Delta Electronics, Inc.

Security Handbook

Mission Critical Infrastructure

Model: InsightPower IPv6 Card, AIO Card, SNMP G3 Mini Card, EMS2000, Device Touch Panel
Doc. Version: v.10

Contents

1. Introduction

This guide describes the security features applicable to Delta Network Management Cards and devices with embedded components of Delta Network Management Cards. These functions enable devices to operate remotely through network.

1.1 Purpose of this Guide

This document introduces the following protocols and functions in the security system. Please choose the suitable protocols and functions for your network environment.

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

Furthermore, this guide documents how to enhance Delta network management cards, improving the security of your facilities.

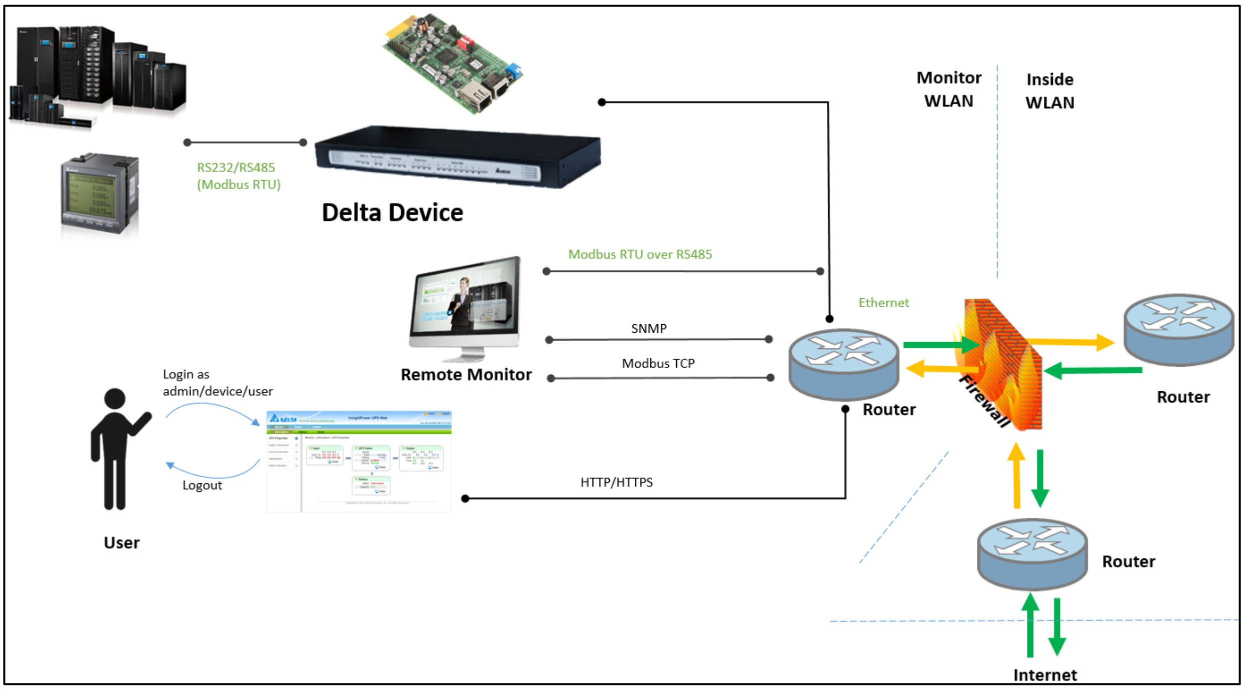
2. Security Deployment Guide

This article provides general defense-in-depth security guidance to help users decide on the appropriate security deployment based on specific security requirements. To maintain security throughout the device life cycle, please note the following:

2.1 User Environment

It is recommended that users deploy Delta products in an environment with the following conditions:

- The local area network (LAN) for monitored devices, office network and external network should be separated.
- The communication between subnetworks should be isolated with network devices, e.g., routers, which have basic information security functions such as firewall, abnormal network traffic detection and recording.



