Delta Electronics, Inc

資訊安全手冊

關鍵基礎設施

型號：InsightPower IPv6 Card, AIO Card, SNMP G3 Mini Card, EMS2000, Device Touch Panel

文件版本：v10

內容

1. 簡介

本指南介紹內容適用於，台達網路管理卡和帶有台達網路管理卡的嵌入式構件設備的安全功能。 這些功能使設備可以通過網路進行遠端操作。

目的

本文介紹以下協議和功能，請選擇適合您網路環境的協議和功能，以及在安全系統中如何設置和使用它們的方式：

- Telnet 與 SSH
- FTP 與 SFTP
- HTTP 與 HTTPS
- SNMPv1, v2c 與 v3
- Modbus TCP

此外，本指南記錄如何強化台達網絡管理卡，以增強設施的安全性。

2. 設備安全部署指南

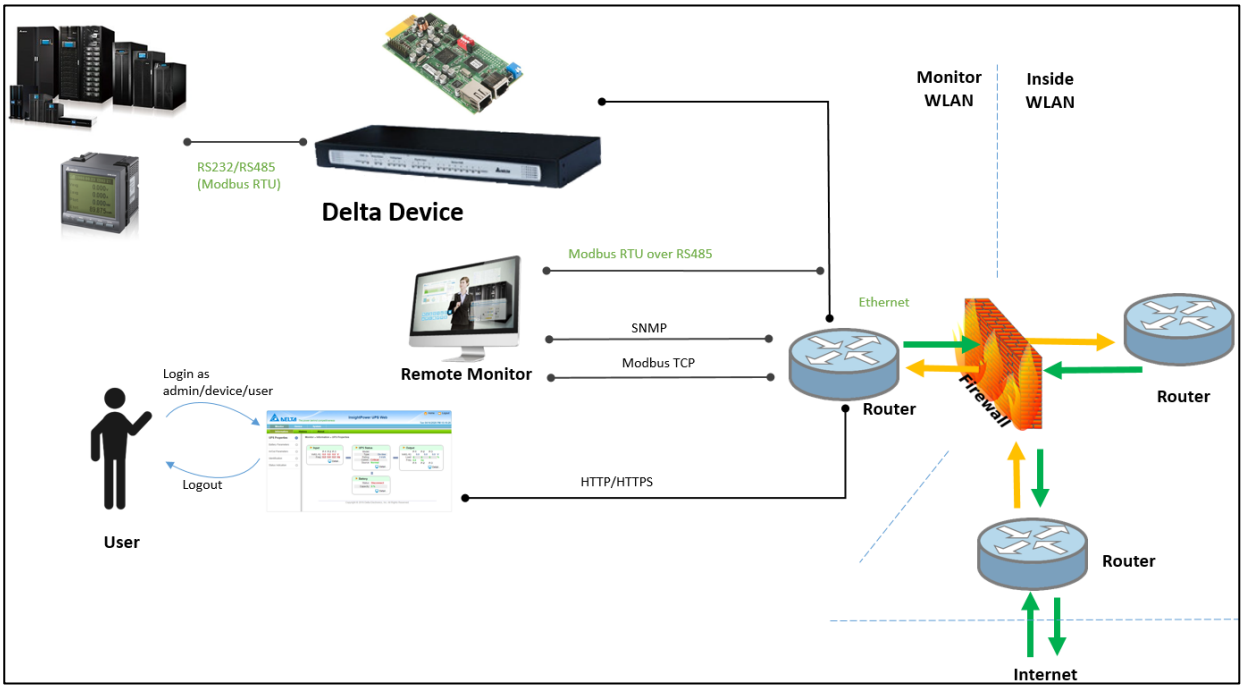
本文提供了一般性縱深防禦安全指導，可幫助您根據特定的安全要求來決定適當的安全部署。

