財團法人全國認證基金會
Taiwan Accreditation Foundation

工業自動化與控制系統資訊安全產品驗證方案(ISASecure® Certification Scheme)測試實驗室評鑑指引

指引與報告

TAF-CNLA-G47(1)

目錄

目的

”評鑑”為認證過程中的關鍵步驟，為協助評鑑小組完成評鑑工作與提昇評鑑品質，特編撰本文件。本文件係以 ISO/IEC 17025 規定為基礎，納入國際自動化協會資訊安全符合性機構(ISA Security Compliance Institute,簡稱 ISCI）制定之工業自動化與控制系統資訊安全產品驗證方案(簡稱 ISASecure® Certification Scheme)中對特許實驗室(Chartered Laboratory)之要求制訂，作為評鑑小組執行評鑑作業之指引。

1.適用範圍

1.1 本文件適用於財團法人全國認證基金會(以下簡稱本會)，關於符合性評鑑機構申請 ISASecure® Certification Scheme 之特許實驗室(Chartered Laboratory)認證活動之評鑑工作。

註：符合性評鑑機構(conformity assessment body; CAB) 是能提供符合性評鑑服務且能作為認證對象之機構。

1.1.1 申請組件安全性保障 Component Security Assurance (CSA)驗證方案者，應符合 ISO/IEC 17025 認證及 ISO/IEC 17065 認證。有關產品驗證機構(ISO/IEC 17065)申請事宜，請洽本會驗證機構認證處。

註: 參見 CSA-100 第 4.5.3 節，CSA-200 第 5.2 節。

1.2 認證範圍如下

1.2.1 組件安全性保障 Component Security Assurance (CSA)

(1). 組件功能安全性評鑑(FSA-C, Functional security assessment for components，對應 ISASecure® Certification Scheme 文件編號: CSA-311)

(2). 組件漏洞識別測試(VIT-C, Vulnerability Identification Testing Specification，對應 ISASecure® Certification Scheme 文件編號: SSA-420)

1.3 認證機構應符合 ISASecure® Certification Scheme 中對認證機構之要求，並依第 1.2 節認證範圍進行評鑑作業。

2.參考文件

(1). ISO/IEC 17000 Conformity assessment – Vocabulary and general principles

(2). ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

(3). ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services

(4). CSA-100-ISA Security Compliance Institute – Component Security Assurance – ISASecure® certification scheme

(5). CSA-102- ISA Security Compliance Institute – Component Security Assurance – Baseline document versions and errata for CSA specifications

(6). CSA-200-ISA Security Compliance Institute – Component Security Assurance – ISASecure CSA chartered laboratory operations and accreditation

(7). CSA-204- ISCI Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates

(8). CSA-205- ISCI Component Security Assurance – Certificate Document Format

(9). CSA-300- ISCI Component Security Assurance – ISASecure certification requirements

(10). CSA-301- ISCI Component Security Assurance – Maintenance of ISASecure certification

(11). CSA-303- ISASecure CSA Sample Report

(12). CSA-311- ISCI Component Security Assurance – Functional security assessment for components

(13). CSA-312- ISCI Component Security Assurance – Security development artifacts for components

(14). SSA-420- ISCI System Security Assurance – Vulnerability Identification Test Specification

註: ISASecure 文件查詢網址(有關本文所提供之 ISASecure 資訊僅供參考，所有最新資訊以 ISASecure 網站公告為準)：https://www.isasecure.org/

3.名詞定義

3.1 組件(component)

屬於工業自動化與控制系統的實體物，具備一個或多個主機設備、網路設備、應用軟體、或嵌入式裝置的特性。

3.2 應用軟體(Software applications)

一個或多個軟體程式及其依存關係，用以與過程或控制系統本身相互作用(例如組態軟體與歷史紀錄)。

註 1：軟體應用程式傳統上是在主機設備或嵌入式裝置中執行。

註 2：依存關係是指軟體應用程式運作所必需的任何軟體程式，例如資料庫套件、回報工具、或任何第三方或開放原始碼軟體。

3.3 嵌入式裝置(Embedded Devices)

