Delta Electronics, Inc

信息安全手册

关键基础设施

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

文件版本：v10

内容

1. 简介

本指南介绍内容适用于，台达网络管理卡和带有台达网络管理卡的嵌入式构件设备的安全功能。 这些功能使设备可以通过网络进行远程操作。

目的

本文介绍以下协议和功能，请选择适合您网络环境的协议和功能，以及在安全系统中如何设置和使用它们的方式：

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

此外，本指南记录如何强化台达网络管理卡，以增强设施的安全性。

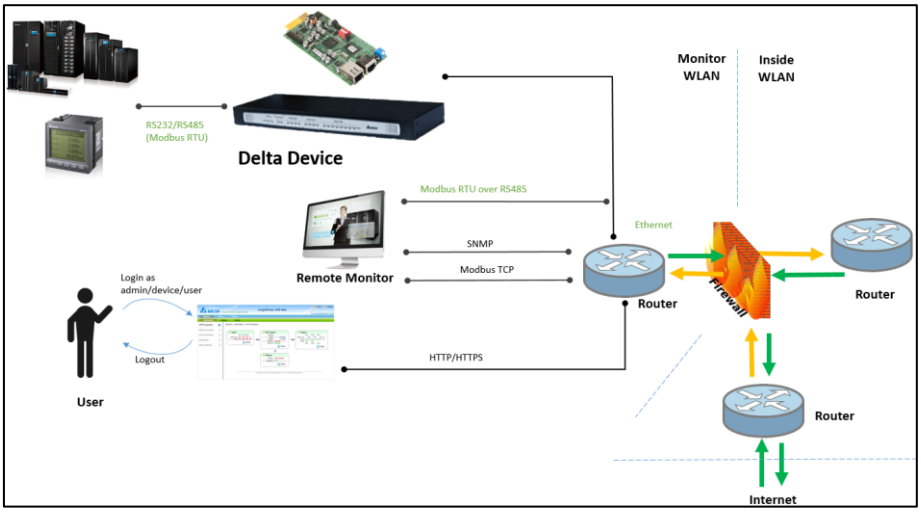
2. 设备安全部署指南

本文提供了一般性纵深防御安全指导，可帮助您根据特定的安全要求来决定适当的安全部署。在整个部署生命周期中维持安全性，需要考虑以下注意事项：

2.1 产品使用情境

设备拥有者部署台达产品，建议使用情境如下：

- 局域网络应独立分开，分为监控设备区网、内部办公区网与对外因特网。
- 分割后的子网之间通讯，应使用网络设备(如 Router)隔离，且网络设备应具基本信息安全防护功能，如防火墙、异常流量侦测与回报纪录等功能。



台达产品使用情境示意图

2.2 物理的安全

设备拥有者应保护启用的网络设备免受未经授权人的物理访问。

- 访问权限应仅限于需要维护设备的人员。
- 限制区应明确标明仅供授权人员使用。
- 限制区应上门锁。
- 进入限制区时应进行物理或电子审核追踪。
- 现场监控使用之接线插座(头)，应固定锁附与避免外露，并检查接线是否有破损，以防止有心人士接线进行侧录与攻击行为发生。

2.3 设备的安全

设备安全性包括以下几项：

- **使用最新版本韧体**

Delta Software Center 网站为您的设备网卡提供了最新韧体，请定期检查网站，并使用最新韧体更新您的网络管理卡，这将帮助您确保修正已知漏洞以及功能是最新，免遭受零时差攻击(Zero-Day Attack)。

- **停用 HTTP 使用 HTTPS**

因 HTTP 为明码传输，攻击者可透过监听通信来获取信息，例如用户名称、密码，从而获得未经授权的权限，为了获得更可靠和加密的通信通道，台达强烈建议禁用 HTTP（如果已启用）并启用 HTTPS。