在整個部署生命週期中維持安全性，需要考慮以下注意事項：

2.1 產品使用情境

設備擁有者部署台達產品，建議使用情境如下：

- 區域網路應獨立分開，分為監控設備區網、內部辦公區網與對外網際網路。
- 分割後的子網路之間通訊，應使用網路設備(如 Router)隔離，且網路設備應具基本資訊安全防護功能，如防火牆、異常流量偵測與回報紀錄等功能。



台達產品使用情境示意圖

2.2 物理的安全

設備擁有者應保護啟用的網路設備免受未經授權人的物理訪問。

- 訪問權限應僅限於需要維護設備的人員。

- 限制區應明確標明僅供授權人員使用。
- 限制區應上門鎖。
- 進入限制區時應進行物理或電子審核追蹤。
- 現場監控使用之接線插座(頭)，應固定鎖附與避免外露，並檢查接線是否有破損，以防止有心人士接線進行側錄與攻擊行為發生。

2.3 設備的安全

設備安全性包括以下幾項：

- **使用最新版本韌體**

Delta Software Center 網站為您的設備網卡提供了最新韌體，請定期檢查網站，並使用最新韌體更新您的網絡管理卡，這將幫助您確保修正已知漏洞以及功能是最新，免遭受零時差攻擊(Zero-Day Attack)。

- **停用 HTTP 使用 HTTPS**

因 HTTP 為明碼傳輸，攻擊者可透過監聽通信來獲取信息，例如用戶名稱、密碼，從而獲得未經授權的權限，為了獲得更可靠和加密的通信通道，台達強烈建議禁用 HTTP（如果已啟用）並啟用 HTTPS。

- **上傳自定義 HTTPS 網路憑證**

台達設備中的預設 HTTPS 憑證不適用於部署作業與後續營運，應予以替換。台達建議您將設備配置使用 OpenSSL 創建自定義憑證或使用信譽良好的認證機構（CA）發行的憑證或企業 CA 發行的憑證，以建立瀏覽器和網站伺服器之間的安全通道，提供伺服器身分鑑別及資料傳輸加密，並保護網路使用者所傳輸的個人資料(如帳號、密碼等)不被截取或竄改。

- **停用 Telnet 使用 SSH**

因 Telnet 為明碼傳輸，攻擊者可透過監聽通信來獲取信息，例如用戶名稱、密碼，從而獲得未經授權的權限，台達強烈建議停用 Telnet（如果已啟用）並啟用 SSH。

- **停用 FTP 使用 SFTP**

因 FTP 為明碼傳輸，攻擊者可透過監聽通信來獲取信息，例如用戶名稱、密碼，從而獲得未經授權的權限，為了獲得更可靠和加密的通信通道，台達強烈建議停用 FTP（如果已啟用），啟用 SFTP。

- **停用 SNMPv1、v2 使用 SNMPv3**

常見的 SNMP 攻擊與威脅如下：

1) 攻擊者通過修改發送數據包的來源 IP 地址來執行未經授權的管理操作，從而獲得授權用戶的權利。
2) 攻擊者通過監聽 NMS 和 SNMP 代理之間的通信來獲取信息，例如用戶名稱，密碼和社群(Community)字串，從而獲得未經授權的權限。
3) 攻擊者截取然後重新排序，延遲或重新傳輸 SNMP 消息，以影響正常操作，直到獲得未授權的訪問權限。

SNMP 用於管理網絡設備，並具有三個版本：SNMPv1，SNMPv2 和 SNMPv3。SNMPv1 和 SNMPv2 安全性較低，僅以社群(Community)字串限制可以訪問該交換機的 NMS 和節點。

SNMPv3 支持基於用戶的安全模型（USM），提供 MD5、SHA、DES、AES 加密演算法，通過對通信數據進行身份驗證和加密，SNMPv3 解決了偽裝，篡改和洩漏等安全問題。

因此，若設備需要使用 SNMP 進行通訊，台達建議使用 SNMPv3，因為它比 SNMPv1/v2 更安全。如果使用 SNMPv1/v2，建議指定管理主機 IP 地址，啟用唯