Delta Product User Envrionment

2.2 Physical Environment

The device owner should protect the network enabled device from unauthorized physical access.

- Access should be restricted to those who require access to maintain the equipment.

- Restricted areas should be clearly marked for authorized personnel only.
- Restricted areas should be secured by locked doors.
- A physical or electronic audit trail should be conducted when entering the restricted zone.
- Wiring sockets and plugs used for on-site monitoring should be locked and avoid exposure, and the wiring skin should be checked if there is damage, preventing the wiring from attacking.

2.2 Devices

Device security includes the following:

- **Firmware updates**

Delta Software Center website provides the latest firmware for your device network cards. Please regularly check on the website and update your network management cards with the latest firmware. This will help you ensure the security holes and features are up-to-date so that the system can prevent from Zero-Day Attack.

- **Disable HTTP and enable HTTPS**

The data transmission via HTTP is in plain text. This allows the attackers to obtain information such as username and password so that the system could be illegally accessed with unauthorized privilege. In order to obtain a more reliable and encrypted communication channel, it is strongly recommends to disable HTTP and enable HTTPS.

- **Upload a custom HTTPS certificate**

The default HTTPS certificate of Delta equipment is not suitable for deployment and subsequent operations and should be replaced. It is recommended to use OpenSSL to create a custom certificate or use a certificate issued by a reputable certification authority (CA) or an enterprise CA to establish a secure channel between the browser and server. This provides the server authentication and data transmission encryption, and protect personal data such as account numbers, passwords, etc.

- **Disable Telnet and enable SSH**

The data transmission via Telnet is in plain text. This allows the attackers to obtain information such as username and password so that the system could be illegally accessed with unauthorized privilege. In order to obtain a more reliable and encrypted communication channel, it is strongly recommends to disable Telnet and enable SSH.

- **Disable FTP and enable SFTP**

The data transmission via FTP is in plain text. This allows the attackers to obtain information such as usernams and passwors so that the system could be illegally accessed with unauthorized privilege. In order to obtain a more reliable and encrypted communication channel, it is strongly recommends to disable FTP and enable SFTP.

- **Disable SNMPv1, v2 and enable SNMPv3**

Common SNMP attacks and threats are as follows:

1) The attacker performs unauthorized management operations by modifying the source IP address of the data packet to illegally obtain the rights of authorized users.
2) The hacker obtains information such as user name, password, and community string by monitoring the communication between the NMS and the SNMP agent.
3) The attacker intercepts, delays, retransmits and re-sequences SNMP messages to affect normal operations.

SNMP is used to manage network devices, there are SNMPv1, SNMPv2 and SNMPv3. SNMPv1 and SNMPv2 have lower security, which only use community string to restrict the NMS and nodes that can access the switch.

SNMPv3 supports user-based security model (USM) and provides MD5, SHA, DES, and AES encryption algorithms. Through authentication and encryption of communication data, SNMPv3 solves security problems such as camouflage, tampering, and leakage.

Therefore, if the devices need to be communicated with SNMP, Delta recommends SNMPv3 since it is more secure than SNMPv1 and SNMPv2.

For users of SNMPv1 or SNMPv2, it is recommended to specify the IP address of the host, enable read-only permission and reconfigure a stronger community string, and prohibit the use of default or common strings, such as "public".

- **Disable Modbus TCP**

The Modbus TCP protocol is easier to be attacked since it is broadcast in plain text and lack of identity authentication. It is not recommended to use Modbus TCP. If you still need to enable it, please restrict the Modbus host IP address and set the permission read-only.

- **Use custom network ports**

To prevent malicious monitoring of the default standard communication ports, for HTTPS, SSH, SFTP, SMTP protocols, please use custom communication ports.

- **Change default account and password**

After the device installation and configuration are completed, please change the default administrator, device manager and general user accounts and passwords. Also, please make sure that the passwords are secure enough. For the password setting principles, please refer to the user access management in Chapter 5.