- **上传自定义 HTTPS 网络凭证**

台达设备中的预设 HTTPS 凭证不适用于部署作业与后续营运，应予以替换。台达建议您将设备配置使用 OpenSSL 创建自定义凭证或使用信誉良好的认证机构（CA）发行的凭证或企业 CA 发行的凭证，以建立浏览器和网站服务器之间的安全通道，提供服务器身分鉴别及数据传输加密，并保护网络用户所传输的个人资料(如账号、密码等)不被截取或窜改。

- **停用 Telnet 使用 SSH**

因 Telnet 为明码传输，攻击者可透过监听通信来获取信息，例如用户名称、密码，从而获得未经授权的权限，台达强烈建议停用 Telnet（如果已启用）并启用 SSH。

- **停用 FTP 使用 SFTP**

因 FTP 为明码传输，攻击者可透过监听通信来获取信息，例如用户名称、密码，从而获得未经授权的权限，为了获得更可靠和加密的通信通道，台达强烈建议停用 FTP（如果已启用），启用 SFTP。

- **停用 SNMPv1、v2 使用 SNMPv3**

常见的 SNMP 攻击与威胁如下：

1) 攻击者通过修改发送数据包的来源 IP 地址来执行未经授权的管理操作，从而获得授权用户的权利。
2) 攻击者通过监听 NMS 和 SNMP 代理之间的通信来获取信息，例如用户名称，密码和社群(Community)字符串，从而获得未经授权的权限。
3) 攻击者截取然后重新排序，延迟或重新传输 SNMP 消息，以影响正常操作，直到获得未授权的访问权限。

SNMP 用于管理网络设备，并具有三个版本：SNMPv1，SNMPv2 和 SNMPv3。SNMPv1 和 SNMPv2 安全性较低，仅以社群(Community)字符串限制可以访问该交换机的 NMS 和节点。

SNMPv3 支持基于用户的安全模型（USM），提供 MD5、SHA、DES、AES 加密算法，通过对通信数据进行身份验证和加密，SNMPv3 解决了伪装，篡改和泄漏等安全问题。

因此，若设备需要使用 SNMP 进行通讯，台达建议使用 SNMPv3，因为它比 SNMPv1/v2 更安全。如果使用 SNMPv1/v2，建议指定管理主机 IP 地址，启用只读权限并重新设定强度较高的社群(Community)字符串，禁止使用默认或常见的字符串，如”public”。

- **停用 Modbus TCP**

Modbus TCP 协议具明码传输、广播 (Broadcast) 机制及缺乏身份认证等特性，特别容易遭到攻击。不建议使用 Modbus TCP，若需要启用请管理(限制)Modbus 主机 IP 地址并启用只读权限。

- **使用自定义通讯端口**

为了预防被恶意监听预设标准通讯端口，请改用自定义通讯端口，这适用于 HTTPS，SSH，SFTP，SMTP 等协议。

- **修改默认帐户与密码**

安装配置完成后，请更改默认的管理员、设备管理者与一般用户帐户和密码并确保密码足够安全，密码编码原则可参阅第五章节的用户访问管理。

- **使用 SNTP**

启用 SNTP 并确保已启用网络的设备系统时间与当前网络时间正确同步。从而使设备可以将事件记录在日志档案中以跟踪问题。

- **停用 NBNS 服务**

NBNS 服务允许您的设备响应主机名，建议禁用此功能以增强设备安全性。

- **实施来源零信任机制**

设备提供网络监控服务时，建议使用已提供的白名单机制，仅允许名单内的来源进行读取。

- **默认禁用/关闭 USB 界面**

USB 接口除了进行设备维护需求，建议关闭或禁用 USB 接口。

- **避免(或禁用)使用远程操作服务**

远程操作服务(如 SSH) 提供安全的数据传输协议信道，在系统 Shell 层(命令行接口)上实现数据交换的功能；相对的，也提供黑客尝试入侵的管道之一。尽量避免使用类似的服务。