讀權限並重新設定強度較高的社群(Community)字串，禁止使用預設或常見的字串，如”public”。

- **停用 Modbus TCP**

Modbus TCP 協定具明碼傳輸、廣播 (Broadcast) 機制及缺乏身份認證等特性，特別容易遭到攻擊。不建議使用 Modbus TCP，若需要啟用請管理(限制)Modbus 主機 IP 位址並啟用唯讀權限。

- **使用自定義通訊埠**

為了預防被惡意監聽預設標準通訊埠，請改用自定義通訊埠，這適用於 HTTPS，SSH，SFTP，SMTP 等協議。

- **修改預設帳戶與密碼**

安裝配置完成後，請更改默認的管理員、設備管理者與一般用戶帳戶和密碼並確保密碼足夠安全，密碼編碼原則可參閱第五章節的用戶訪問管理。

- **使用 SNTP**

啟用 SNTP 並確保已啟用網路的設備系統時間與當前網路時間正確同步。從而使設備可以將事件記錄在日誌檔案中以跟蹤問題。

- **停用 NBNS 服務**

NBNS 服務允許您的設備回應主機名，建議禁用此功能以增強設備安全性。

- **實施來源零信任機制**

設備提供網路監控服務時，建議使用已提供的白名單機制，僅允許名單內的來源進行讀取。

- **預設禁用/關閉 USB 介面**

USB 介面除了進行設備維護需求，建議關閉或禁用 USB 介面。

- **避免(或禁用)使用遠端操作服務**

遠端操作服務(如 SSH) 提供安全的資料傳輸協定通道，在系統 Shell 層(命令列介面)上實現資料交換的功能；相對的，也提供駭客嘗試入侵的管道之一。盡量避免使用類似的服務。

2.4 網路的安全

將台達網路(卡)設備部署到作業環境時，台達強烈建議進行以下關鍵配置更改：

- **防火牆**

台達強烈建議不要將設備暴露在公共網路，而應部署在有狀態封包檢查防火牆(SPI)，以監控傳入和傳出網路流量，並設定規則決定允許或封鎖特定流量。

- **網路分段**

平面式的網路體系結構將使惡意行為者更容易在網路中移動。藉由網路分段可以通過啟用或拒絕網路訪問來控制對敏感數據的訪問，從而增強網路安全性。

強大的安全策略要求根據不同的安全要求將網路劃分為多個區域，並嚴格執行允許區域之間移動的策略。台達強烈建議將設備管理介面上的網絡流量在物理上或邏輯上與普通網路分開。

- **建議使用實體網路**

使用無線電波進行通訊時，只要路由器的設定不完全，且第三方也在通訊範圍內的話，機敏資訊就容易被盜取。監控設備網路的使用，台達建議使用有線網路做為資料傳輸媒介，如 Ethernet Cable 或 RS-485 實體線路。

- **WIFI 無線網路使用建議**

若因監控環境限制，需要使用 WIFI 無線網路做為資料傳輸媒介，台達強烈建議禁止將設備連結至公用無線(網路)基地台。若監控系統，需使用無線網路基地台與設備

進行通訊與資料傳輸，應部署具備防火牆、監控網路流量、能夠設定規則決定允許或封鎖特定流量等功能的無線基地台，且為了防止遭竊聽並提升設備資訊安全性，台達建議 WIFI 安全部署與建置如下：

