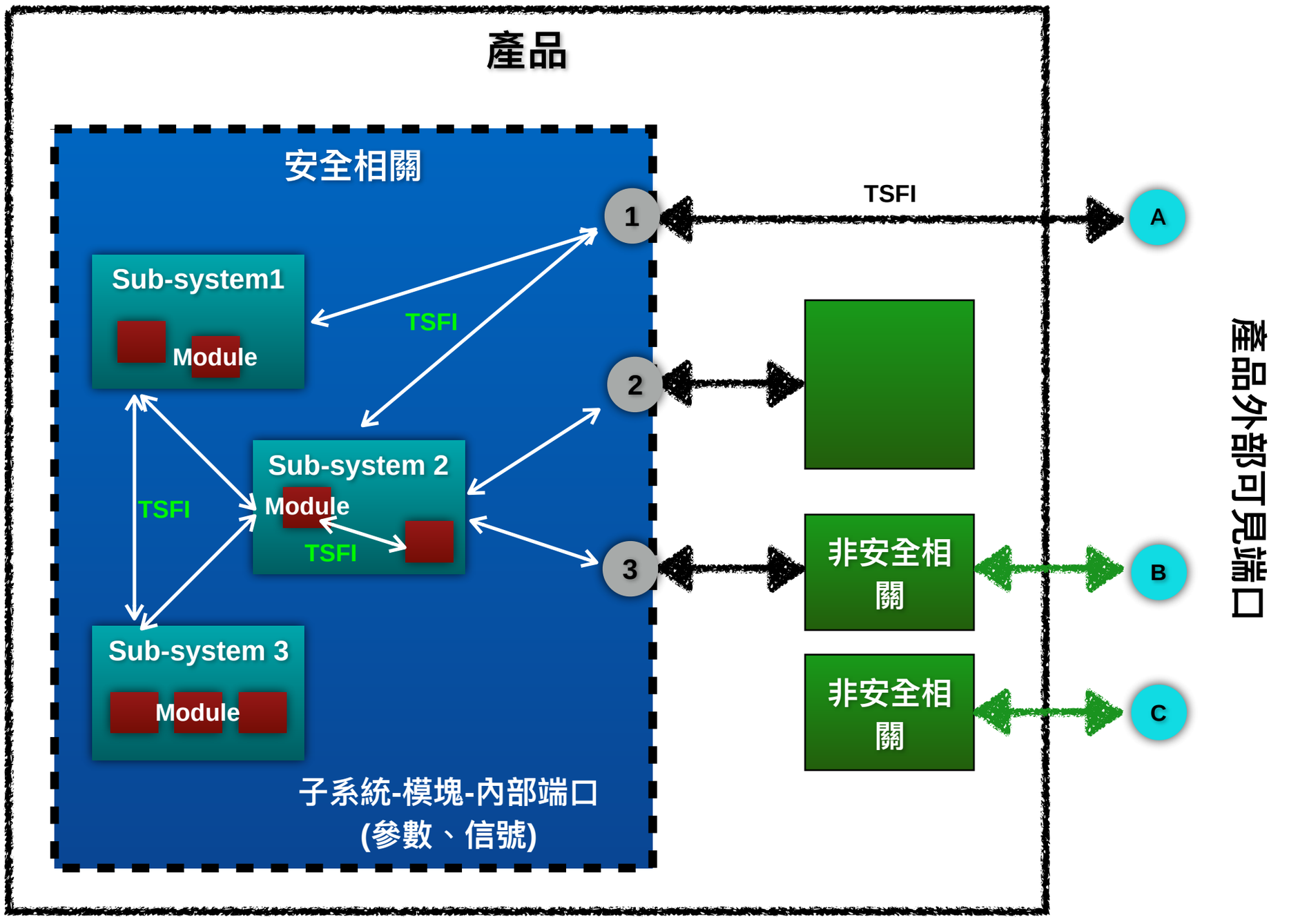