2.4 网络的安全

将台达网络(卡)设备部署到作业环境时，台达强烈建议进行以下关键配置更改：

- **防火墙**

台达强烈建议不要将设备暴露在公共网络，而应部署在有状态封包检查防火墙（SPI），以监控传入和传出网络流量，并设定规则决定允许或封锁特定流量。

- **网络分段**

平面式的网络体系结构将使恶意行为者更容易在网络中移动。藉由网络分段可以通过启用或拒绝网络访问来控制对敏感数据的访问，从而增强网络安全性。

强大的安全策略要求根据不同的安全要求将网络划分为多个区域，并严格执行允许区域之间移动的策略。台达强烈建议将设备管理接口上的网络流量在物理上或逻辑上与普通网络分开。

- **建议使用实体网络**

使用无线电波进行通讯时，只要路由器的设定不完全，且第三方也在通讯范围内的话，机敏信息就容易被盗取。监控设备网络的使用，台达建议使用有线网络做为数据传输媒介，如 Ethernet Cable 或 RS-485 实体线路。

- **WIFI 无线网络使用建议**

若因监控环境限制，需要使用 WIFI 无线网络做为数据传输媒介，台达强烈建议禁止将设备链接至公用无线(网络)基地台。若监控系统，需使用无线网络基地台与设备进行通讯与数据传输，应部署具备防火墙、监控网络流量、能够设定规则决定允许或封锁特定流量等功能的无线基地台，且为了防止遭窃听并提升设备信息安全性，台达建议 WIFI 安全部署与建置如下：

1) 使用 WPA2(含)以上的无线加密协议或 VPN 通讯。
2) 关闭无线基地台的 SSID 广播功能，以免联机信息暴露于公共空间。
3) 使用加密的通信协议，如 VPN、HTTPS 等，尤其针对具备机密数据的传递。
4) 针对无线(网络)基地台或设备的韧体/驱动，请定期同步至官方网站版次。

5) 建议在目标无线存取点场域的周边墙壁建置金属网以隔离外部干扰。

- **其他安全检测和监控工具**

台达建议通过适当的物理，技术和管理工具来保护和监视环境，以进行网络入侵监视。

3. 通过凭证和密钥进行身份验证

验证用户或网络设备的身份，密码通常用于识别用户。但是，对于网络管理卡和设备之间的通信，需要更严格的安全认证方法。

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

SSL/TLS 是一种使用数字证书进行身份验证的技术，可确保 Web 访问的安全性并保护在两个系统之间发送不被监听通信并获取的敏感数据。

数字证书是由凭证认证机构（CA）颁发的，作为公共密钥基础结构的一部分，其数字签名必须与管理卡或设备上服务器证书的数字签名匹配。

- **Secure SHell (SSH)**

SSH 用于远程终端访问网卡或设备的命令界面，使用公共密钥进行身份验证。

3.1 建立私有 HTTPS SSL 凭证档案(PEM 格式)

确保具有网络功能的设备和工作站之间的连接安全性，可创建一个私有的 SSL 凭证。 请从以下位置下载并安装 OpenSSL 工具包 http://www.openssl.org. 启动 Shell 或 DOS 命令模式，参考以下命令创建私有的凭证档案：

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

按照指示进行操作，完成后将在当前工作目录中创建一个名为 cert.pem 的档案。透过 Web 接口将 cert.pem 上载到启用了网络的设备（以管理员权限登录）。

3.2 建立 SSH 密钥

1) 请从下列网站下载并安装 PuTTY：http://www.putty.org.