1) 使用 WPA2(含)以上的無線加密協定或 VPN 通訊。

2) 關閉無線基地台的 SSID 廣播功能，以免連線資訊暴露於公共空間。

3) 使用加密的通信協議，如 VPN、HTTPS 等，尤其針對具備機密資料的傳遞。

4) 針對無線(網路)基地台或設備的韌體/驅動，請定期同步至官方網站版次。

5) 建議在目標無線存取點場域的周邊牆壁建置金屬網以隔離外部干擾。

- **其他安全檢測和監控工具**

台達建議通過適當的物理，技術和管理工具來保護和監視環境，以進行網路入侵監視。

3. 通過憑證和金鑰進行身份驗證

驗證用戶或網路設備的身份，密碼通常用於識別用戶。但是，對於網絡管理卡和設備之間的通信，需要更嚴格的安全認證方法。

- **Secure Sockets Layer / Transport Layer Security (SSL/TLS)**

SSL/TLS 是一種使用數位憑證進行身份驗證的技術，可確保 Web 訪問的安全性並保護在兩個系統之間發送不被監聽通信並獲取的敏感資料。

數位憑證是由憑證認證機構（CA）頒發的，作為公共密鑰基礎結構的一部分，其數位簽章必須與管理卡或設備上伺服器憑證的數位簽章匹配。

- **Secure SHell (SSH)**

SSH 用於遠端終端訪問網卡或設備的命令界面，使用公共金鑰進行身份驗證。

3.1 建立私有 HTTPS SSL 憑證檔案(PEM 格式)

確保具有網絡功能的設備和工作站之間的連接安全性，可創建一個私有的 SSL 憑證。 請從以下位置下載並安裝 OpenSSL 工具包 http://www.openssl.org. 啟動 Shell 或 DOS 命令模式，參考以下命令創建私有的憑證檔案：

```
openssl req –x509 –nodes –days 3650 –newkey rsa:1024 –keyout cert.pem –out cert.pem
```

按照指示進行操作，完成後將在當前工作目錄中創建一個名為 cert.pem 的檔案。透過 Web 介面將 cert.pem 上載到啟用了網絡的設備（以管理員權限登錄）。

3.2 建立 SSH 金鑰

1) 請從下列網站下載並安裝 PuTTY：http://www.putty.org.

2) 從安裝目錄中執行 puttygen.exe

3) 從工具列 Key 下拉選項選擇 SSH-2 RSA，點擊 Generate -> “產生私密金鑰組”以

生成 RSA 金鑰。

4) 點選 Conversions→Export OpenSSH key，然後為 RSA 金鑰命名。當提示您提供金鑰密碼時，請忽略它。

5) 從工具列 Key 下拉選項選擇 SSH-2 DSA，點擊 Generate-> “產生私密金鑰組”以生成 DSA 金鑰。

6) 點選 Conversions→Export OpenSSH key，然後為 DSA 金鑰命名。當提示您提供金鑰密碼時，請忽略它。

7) 從文本中複製生成的金鑰，貼到文字編輯器並另存文字檔。

8) 透過 Web 介面將 DSA 及 RSA 公共金鑰檔案上傳到啟用網路的設備。

4. 產品安全維運和管理建議

攻擊面是攻擊者可以利用的所有網路設備潛在缺陷和技術後門的組合。這些組合可能以多種方式發生，包括：

- 默認密碼。
- 未修補的軟體和韌體漏洞。
- 配置不當的，防火牆，端口，服務器，交換機，路由器或基礎架構的其他部分。
- 未加密的網絡流量或靜態數據。
- 權限訪問控制的缺失或不足。

維運安全與管理目標是通過消除潛在的**攻擊面**，並減少系統的攻擊面來降低安全風險。建議項目如下：

- 審核您的現有系統：

  對您現有的系統進行全面的審核。使用滲透測試，漏洞掃描，配置管理和其他安全審核工具來查找網路監控系統中的缺陷並確定修復的優先級。

- 立即修補漏洞：

  確保所有網路設備軟(韌)體已更新至最新的版本。

- 網路強化：

  確保正確配置防火牆，並定期審核所有規則；關閉任何未使用或不需要的網路通訊端口；禁用所有網路設備不必要的協議和服務；建立遠端訪問清單，並使用加密通訊協議通訊，例如 HTTPS, SSH, SFTP。

