-Documentation

ALC_DVS.2.1C requires that the developer shall have a security documentation and ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection, and provide evidence that these security measures are followed during the development and maintenance of the TOE. Therefore, this objective contributes to meet the Security Assurance Requirements.

ALC_DVS.2.1C 要求开发商应具有安全文件，ALC_DVS2.2C 要求证明所述措施适合提供必要的保护级别，并提供证据证明 TOE 的开发和维护遵循这些安全措施。因此，这一目标有助于满足安全保证要求。

O.Staff-Engagement

ALC_DVS.2.1C requires the description of personnel security measures that are necessary to protect the confidentiality and integrity of the intended TOE design and implementation in its development environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS.2.2C justify the security measures are sufficient. Thereby the objective fulfils this combination of Security Assurance Requirements.

ALC_DVS.2.1C 要求说明在其开发环境中保护预期 TOE 设计和实施的机密性和完整性所必需的人员安全措施，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS.2.2C 证明安全措施足够。因此，该目标满足了安全保证要求的组合。

O.Transfer-Data

ALC_DVS.2.1C: The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the product design and implementation in its development environment, and provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_DVS2.2C requires the justification that the described measures are appropriate to provide the necessary level of protection. This protection also includes internal transportation. Thereby this objective is suitable to meet the combination of Security Assurance Requirements.

ALC_DVS.2.1C：开发安全文件应描述在开发环境中保护产品设计和实施的机密性和完整性所需的所有物理、程序、人员和其他安全措施，并提供证据证明 TOE 的开发和维护遵循这些安全措施。ALC_DVS2.2C 要求证明所述措施适合提供必要的保护水平。这种保护还包括内部运输。因此，该目标适合于满足安全保证要求的组合。

O.Zero-Balance

ALC_CMC.5.6C requires that the CM system supports the production of the intended TOE by automated means. ALC_CMC.5.15C requires the evidence can demonstrate that all configuration

items have been and are being maintained under the CM system. ALC_CMC.5.16C requires evidence demonstrating that the CM system is operated in accordance with the CM plan. ALC_DVS.2.2C requires security measures that are necessary to protect the confidentiality and integrity of the intended TOE. ALC_LCD.1.2C requires control over the development and maintenance of the intended TOE. Thereby this objective is suitable to meet the Security Assurance Requirement.

ALC_CMC.5.6C 要求 CM 系统支持通过自动化手段生产预期的 TOE。ALC_CMC.5.15C 要求有证据可以证明所有配置项目都在 CM 系统下得到维护。ALC_CMC.5.16C 要求有证据表明，CM 系统是按照 CM 计划运行的。ALC_DVS.2.2C 要求采取必要的安全措施，以保护预定 TOE 的保密性和完整性。ALC_LCD.1.2C 要求对预期的 TOE 的开发和维护进行控制。因此，该目标适合于满足安全保证要求。

O.Flaw-Remediation

ALC_FLR.1.1C requires procedures used to track all reported security flaws in each release of the production lot shall be provided. ALC_FLR.1.2C requires a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. ALC_FLR.1.3C requires corrective actions be identified for each of the security flaws. ALC_FLR.1.4C requires the methods used to provide flaw information, corrections and guidance on corrective actions to finished good receiver. Therefore, this objective is suitable to meet the Security Assurance Requirement.

ALC_FLR.1.1C 要求提供用于跟踪每个生产批次的所有报告的安全缺陷的程序。ALC_FLR.1.2C 要求提供对每个安全缺陷的性质和影响的描述，以及找到该缺陷的纠正措施的情况。ALC_FLR.1.3C 要求为每个安全缺陷确定纠正措施。ALC_FLR.1.4C 要求用于提供缺陷信息、纠正措施和指导纠正措施的方法要完成良好的接收。因此，该目标适合于满足安全保证要求。

8.6 评估文件的映射 Mapping of the Evaluation Documentation

The scope of the evaluation according to the assurance class ALC comprises the processing and handling of security products and associated data as well as the complete documentation of the site provided for the evaluation.

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

根据保证等级 ALC 的评估范围包括安全产品和相关数据的处理和处置，以及为评估提供的完整的现场文件。

内部现场文档和安全保证要求之间的映射仅在现场安全目标的完整版本中可用。

9 参考文献 Bibliography

1. **EUROSMART.** *Security IC Platform Protection Profile with Augmentation packages.* Version 1.0, 2014.

2. **Common Criteria for Information Technology Security Evaluation.** *Part 1: Introduction and General Model.* Version 3.1, Rev. 5, April 2017.

3. —. *Part 3: Security Assurance Components.* Version 3.1, Rev. 5, April 2017.

4. **Common Methodology for Information Technology Secuirty Evaluation.** *Evaluation methodology.* Version 3.1, Rev.5, April 2017.

5. **Library, Join International.** *Minimum Site Security Requirements, version 3.0.* 2020 February.

6. **Common Methodology for Information Technology Secuirty Evaluation.** *Supporting Document, Site Certification.* Version 1.0, Rev.1, October 2007.

7. **HENGHUI Technology Corporation Limited.** *Configuration Management System Usage Procedure CJ#4#2-2018A-05 v0.8.*

8. —. *Development Security Policy ZHGLB-2018A-01 v0.9.*

9. —. *Lifecycle Definition Document CJ#4#2-2018A-06 v0.7.*

10. —. *Flaw Remediation Procedure ZHGLB-2018A-29 v0.7.*

11. —. *CM Item list CJ#4#2-2021C-84 v1.2.*

PUBLIC