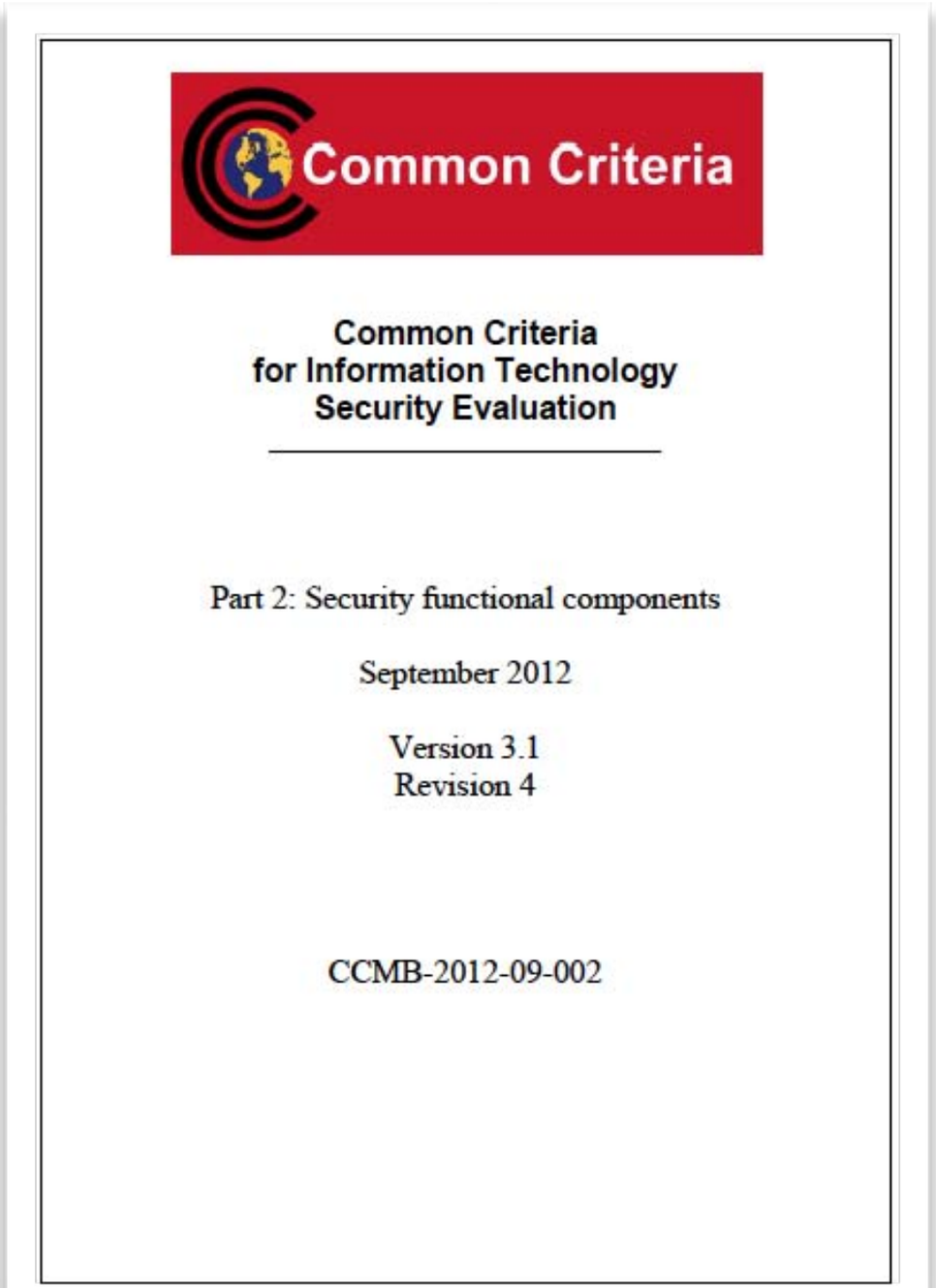
評估對象 (TOE) - 子系統 - 模塊 - 端口