- 服務器加強：

  將所有網路設備置於安全的數據中心；避免在網路設備上安裝不必要的軟體；確保正確設定管理用戶，並根據最小權限原則限制權限和訪問。

- 應用程序加強：

刪除所有網路設備預設密碼。並通過應用程序密碼管理/權限密碼管理解決方案來管理應用程序密碼，該解決方案可實施密碼最佳實施(密碼輪換，長度要求等)。

- 刪除不必要的帳戶和權限：

通過在整個 IT 基礎架構中刪除不必要的帳戶(例如，未使用的帳戶)和權限，以強制執行最低權限。

5. 用戶訪問管理

用戶訪問管理（UAM），也稱為身份和訪問管理（IAM），使各個用戶權限適當的訪問或控制他們所需項目；最高管理員(用戶)透過以下任務，增加設備的資訊網路安全：

- 為每個設備角色修改帳號與密碼。
- 根據需要維護(運)或網路服務需求，依據本文件建議項目進行設置。
- 利用密碼管理政策，加強密碼的強度。

5.1 設備用戶權限政策

用戶訪問管理依權限與操作需求，區分一般使用者、設備操作者與系統管理員三種身份，以確保訪問/控制他們所需的設備項目。

使用者為設備管理人員，需控制相關設備，台達建議授與設備操作者權限；使用者為系統管理人員，需設定設備網路服務、帳號密碼管理等項目，台達建議授與系統管理員權限；使用者非設備管理人員與系統管理員，台達強烈建議僅授與一般使用者權限。

5.2 密碼管理政策

台達建議制訂密碼管理流程，設備於安裝後，強烈建議修改每個角色預設密碼，免遭受暴力破解或其它手法進行攻擊。密碼強度，指一個密碼對抗猜測或是暴力破解的有效程度。一般來說，指一個未授權的訪問者得到正確密碼的平均嘗試次數。密碼的強度和其長度、復雜度及不可預測度有關。

強密碼可以降低安全漏洞的整體風險。因此，台達建議至少每 90 天修改密碼一次，並遵循以下密碼編碼與管理原則，降低被破解風險。

- 密碼至少八個字元長度，且為數字與大小寫字母混合組合，並不能包含全部或部分的使用者名稱。
- 參閱 Windowns 作業系統-密碼必需符合複雜性需求，須符合下列最小需求: (A)

不包含使用者的帳戶名稱全名中, 超過兩個以上的連續字元. (B) 長度至少為 6 個字元. (C) 包含下列四種字元中的三種: (1) 英文大寫字元 (A 到 Z) (2) 英文小寫字元 (a 到 z). (3) 10 進位數字 (0 到 9). (4) 特殊符號等。

- 避免使用重複、過於簡單且易於猜測或與帳號相同的字母或數字(例如：aaa、abc、123...)。
- 避免使用他人容易取得之資料設為密碼(例如：英文名、生日或電話...等)。
- 勿與他人共用帳號密碼。
- 勿將密碼書寫並張貼於明顯處。