- **Enable SNTP**

Please enable SNTP and make sure that the system time is correctly synchronized with the current network time. This helps the devices to record events with correct time.

- **Disable NBNS Service**

The NetBIOS Name Service (NBNS) allows your device to respond the hostname. It is recommended to disable this feature to enhance device security.

- **Implement Zero-trust Mechanism**

If the device provides network monitoring service, it is recommended to set up a whitelist and allow the users to read from specific sources.

- **Disable/Close USB interface**

Unless there is device maintenance requirements, it is recommended to disable or close the USB interface.

- **Disable or Avoid Using Remote Access**

Remote Access Service, e.g., SSH, provides a secure data transmission tunnel, which enables the data exchange function. On the other hand, it also becomes a weakness that hackers may try to attack at. Therefore, please avoid using this kind of services.

2.3 Network

When deploying a Network Card to a production environment, Delta strongly recommends that the below key configuration changes are made.

- **Firewall**

It is strongly suggested not to expose devices to a public network. Instead, the devices should be deployed in a stateful packet inspection firewall (SPI) to monitor incoming and outgoing network traffic, and set rules to allow or block specific traffic.

- **Network Segmentation**

A flat network architecture will make it easier for hackers to intercept data on the network. With network segmentation, the network security will be enhanced by enabling or denying network access to sensitive data.

A strong security policy requires that the network be divided into multiple areas according to different security requirements. A policy that allows movement between these areas should be strictly enforced. It is strongly recommended that the network traffic on the device management interface be physically or logically isolated from normal network.

- **Use Physical Network**

When using radio waves for communication, sensitive information could easily be stolen if the router settings are incomplete. For the use of monitored devices, it is recommended that data transmited via physical network, e.g., Ethernet cables or RS-485 cables.

- **Suggestions for Using Wi-Fi Network**

When Wi-Fi network is required due to the limitation of the monitoring environment, it is strongly recommended that the devices not to be connected to public Wi-Fi network. If the monitoring system needs wireless network station for transmitting data with the devices, the deployment of firewall, network traffic detection and management are necessary. To prevent eavesdropping and improve equipment information security, Delta suggests the users to follow the Wi-Fi security deployment as below:

1) Use WPA2 or higher level of wireless encryption protocol or VPN communication.

2) Disable the SSID broadcasting function of wireless access points to avoid exposing connection information to public spaces.

3) Use encrypted protocols, e.g., VPN and HTTPS, especially for the transmission of confidential information.

4) Please regularly update the firmware/drivers of your wireless access points or devices to the latest version.

5) It is recommended to build a metal mesh on the surrounding walls of the target wireless access point field to isolate external interference.

- **Other Security Detection and Monitoring Tools**

It is recommended to protect and monitor network environment through appropriate, physical, technical, and management tools.

3. Authentication by Certificates and Host Keys

Authentication verifies the identity of users or network devices. Passwords are often used for identifying users. However, for communication between Network Management Cards and devices, stricter security authentication method is required.

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

  SSL/TLS is the technology uses digital certificates for authentication to keep Web access secure and protect sensitive data sent between two systems. A digital CA root certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Management Card or device.

- **Secure SHell (SSH)**

  SSH is used for remote terminal access to the command line interface of the network card or device, uses a public host key for authentication.

3.1 Generate a private SSL certificate file (in PEM format) for HTTPS

To ensure connection security between network enabled devices and your workstation, you can create a private SSL certificate file. Please download and install OpenSSL Toolkit from http://www.openssl.org. Launch Shell or DOS prompt mode, and refer to the following command to create your own certificate file:

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

Then, proceed with the given directions. When it is completed, a file named **cert.pem** will be created in the current working directory.

Upload **cert.pem** to the network enabled device through web interface (Login with Administrator privilege).