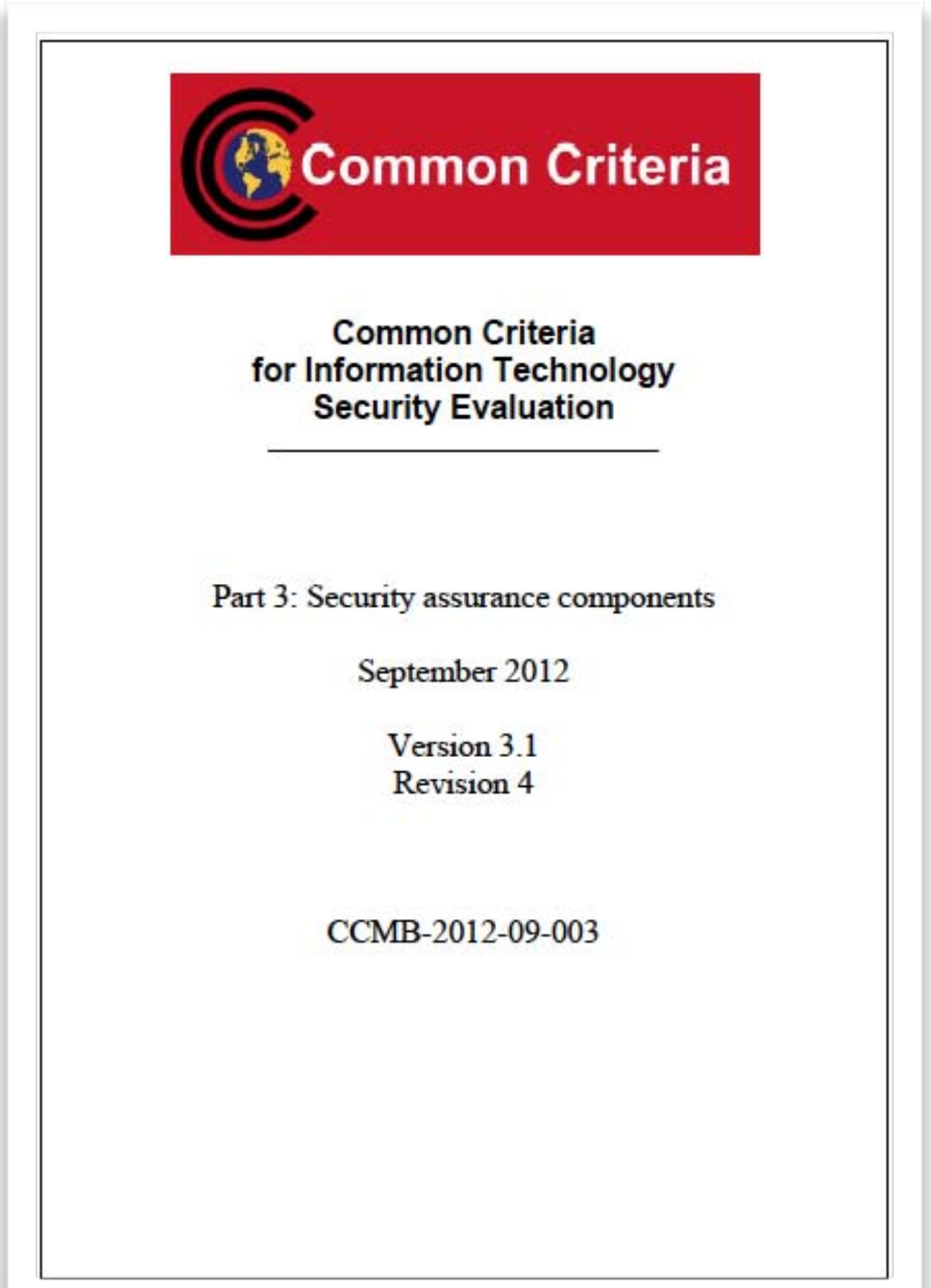


第二部分：安全功能要求



1. Class FAU: Security audit 安全審計
2. Class FCO: Communication 通信
3. Class FCS: Cryptographic support 密碼支持
4. Class FDP: User data protection 用戶數據保護
5. Class FIA: Identification and authentication 標示與鑑別
6. Class FMT: Security management 安全管理
7. Class FPR: Privacy 隱私
8. Class FPT: Protection of TSF 安全功能保護
9. Class FRU: Resource utilization 資源利用
10. Class FTA: TOE access TOE 訪問
11. Class FTP: Trusted path/channels 可信路徑/通道

第三部分：安全保障要求


Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 3: Security assurance components