6. 設備除役

為防止已除役的設備洩漏您使用的帳號、密碼與歷史資料，請遵守以下操作：

6.1 清除歷史資料

請由 Web 介面登入，前往歷史紀錄設置頁面。按下清除事件紀錄與清除歷史紀錄按鈕將歷史紀錄清除。

6.2 清除所有設定

請由 Web 或 SSH 介面登入，尋找恢復預設值選項並按下此按鈕。恢復預設值選項將清除您所有設定包含帳號與密碼。

6.3 物理破壞

為避免設備儲存媒體內的資料被復原取得，建議委託專業資料銷毀業者進行硬體銷毀作業，以防止資料外洩。

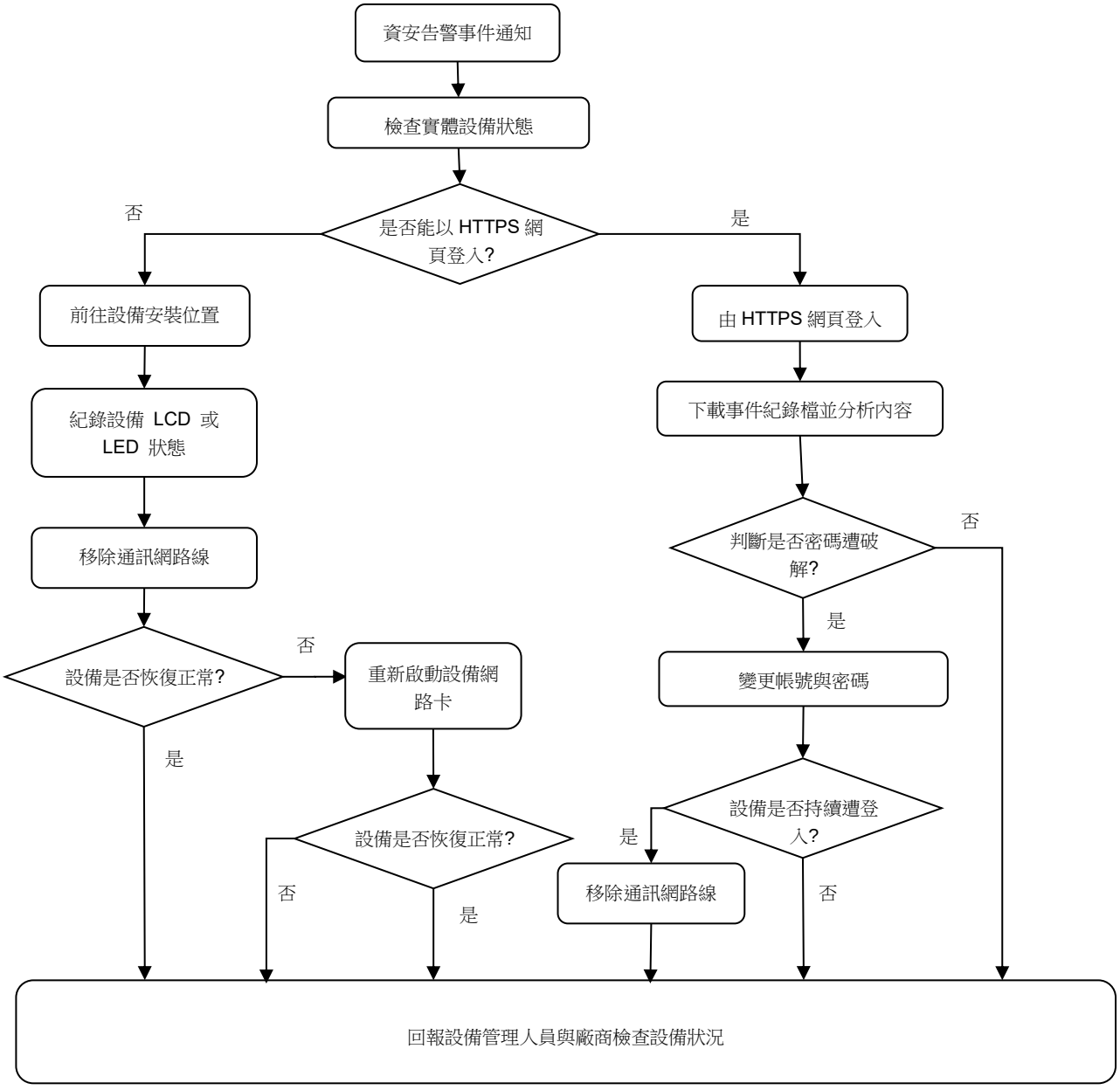
7. 資訊安全事件處理

當發生資安事件時，建議依照下方流程處理：

1. 確認受影響設備：當設備被入侵後，可能會進行對外攻擊行為，建議先確認受影響設備，並蒐集該設備之基本資訊，內容應包含實體主機 IP 位址、設備廠牌與機型、網際網路位址與程式版本。
2. 執行通報程序：判定為資安事件後，請依照貴單位規定執行內部通報程序，提供事件細節、影響等級和支援項目等資訊，並陸續回報後續處理情形。
3. 判斷與應變措施：建議包含下列工作。
   3.1 判斷是否需中斷受駭資訊設備的連線行為，其目的為避免機敏資料洩漏，減少因資安事件所造成之損害程度。
   3.2 判斷是否需停止受駭之設備所提供的網路服務，如：網站伺服器（Web Server）、SSH 或 FTP 等，其目的為縮小因此事件所造成之受駭範圍。
   3.3 確認設備的破壞程度，設備可能在被入侵或植入惡意程式後出現異常的網路連線情形，需確認其造成的破壞程度，例如：系統當機、網路癱瘓、資料毀損或網頁遭竄改。
   3.4 判斷事件影響等級，以該事件造成對資訊機密性、完整性及可用性的衝擊，綜合評估該事件的影響等級。
4. 釐清事件發生原因：每個資安事件的發生，其背後一定有特定的原因，管理人員可以透過分析其它網路設備的各種日誌檔，例如：網站伺服器、防火牆、DNS 伺服器、電子郵件伺服器、系統錯誤訊息，或是檢查受駭設備，找出資安事件發生的原因。例如：惡意程式、系統設定錯誤、應用程式弱點、人為因素等。在分析與釐清資安事件發生原因時，若管理人員遇到技術上的困難或問題，建議先向協力廠商尋求支援，進行數位鑑定，請其調查事件發生原因與提供解決方案。為了有利於後續分析與處理，請連絡台達電客服人員，並提

供**附錄 A-Delta RMA Analysis Request** 詳細撰寫相關資訊或事件紀錄，並寄送電子郵件至台達客戶服務電子郵件信箱(ups.taiwan@deltaww.com) 或至台達客服官網(https://www.deltaww.com/zh-TW/Customer-Service)，台達將以最迅速且優先分析與處理。