特殊用途的裝置，執行設計用以直接監視、控制或啟動工業程序的嵌入式軟體。

註：嵌入式裝置的屬性：無旋轉媒體、數量有限的暴露服務、透過外部介面程式化、嵌入式作業系統或等效韌體、即時排程器、可能有附加的控制面板、可能有通訊介面。例如：可程式控制器(PLC)、磁場感測器裝置、安全儀表系統(SIS)控制器、分散控制系統(DCS)控制器。

3.4 主機設備(Host Devices)

通用設備，執行作業系統(例如 Microsoft Windows OS 或 Linux)，主機能夠代管一個或多個供應商的一個或多個軟體應用程式、資料儲存或功能。

註：典型的屬性包括：檔案系統、可程式服務、無即時排程器及完整的人機介面(鍵盤、滑鼠等)。

3.5 網絡設備(Network Devices)

加快設備間的資料流程的設備，或限制資料的流程，惟可能不會直接與控制程序交互作用。

註：典型的屬性包括：嵌入式作業系統或韌體，無人機介面、無即時排程器並透過外部介面進行配置。

以下章節依據 ISO/IEC 17025：2017(中文版為 CNS 17025：2018)的章節編排，如章節內容之 ISO/IEC 17025：2017 的要求已足夠，無需另增加特定技術要求時，於對應章節將以「無特別要求」呈現。

4 一般要求事項

4.1 公正性

依據 CSA-200 Requirement CSA.R8

4.2 保密

依據 CSA-200 Requirement CSA.R1

依據 CSA-200 Requirement CSA.R3

5 架構要求事項(無特別要求)

6 資源要求事項

6.1 一般(無特別要求)

6.2 人員

依據 CSA-200 Requirement CSA.R13

依據 CSA-200 Requirement CSA.R32~R35

依據 CSA-200 Requirement CSA.R44

依據 CSA-200 Requirement CSA.R47

6.3 設施與環境條件

依據 CSA-200 Requirement CSA.R45

依據 CSA-200 Requirement CSA.R47

6.4 設備

依據 CSA-200 Requirement CSA.R28

依據 SSA-420 Requirement VIT-C.R1

依據 SSA-420 Requirement VIT-C.R12~R13

6.5 計量追溯性(無特別要求)

6.6 外部提供的產品與服務(無特別要求)

7 過程要求事項

7.1 需求事項、標單及合約之審查

依據 CSA-200 Requirement CSA.R15

依據 CSA-300 Requirement ISASecure_C.R4

7.2 方法的選用、查證及確證

依據 CSA-200 Requirement CSA.R18

依據 CSA-200 Requirement CSA.R29

依據 CSA-200 Requirement CSA.R32~R34

依據 SSA-420 Requirement VIT-C.R2~R5, R11

依據 SSA-420 Requirement VIT-C.R11

7.3 抽樣(無特別要求)

7.4 試驗件或校正件的處理

依據 CSA-200 Requirement CSA.R46

7.5 技術紀錄

依據 CSA-200 Requirement CSA.R31

依據 CSA-200 Requirement CSA.R50

7.6 量測不確定度的評估(無特別要求)

7.7 確保結果的效力(無特別要求)

7.8 結果的報告

依據 CSA-200 Requirement CSA.R21~R22

依據 CSA-200 Requirement CSA.R35

依據 SSA-420 Requirement VIT-C.R14~R23

7.9 抱怨

依據 CSA-200 Requirement CSA.R40~R42

依據 CSA-200 Requirement CSA.R57~R58

7.10 不符合工作(無特別要求)

7.11 數據管制與資訊管理(無特別要求)

8 管理系統要求事項

8.1 選項(無特別要求)

8.2 管理系統文件化(選項 A) (無特別要求)

8.3 管理系統的文件管制(選項 A)

依據 CSA-200 Requirement CSA.R48~R49

8.4 紀錄管制

依據 CSA-200 Requirement CSA.R47

8.5 處理風險與機會之措施(選項 A) (無特別要求)

8.6 改進(選項 A) (無特別要求)

8.7 矯正措施(選項 A) (無特別要求)

8.8 內部稽核(選項 A)

依據 CSA-200 Requirement CSA.R52~R55

8.9 管理階層審查(選項 A)

依據 CSA-200 Requirement CSA.R51