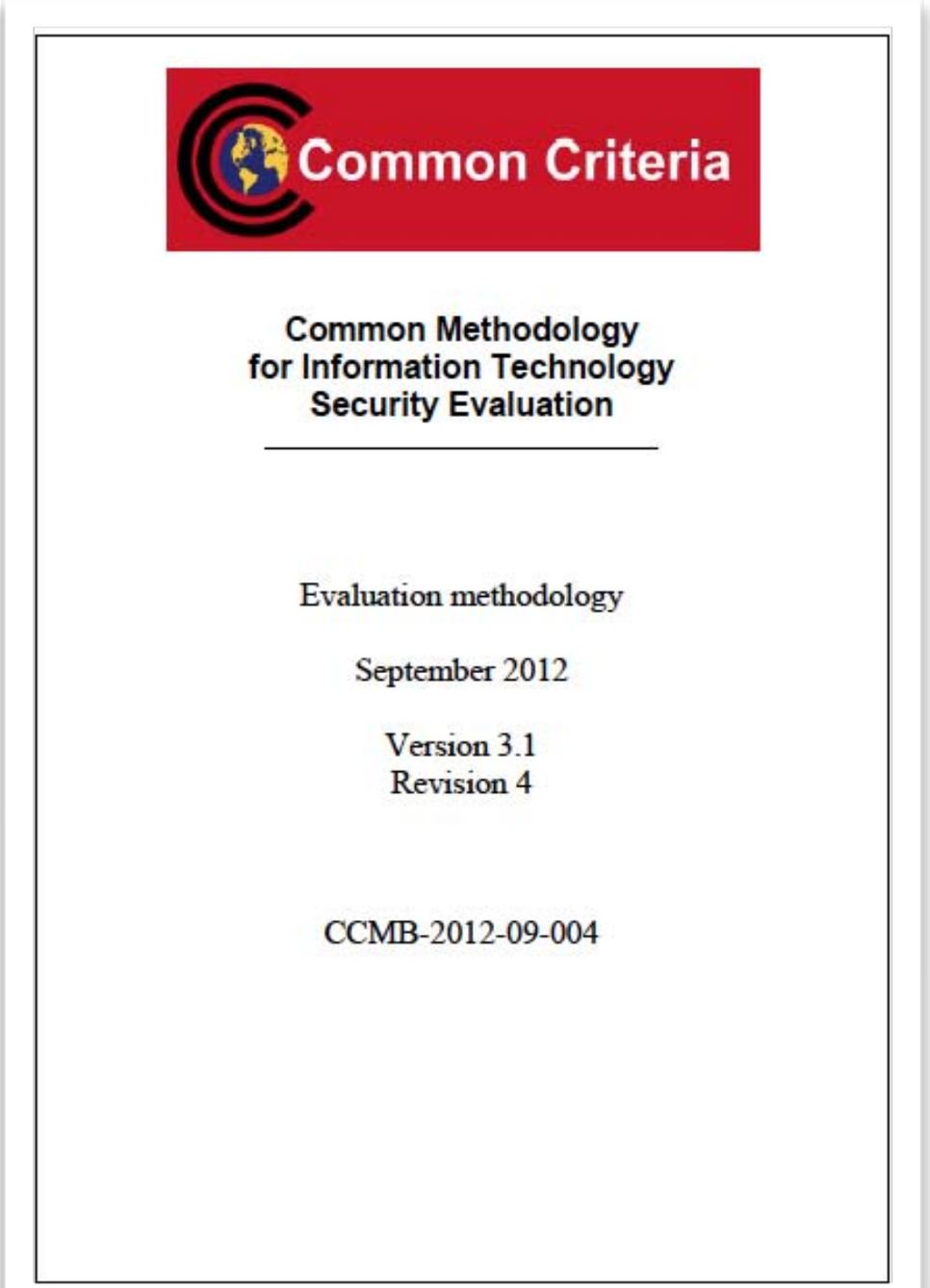
September 2012

Version 3.1
Revision 4

CCMB-2012-09-003

1. Overview 概述
2. Assurance paradigm 保障範型
3. Security assurance components 安全保障組件
4. Evaluation assurance levels 評估保護等級
5. Composed assurance packages 組合保障包
6. Class APE: Protection profile evaluation 保護輪廓評估
7. Class ASE: Security Target Evaluation 安全目標評估
8. Class ADV: Development 開發
9. Class AGD: Guidance documents 指導性文檔
10. Class ALC: Life-cycle support 生命週期支持
11. Class ATE: Tests 測試
12. Class AVA: Vulnerability assessment 脆弱性評定
13. Class ACO: Composition 組合

Common Methodology for Information Technology Security Evaluation
信息技術安全評估方法



1. Class APE: Protection Profile evaluation 保護輪廓評估方法
2. Class ASE: Security Target evaluation 安全目標評估方法
3. Class ADV: Development 開發過程評估方法
4. Class AGD: Guidance documents 指導性文檔評估方法
5. Class ALC: Life-cycle support 生命週期支持評估方法
6. Class ATE: Tests 測試過程評估方法
7. Class AVA: Vulnerability assessment 脆弱性評估方法
8. Class ACO: Composition 組合評估方法