3.2 Create a SSH Host Key

1) Please download and install PuTTY at: http://www.putty.org
2) Run **puttygen.exe** from the installed directory.
3) Select SSH-2 RSA from the Parameters area and click Key → Generate key pair to generate

a RSA key.

4) Click Conversions → Export OpenSSH Key and assign a filename to the RSA key. Please ignore it when prompted to provide key passphrase.

5) Select SSH-2 DSA from the Parameters, click Key → Generate key pair to generate a DSA key.

6) Click Conversions → Export OpenSSH Key and assign a filename to the DSA key. Please ignore it when prompted to provide key passphrase.

7) Copy the generated key from the text box, paste in a text editor and save as a text file.

8) Upload the DSA/ RSA/ Public keys files to the network enabled device through web interface.

4. Suggestions of Product Security Operation and Management

An **Attack Surface** is the total sum of device potential flaws and technical backdoors. This can be occurred in a variety of ways:

- Default password
- Unfixed software and firmware security vulnerabilities.
- Improperly configured firewalls, ports, servers, switches, routers or other parts of the infrastructure.
- Unencrypted network traffic or static data.
- Lack or inadequacy of privileged access control.

The goal of maintenance security and management is to reduce security risks by eliminating the potential attack surface and reducing the attack surface of the system. The following are the suggested actions:

- Review your current system

  Comprehensively review your system with specific tools, e.g., penetration testing, vulnerability scanning, configuration management and other security audit tools. This will help the users to find defects in the network monitoring system and decide the priority of repairs.

- Fix vulnerabilities immediately

  Make sure all software and firmware of network devices have been updated to the latest version.

- Network enhancement

  Ensure that the firewall is properly configured and regularly review all setting rules; close any unused or unnecessary network communication ports; disable all unnecessary protocols and services; establish a remote access list and use encrypted communication protocols for communication, such as HTTPS, SSH, SFTP.

- Enhance the servers

  Deploy all network devices in a secure data center; avoid installing unnecessary software on network equipment; ensure that the users are set correctly, and restrict permissions and access according to the principle of least privilege.

- Application enhancement

Delete all default passwords of network devices. In addition, use the application password management/authority password management solution to manage the passwords of applications. Password setting policies such as changing period and length requirements can also enhance the security of applications.

- Remove the unnecessary accounts and privilege settings

Delete unnecessary/unused accounts and permissions in the IT infrastructure.

5. User Access Management

User Access Management (UAM), also known as identity and access management (IAM), is the administration of giving each user an appropriate system access or control permissions; the highest administrator (user) enhances the network security of devices through the following:

- Modify the account and password for each device.
- For the requirements of maintenance (operation) or network service, please use settings according to the listed items in this document.
- Use password management policies to enhance password strength.

5.1 Device User Privilege Policies

For user access management, there are three types of identities: Common users, device operators, and system administrators based on permissions and operational requirements to ensure access/control of the devices they need.

For device management users, it is recommended to provide them device operator permission; for system managers, it is required to provide them system administrator permission; if the user is neither the device manager nor the system administrator, it is strongly recommended to only provide common user permission to him/her.

5.2 Password Management Policy

It is strongly recommended for users to change the login passwords to prevent from being brute-forcing attacked by hacker tools or techniques. Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. Generally speaking, it means the average times of login attempts by an unauthorized visitor to get the correct password. The strength of a password is related to its length, complexity and unpredictability. A strong password lowers the risks of security vulnerabilities. Therefore, Delta recommends that the password be at least 8 characters long, and be a combination of numbers and uppercase and lowercase letters to reduce the risk of being cracked. Also, it is recommended to change the password at least once every quarter.

- ■ The passwords must be at least 8 characters long. It should be a combination of digits, Uppercase and Lowercase characters. Also, it should not contain all or part of the account name.

- Please refer to Microsoft Windows Documentation: **Password must meet complexity requirements security** policy setting. The password should meet the following minimum requirements: (A) Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). (B) At least 6 characters long. (C) Contains three of the following four categories:

  (1) Uppercase letters of European languages (A through Z)

  (2) Lowercase letters of European languages (a through z).

