**附件**

1. 安全功能介面表

| **安全功能介面名稱****TSFI** | **目的****Purpose** | **安全功能介面可實現之安全功能需求****SFR** | **操作方式****Method of Use** | **參數****Parameter** | **執行動作****Actions** | **錯誤訊息****Error Message** |
| --- | --- | --- | --- | --- | --- | --- |
| 列出所有安全功能介面。 | 說明各安全功能介面之安全功能目的。 | 說明各安全功能介面如何實現附表1-2所列之安全功能需求。 | 說明如何使用各安全功能介面。 | 說明各安全功能介面所有參數及其意義。 | 說明各安全功能介面如何運作及其執行細節。 | 說明執行各安全功能介面產生之錯誤訊息，包含其意義及產生條件。 |
| *範例：**TSFI\_CLI* | *範例：**提供命令列模式操作介面* | *範例：**SFR\_安全管理：提供安全管理功能* | *範例：**以ssh連接待測物，即提供命令列模式操作介面* | *範例：**ID & password* | *範例：**可下達管理命令操作待測物* | *範例：**連接失敗**認證失敗* |

1. 子系統描述與分類表

| **子系統名稱****Subsystem** | **目的****Purpose** | **子系統隸屬之安全功能介面****TSFI** | **子系統行為說明****Behavior Description** |
| --- | --- | --- | --- |
| 列出各安全功能介面之子系統。 | 說明各子系統之安全功能目的。 | 說明各子系統隸屬於附件一所列之安全功能介面。 | 說明各子系統行為如下：(1) 如何實現安全功能介面的功能。(2) 與其他子系統間互動之資訊，包含不同子系統間的溝通以及傳遞資料的特性。 |
| *範例：**Subsystem\_ssh* | *範例：**提供ssh服務* | *範例：**TSFI\_CLI* | *範例：**(1) 提供TSFI\_CLI命令列模式操作介面**(2) 與其他子系統之互動：* *(A) Subsystem\_auth: 傳遞認證資訊給Subsystem\_auth，並由回覆訊息確認認證是否成功**(B) Subsystem\_terminal: …* |

1. 安全架構描述表

| **項目** | **說明** |
| --- | --- |
| 1.安全領域Security Domain | **安全領域名稱** | **安全領域說明** |
| 列出各安全功能介面對應之安全領域*範例：**TSFI\_GUI:**Domain\_SecureLogAudit**Domain\_SecureConnection* | 在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。*範例：**透過TSFI\_GUI來執行管理功能石，該TSFI同一時間只能有單一遠端連線，並只能執行單一稽核資料處理請求。* |
| 2.初始程序Secure Initialization | **相關元件** | **初始程序說明** |
| 操作待測物的相關元件/環境*範例：**待測物網路連接程序* | 提供安全啟動待測物之相關元件起始步驟及安裝程序。*範例：**1. 從端口標記為 0/ 0（ethernet0 / 0接口）連接一個 RJ- 45電纜到交換機或路由器Trust安全區。**2. 從端口標記為 0/ 1（ethernet0 / 1接口）連接一個 RJ- 45電纜到交換機或路由器中的DMZ安全區。* |
| 3.自我保護Self-Protection | **自我保護功能** | **與外部設備之關係** | **自我保護機制說明** |
| 列出各安全功能介面對應之自我保護機制*範例：**TSFI\_WEB:**自我保護1:身分驗證**自我保護2:遠端連線加密* | 說明安全功能及其介面與外部設備之資料交換動作*範例：**遠端以瀏覽器連線待測物進行管理功能時，以TSFI\_WEB GUI介面進行身分認驗證* | 需說明安全功能介面提供實體上或邏輯上的自我保護機制*範例：**1. 應輸入通行碼才能進入介面。**2. 資料傳輸機制：TLS/SSL。**3. 特殊執行方式：指紋辨識。**4. 特殊設備需求：指紋辨識器。* |
| 4.防止繞道Non-Bypassibility | **防止繞道功能** | **防止繞道機制說明** |
| 列出各安全功能對應之防止繞道機制*範例：**TSF\_Authentication身分驗證功能* | 1. 列舉可能繞道之手法2. 說明防範作法，包含進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。*範例：**可能直接以維護介面不經身份認證操控待測物。**防範作法：以實體封鎖方式，防止利用維護介面繞道身分認證程序。* |