Evaluation packages and EAL levels

Ref: Common Criteria v 3.1

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development 開發	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents 指引文檔	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support 生命週期支持	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation 評估對象描述	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests 測試	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

安全功能規範 (ADV_FSP) 評估內容

11.2.5 ADV_FSP.2 安全执行功能规范

依赖关系：ADV_TDS.1 基础设计。

11.2.5.1 开发者行为元素

11.2.5.1.1 ADV_FSP.2.1D

开发者应提供一个功能规范。

11.2.5.1.2 ADV_FSP.2.2D

开发者应提供:

功能规范到安全功能要求的追溯关系。

11.2.5.2 证据的内容和形式元素

11.2.5.2.1 ADV_FSP.2.1C

功能规范应完整地描述TSF。

11.2.5.2.2 ADV_FSP.2.2C

功能规范应描述**所有**的TSFI的目的和使用方法。

11.2.5.2.3 ADV_FSP.2.3C

功能规范应识别**和描述**每个TSFI相关的所有参数。

11.2.5.2.4 ADV_FSP.2.4C

对于每个SFR-执行TSFI，

功能规范应**描述**TSFI相关的**SFR-执行行为**。

11.2.5.2.5 ADV_FSP.2.5C

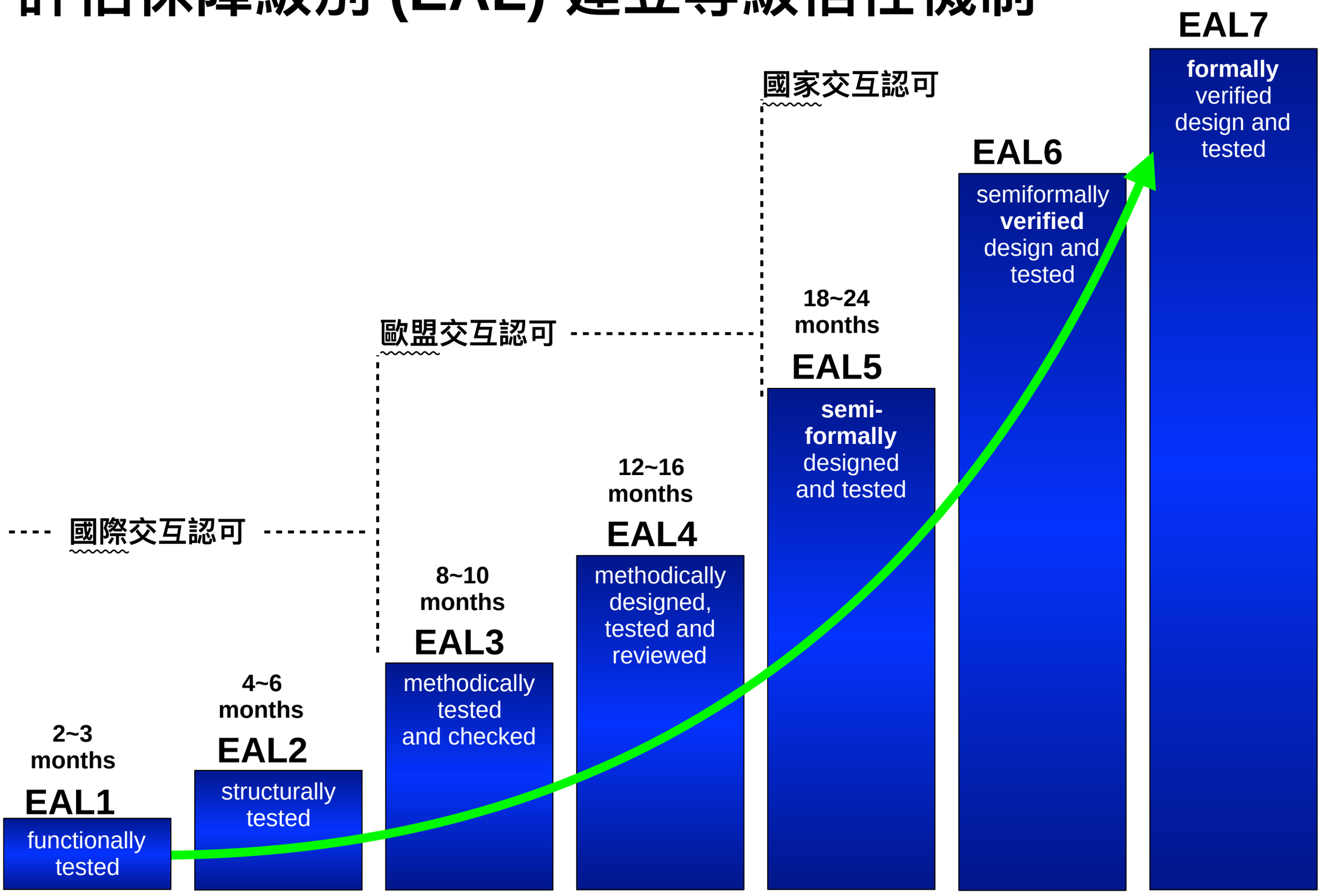
对于SFR-执行TSFI，

功能规范应描述由SFR-执行行为相关处理而引起的直接错误消息。

11.2.5.2.6 ADV_FSP.2.6C

功能规范应论证安全功能要求到TSFI的追溯。

評估保障級別 (EAL) 建立等級信任機制



Introduction to
IoT Protection Profile

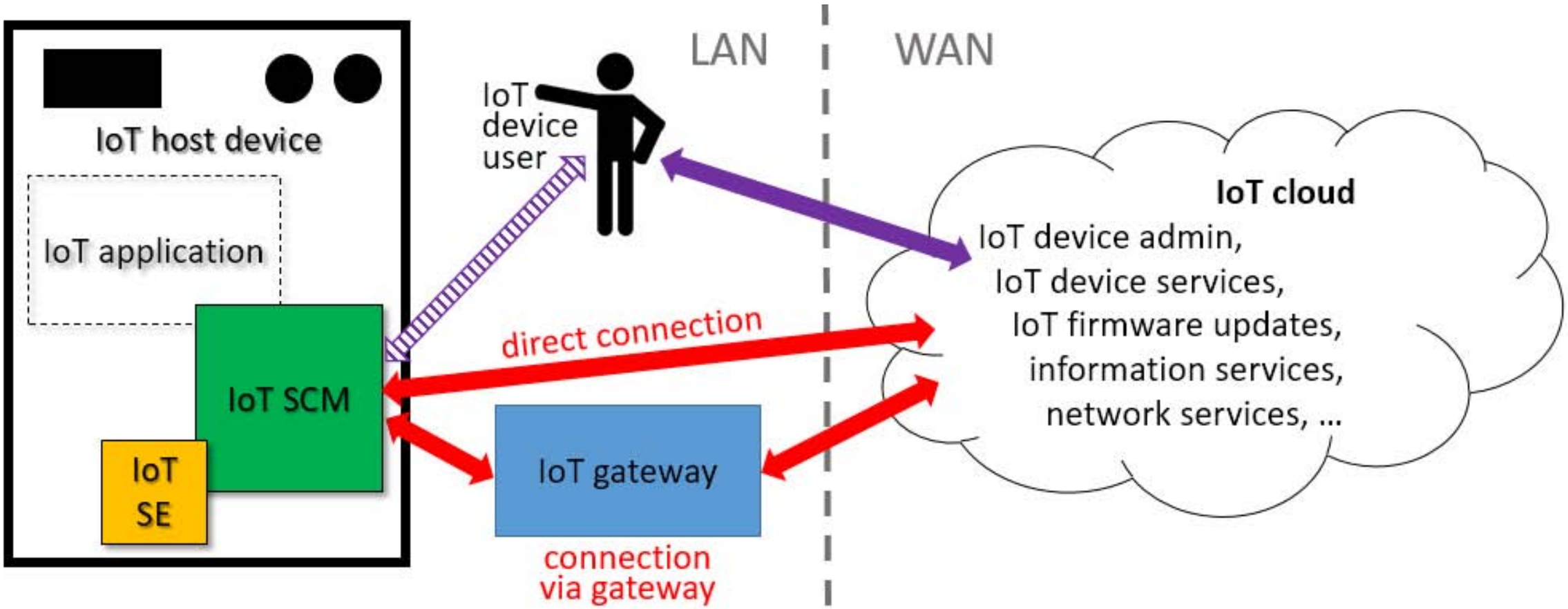
物聯網國際安全技術/產品認證規範

PHILIP KU 古智仲