2) 从安装目录中执行 puttygen.exe

3) 从工具栏 Key 下拉选项选择 SSH-2 RSA，点击 Generate -> “产生私钥组”以生成 RSA 密钥。

4) 点选 Conversions→Export OpenSSH key，然后为 RSA 密钥命名。当提示您提供密钥密码时，请忽略它。

5) 从工具栏 Key 下拉选项选择 SSH-2 DSA，点击 Generate->“产生私钥组”以生成 DSA 密钥。

6) 点选 Conversions→Export OpenSSH key，然后为 DSA 密钥命名。当提示您提供密钥密码时，请忽略它。

7) 从文本中复制生成的密钥，贴到文本编辑器并另存文本文件。

8) 透过 Web 接口将 DSA 及 RSA 公共密钥档案上传到启用网络的设备。

4. 产品安全维运和管理建议

攻击面是攻击者可以利用的所有网络设备潜在缺陷和技术后门的组合。这些组合可能以多种方式发生，包括：

- 默认密码。
- 未修补的软件和韧体漏洞。
- 配置不当的，防火墙，端口，服务器，交换机，路由器或基础架构的其他部分。
- 未加密的网络流量或静态数据。
- 权限访问控制的缺失或不足。

维运安全与管理目标是通过消除潜在的**攻击面**，并减少系统的攻击面来降低安全风险。建议项目如下：

- 审核您的现有系统：

  对您现有的系统进行全面的审核。使用渗透测试，漏洞扫描，配置管理和其他安全审核工具来查找网络监控系统中的缺陷并确定修复的优先级。

- 立即修补漏洞：

  确保所有网络设备软(韧)体已更新至最新的版本。

- 网络强化：

  确保正确配置防火墙，并定期审核所有规则；关闭任何未使用或不需要的网络套接字口；禁用所有网络设备不必要的协议和服务；建立远程访问列表，并使用加密通讯协议通讯，例如 HTTPS, SSH, SFTP。

- 服务器加强：

  将所有网络设备置于安全的数据中心；避免在网络设备上安装不必要的软件；确保正确设定管理用户，并根据最小权限原则限制权限和访问。

- 应用程序加强：

  删除所有网络设备默认密码。并通过应用程序密码管理/权限密码管理解决方案来管理应用程序密码，该解决方案可实施密码最佳实施(密码轮换，长度要求等)。

- 删除不必要的账户和权限：

  通过在整个 IT 基础架构中删除不必要的账户(例如，未使用的账户)和权限，以强制执行

最低权限。

5. 用户访问管理

用户访问管理（UAM），也称为身份和访问管理（IAM），使各个用户权限适当的访问或控制他们所需项目；最高管理员(用户)透过以下任务，增加设备的信息网络安全：

- 为每个设备角色修改账号与密码。
- 根据需要维护(运)或网络服务需求，依据本文件建议项目进行设置。
- 利用密码管理政策，加强密码的强度。

5.1 设备用户权限政策

用户访问管理依权限与操作需求，区分一般使用者、设备操作者与系统管理员三种身份，以确保访问/控制他们所需的设备项目。

使用者为设备管理人员，需控制相关设备，台达建议授与设备操作者权限；用户为系统管理人员，需设定设备网络服务、账号密码管理等项目，台达建议授与系统管理员权限；用户非设备管理人员与系统管理员，台达强烈建议仅授与一般用户权力。

5.2 密码管理政策

台达建议制订密码管理流程，设备于安装后，强烈建议修改每个角色默认密码，免遭受暴力破解或其它手法进行攻击。密码强度，指一个密码对抗猜测或是暴力破解的有效程度。一般来说，指一个未授权的访问者得到正确密码的平均尝试次数。密码的强度和其长度、复杂度及不可预测度有关。

强密码可以降低安全漏洞的整体风险。因此，台达建议至少每 90 天修改密码一次，并遵循以下密码编码与管理原则，降低被破解风险。

- 密码至少八个字符长度，且为数字与大小写字母混合组合，并不能包含全部或部分的使用者名称。
- 参阅 Windowns 操作系统-密码必需符合复杂性需求，须符合下列最小需求: (A) 不包含使用者的账户名称全名中, 超过两个以上的连续字符. (B) 长度至少为 6 个字符. (C) 包含下列四种字符中的三种: (1) 英文大写字符 (A 到 Z) (2) 英文小写字符 (a 到 z). (3) 10 进位数字 (0 到 9). (4) 特殊符号等。