  (3) Decimal numbers (0 to 9).

  (4) Special characters.
- Avoid using letters or numbers that are repetitive, too simple, easy to guess, or the same as account (e.g., aaa, abc or 123).
- Do not use personal information (e.g., name, birthday or phone number) as your password.
- Do not share your account and password to others.
- Do not record the password in any place where others can easily find it.

6. Decommission Devices

To prevent the decommissioned equipment from leaking your account, password and historical data, please follow the following operations:

6.1 Clear Historical Data

Please log in from the web interface and go to the history setting page. Press the clear event log and clear history data button to clear the history record.

6.2 Clear All Settings

Please log in from the Web or SSH interface, look for the option to restore defaults and click this button. The Restore Defaults option will clear all your settings including account and password.

6.3 Physical Destruction

To prevent the data in the storage of devices from being recovered, it is recommended to entrust a professional data destruction and disposal service company to perform hardware destruction operations to prevent data leakage.

7. Information Security Event Handling

When an information security incident occurs, it is recommended to follow the process below:

1. **Confirm the affected devices:**
   When a device is invaded, it may cause external attacks. It is recommended to confirm the affected devices first and collect the basic information of the devices, including the host IP address, brand, model and program version.

2. **Notification procedures:**
   When it is confirmed to be an information security incident, start notifying your internal organizations. Please also provide information on the details of the incident, level of impact and supported items. Please continue to report the follow-up processing situation.

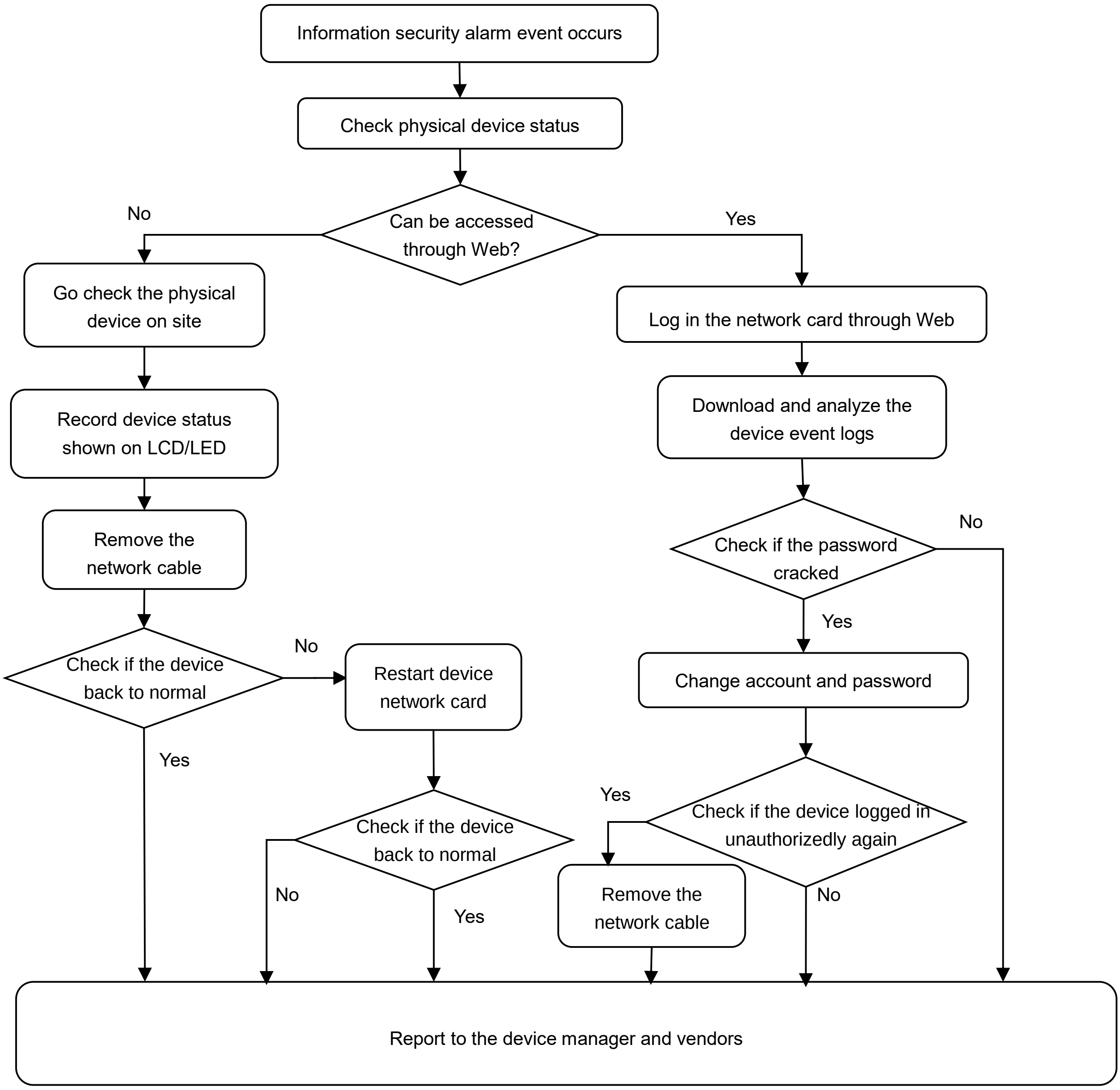
3. **Judge and reaction steps:**
   3.1 Decide if the device connection needs to be stopped. The purpose is to avoid the leakage of sensitive data and reduce the damage caused by information security incidents.
   3.2 Decide if the network service (e.g., such as Web Server, SSH or FTP) of devices needs to be stopped. The purpose is to reduce the scope of the damage caused by the incidents.
   3.3 Confirm the degree of damage. The device may have abnormal network connection after being hacked or implanted with malicious programs. It is necessary to confirm the degree of damage caused, such as system crash, network paralysis, data corruption, or web page being tampered.
   3.4 Comprehensively evaluate the impact level based on the impact on the confidentiality, integrity and availability of the information caused by the incident.