philip.ku@TKSG.Global

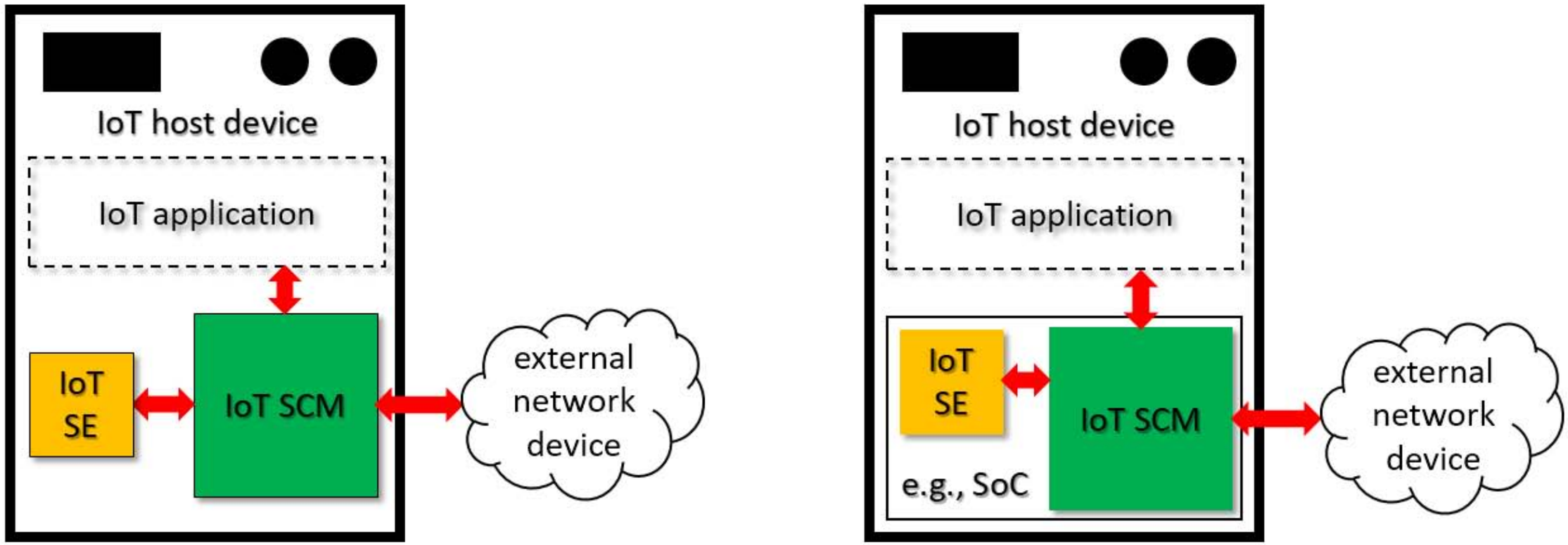
Milestones

- **July 2017 IoT-PPs initiative**
- **October, 2017 SCA signed PP development contract and confirmed working group**
- **November, 2017 1st PP Working Group Meeting**
- **January, 2018 2nd PP Working Group Meeting**
- **May, 2018 Drafted IoT-SCM-PP (EAL2+) and IoT-SE-PP (EAL4+)**
- **(Q3, 2018, PP certification by Germany Federal Office for IT Security - Bundesamt für Sicherheit in der Informationstechnik)**
- **(October, 2018 ICCC 2018 Amsterdam Netherlands, Presentation session - “IoT PP for Smart Home Appliance”)**