- 避免使用重复、过于简单且易于猜测或与账号相同的字母或数字(例如：aaa、abc、123...)。
- 避免使用他人容易取得之数据设为密码(例如：英文名、生日或电话...等）。
- 勿与他人共享账号密码。
- 勿将密码书写并张贴于明显处。

6. 设备除役

为防止已除役的设备泄漏您使用的账号、密码与历史数据，请遵守以下操作：

6.1 清除历史资料

请由 Web 接口登入，前往历史纪录设置页面。按下清除事件纪录与清除历史纪录按钮将历史纪录清除。

6.2 清除所有设定

请由 Web 或 SSH 接口登入，寻找恢复默认值选项并按下此按钮。恢复默认值选项将清除您所有设定包含账号与密码。

6.3 物理破坏

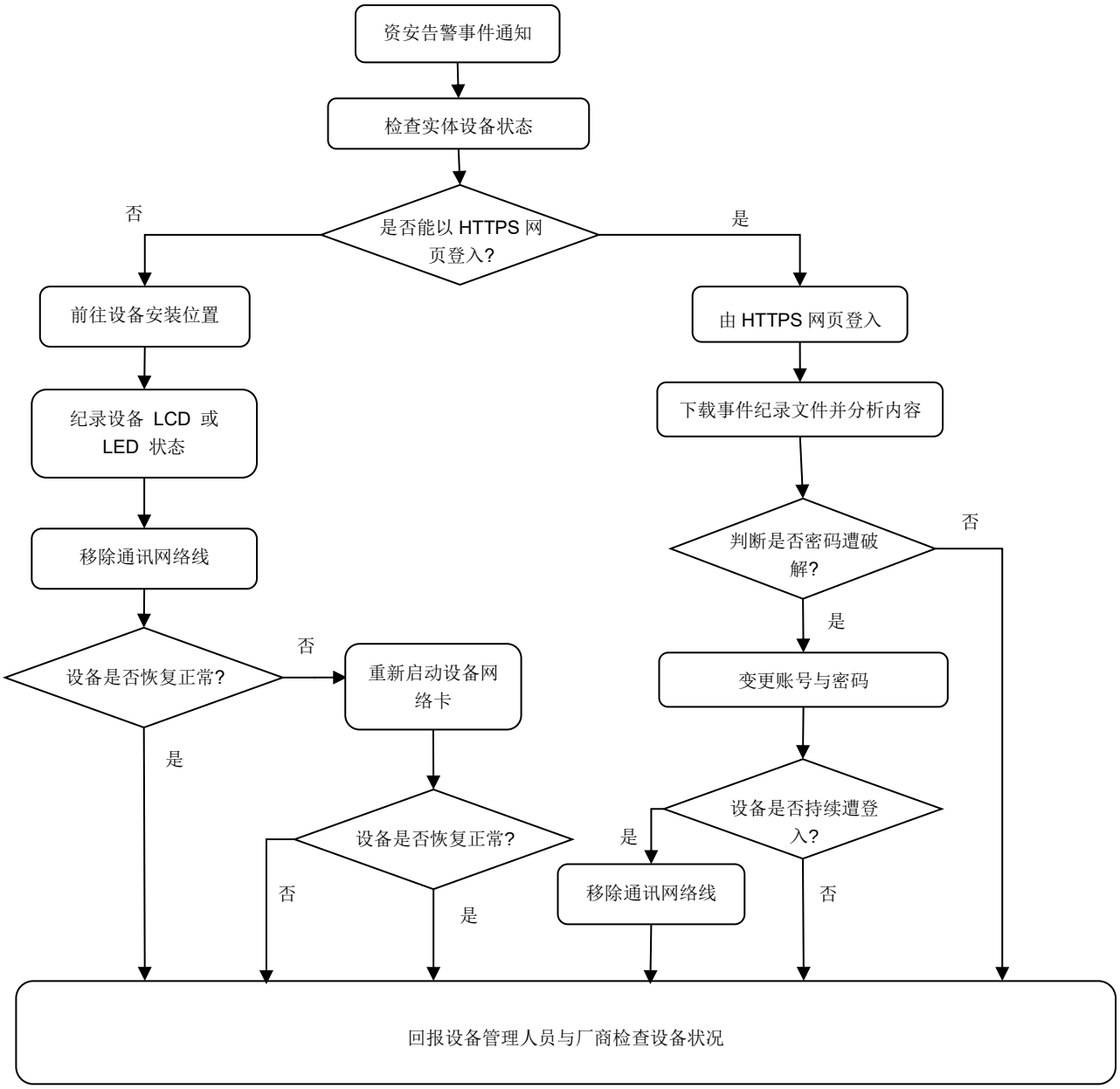
为避免设备储存媒体内的数据被复原取得，建议委托专业数据销毁业者进行硬件销毁作业，以防止数据外泄。