4. **Clarify the cause of the incident:**
   An information security incident has its specific causes. The system managers can analyze the log files from the network devices, such as website servers, firewalls, DNS servers, e-mail server, system error messages, or check the hacked device to find out the cause of the security incident. For example, malicious programs, system configuration errors, application weaknesses, human factors, etc. If the system managers face technical difficulties or problems, please ask for support from third-party vendors. They will help you to investigate the cause and provide solutions. For a better further analysis, please contact Delta customer service. We will quickly provide support and process your issues.

Please contact Delta customer service at: https://www.deltaww.com/en-US/Customer-Service

5. Suggestions for Recovery:

After analyzing the cause of information security incident, the recovery should be proceeded in accordance with the disaster recovery plan. Please refer to the following inpection process when an information security incident occurs:


Information security alarm event occurs
Check physical device status
Can be accessed through Web?
No
Yes
Go check the physical device on site
Log in the network card through Web
Record device status shown on LCD/LED
Download and analyze the device event logs
Remove the network cable
Check if the password cracked
No
Yes
Check if the device back to normal
No
Restart device network card
Change account and password
Yes
Yes
Check if the device logged in unauthorizedly again
Check if the device back to normal
No
Remove the network cable
No
Yes
Report to the device manager and vendors

Appendix A-Delta RMA Analysis Request

Date: 2020/03/26

Filler: John.Tseng / name@company.com

Product Model Name / Part Number: DPS-200KVA GES204HH330009C

Customer / Location: Power SI / USA, California

SNMP Card SW Version: Touch Panel or SNMP Card Version.

Device FW Version: Device FW Version (UPS, PDC, PDU, Cooling...)

Frequency of Occurrence: Number of times per day? Number of times per week?

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