5. 參考復原建議：分析資安事件發生的原因後，應依事先準備的災害復原計畫進行回復作業。 以下是關於台達設備當發生資安事件時的檢查機制：



附錄 A-Delta RMA Analysis Request

日期：2020/03/26

填表人：王大同(Wang Datong)/ups.taiwan@deltaww.com

產品名稱與序號：DPS-200KVA GES204HH330009C

客戶別/地點：Delta/台南廠

網路卡軟體版本：Touch Panel or SNMP Card Version.

裝置韌體版本：Device FW Version (UPS, PDC, PDU, Cooling...)

發生頻率：Number of times per day? Number of times per week?

故障描述：Please describe in detail how to replicate this problem, including the network LED status, screenshots, photos...

Revision History

Name	Date	Reason For Changes	Version	Approve
Gary Chu	2020/10/06	First version	00	Jesse
Gary Chu	2021/01/05	修改第 5 章 用戶訪問管理	01	Jesse
Gary Chu	2021/01/22	修改第 2 章 物理的安全說明	02	Jesse
Richard Lin	2021/02/09	新增 6.3 物理破壞說明	03	Jesse
Richard Lin	2021/02/26	修改第 4 章 產品安全維運和管理建議	04	Jesse
Richard Lin	2021/03/19	新增第 7 章 資訊安全事件處理	05	Jesse
Richard Lin	2021/04/1	新增 2.1 產品使用情境	06	Jesse
Richard Lin	2021/5/6	新增 2.4 WIFI 無線網路 修改 2.1 產品使用情境示意圖(新增 Modbus Device)	07	Jesse
Gary Chu	2021/05/25	修正錯別字將只讀更正為唯讀	08	Jesse
Richard Lin	2021/08/04	新增 2.3 設備安全 – 零信任與關閉 USB 介面使用	09	Jesse
Richard Lin	2021/10/20	新增 2.3 設備安全 -避免(或禁用)使用遠端操作服務 新增 2.4 網路安全-建議使用實體網路 修改 7. 資訊安全事件處理內容 新增附錄 A-Delta RMA Analysis Request. 修改 2.2 物理安全。	10	Jesse