7. 信息安全事件处理

当发生资安事件时，建议依照下方流程处理：

1. 确认受影响设备：当设备被入侵后，可能会进行对外攻击行为，建议先确认受影响设备，并搜集该设备之基本信息，内容应包含实体主机 IP 地址、设备厂牌与机型、因特网地址与程序版本。
2. 执行通报程序：判定为资安事件后，请依照贵单位规定执行内部通报程序，提供事件细节、影响等级和支持项目等信息，并陆续回报后续处理情形。
3. 判断与应变措施：建议包含下列工作。
   - 3.1 判断是否需中断受骇信息设备的联机行为，其目的为避免机敏数据泄漏，减少因资安事件所造成之损害程度。
   - 3.2 判断是否需停止受骇之设备所提供的网络服务，如：网站服务器（Web Server）、SSH 或 FTP 等，其目的为缩小因此事件所造成之受骇范围。
   - 3.3 确认设备的破坏程度，设备可能在被入侵或植入恶意软件后出现异常的网络联机情形，需确认其造成的破坏程度，例如：系统当机、网络瘫痪、数据毁损或网页遭窜改。
   - 3.4 判断事件影响等级，以该事件造成对信息机密性、完整性及可用性的冲击，综合评估该事件的影响等级。
4. 厘清事件发生原因：每个资安事件的发生，其背后一定有特定的原因，管理人员可以透过分析其它网络设备的各种日志文件，例如：网站服务器、防火墙、DNS 服务器、电子邮件服务器、系统错误讯息，或是检查受骇设备，找出资安事件发生的原因。例如：恶意软件、系统设定错误、应用程序弱点、人为因素等。在分析与厘清资安事件发生原因时，若管理人员遇到技术上的困难或问题，建议先向第三方寻求支持，进行数字鉴定，请其调查事件发生原因与提供解决方案。为了有利于后续分析与处理，请连络台达电客服人员，并提供**附录 A-Delta RMA Analysis Request** 详细撰写相关信息或事件纪录，并寄送电子邮件至台达客户服务电子邮件信箱或至台达客服官网(https://www.delta-china.com.cn/zh-CN/customerService_Products)，台达将以最迅速且优先分析与处理。
5. 参考复原建议：分析资安事件发生的原因后，应依事先准备的灾害复原计划进行回复作

业。 以下是关于台达设备当发生资安事件时的检查机制：



附录 A-Delta RMA Analysis Request

日期：2020/03/26

填表人：王大同/ups.taiwan@deltaww.com

产品名称与序号：DPS-200KVA GES204HH330009C

客户别/地点：Delta/台南厂

网络卡固件版本：Touch Panel or SNMP Card Version.

装置固件版本：Device FW Version (UPS, PDC, PDU, Cooling...)

发生频率：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...