Business case



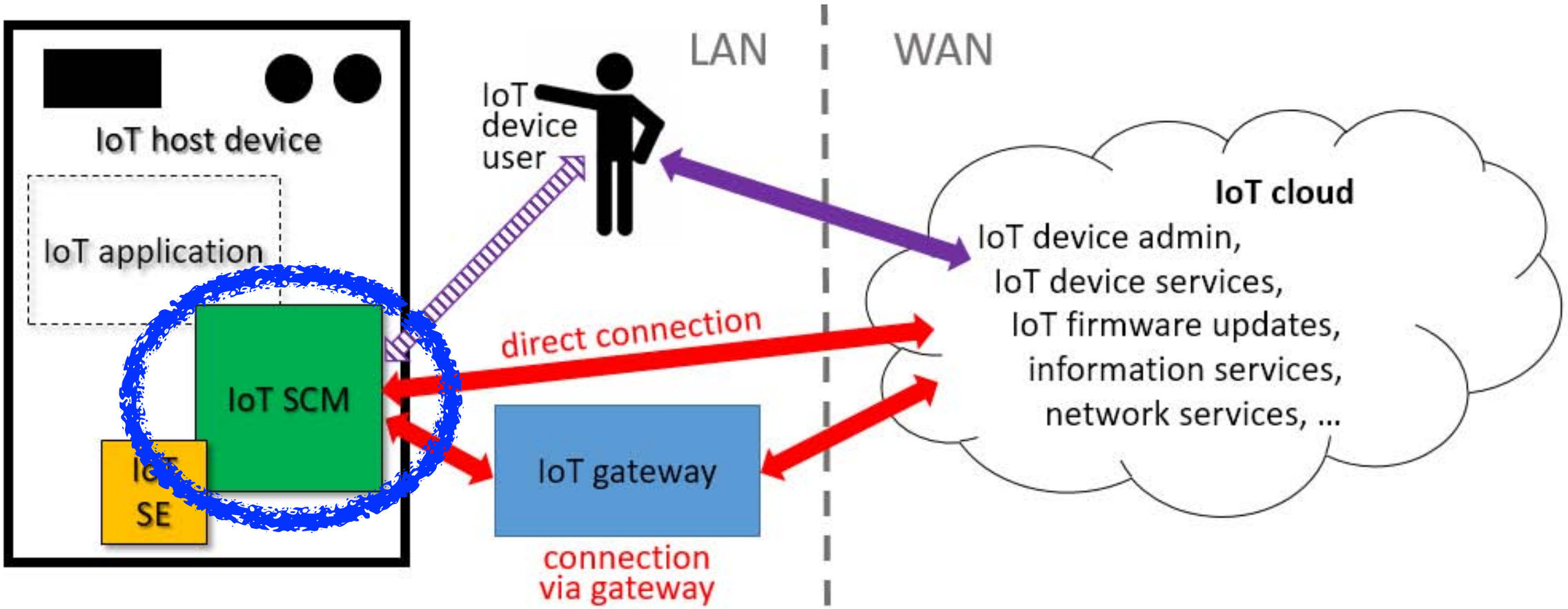
Used case



(a) separate hardware for IoT SCM (TOE), IoT SE and IoT application

(b) shared hardware for IoT SCM (TOE) and IoT SE, separated IoT application

IoT Secure Communications Module Protection Profile (IoT-SCM-PP)



Threats to the IoT Secure Communications Module

- **Impersonation 假扮/冒充認可的 IoT 設備接收或發送信息**
  - **An attacker may try to send data to the IoT device the IoT SCM TOE is integrated in, impersonating a particular external network device, or to send data to an external network device, impersonating the TOE, without the respective receiving party being able to detect that.**
- **Modification 竄改 (modify) / 重送 (replay) SCM 與 IoT 設備之間的通信內容**
  - **An attacker may try to intercept communication between the IoT device the IoT SCM TOE is integrated in and the external network device to modify or replay transmitted IoT device data or external device data, without the respective receiving party being able to detect that.**
- **Disclosure IoT 設備與 SCM 之間的通信遭到竊聽遭到**
  - **An attacker may try to intercept communication between the IoT device the IoT SCM TOE is integrated in and the external network device to gain knowledge about transmitted IoT device data or external device data.**
- **Illegal Connection IoT 應用程式錯誤或惡意竄改，導致非法訪問、機密信息洩露**
  - **A faulty or maliciously modified IoT application may try to establish a network connection to external network devices/addresses, which are not related to the operation of the IoT device, possibly ending up in confidential data being sent to the wrong entity in the network.**

Security objectives for the IoT Secure Communications Module

- **Data authenticity 數據認證**
  - **The TOE shall provide functionality of data authenticity protection by adding electronic signatures or message authentication codes (MACs) to data to be sent to an external network device, and by verification of electronic signatures or message authentication codes (MACs) of data received from an external network device.**
- **Data confidentiality protection 數據加密保護**
  - **The TOE shall provide functionality of data confidentiality protection by encryption of data sent to an external network device, and by decryption of ciphertext data received from an external network device. The encryption mechanism(s) used shall provide security strength of at least 100 bits.**
- **Connection control 連線管制**
  - **The TOE shall provide functionality to allow the IoT device admin to specify/limit the network addresses the TOE is allowed to establish network connections to.**

