



DELTA ELECTRONICS, INC.

DIView X Security Guidelines

Web Site: [Delta Electronics Global | Intelligent, Sustainable, Connecting](#)

Advisory: [Product Security Advisory](#)

Reporting: [Product Security Vulnerability Reporting](#)

Policy: [Product Security Vulnerability Handling Policy](#)

Email: Delta.PSIRT@deltaww.com

Document Version Control	4
1 Overview	4
1.1 Purpose.....	4
1.2 Scope of application	4
1.3 Use cases.....	4
1.4 Usage environment.....	5
1.5 Security assumptions	5
1.6 Document relationships.....	6
1.7 Terms and definitions	6
1.8 Reference documents.....	7
2 Deployment Environment Security Requirements.....	8
2.1 Division of security domains.....	8
2.2 Boundary protection	10
2.3 Physical and endpoint security	11
2.4 Defense in Depth	12
3 Secure Installation.....	13
3.1 Installation package and component verification.....	13
3.2 Minimize installation and component convergence	13
3.3 Initial reinforcement.....	14
3.4 Installation exception handling.....	14
4 Safety Configuration Baseline.....	15
4.1 Security threats and mitigation measures	15
4.2 DIAView X native security features	16
4.2.1 Project password configuration	16
4.2.2 Account and user permission configuration.....	16
4.2.3 HMI Server secure configuration	17

4.2.4 Configuration script security limits	18
4.2.5 Audit Log Management.....	18
4.2.6 Communication and data security	19
5 Operations and Maintenance Security Management.....	22
5.1 Defense in Depth	22
5.1.1 Network layer defense.....	22
5.1.2 Console layer defense.....	23
5.1.3 Data layer defense	23
5.1.4 Physical layer defense	23
5.1.5 Personnel and process defense	24
5.2 Hardened for adaptation to operating systems and network environments	24
5.3 Operations and maintenance security baseline	25
5.4 Account and permission management.....	26
5.5 Operation and maintenance red line	26
5.6 Version and patch management	27
5.6.1 Regular updates.....	27
5.7 Update exception handling.....	28
6 Retirement and Data Destruction	28
6.1 Business migration and offline management.....	28
6.2 Permissions and authorization cleanup	28
6.3 Data and engineering destruction	28
6.4 Residual risk management	29
7 Incidents and Vulnerability Reporting.....	29
7.1 Emergency response.....	29
7.2 Vulnerability reporting	29
7.3 Vulnerability disclosure	30

8 Third-Party Component and Product Vulnerability Management.....	30
8.1 Third-party component vulnerability management.....	30
8.2 Product vulnerability management	30
9 End User Responsibility	31
10 Document Maintenance.....	31

Document Version Control

Version number	Revision date	Revision notes
1.0	2026-09-30	First compilation

1 Overview

1.1 Purpose

The formulation of this guide follows the industrial control system security development process and references the requirements of cybersecurity regulations, defining the threat response scope of DIAView X and guiding installation, debugging, verification, and maintenance of DIAView X; At the same time, this document provides supporting guidance in conjunction with the "DIAView X 1.0 User Manual" for system integrators and end users to reference.

1.2 Scope of application

The applicable subjects of this article include equipment and personnel:

Supported components: real-time database, runtime, configuration development terminal, web monitoring server, IO communication suite.

Applicable personnel: system integrators, asset owners, operations and maintenance personnel

This article applies to DIAView X v1.0 and later compatible versions. The security hardening of PLC/sub-computer firmware itself is not covered by this guide.

1.3 Use cases

The DIAView X system is used for automation monitoring and operation and maintenance management on industrial production sites, including equipment data collection, process screen monitoring, production status display, alarm prompts, parameter viewing, and engineering configuration maintenance. Typical usage scenarios:

1. Configuration engineers edit, upload, and update project configuration files at the intranet workstation
2. On-site operators monitor production footage in real time, view alarms, and query historical data
3. System administrators configure account permissions, maintain system security parameters, and audit logs

4. The server continuously communicates with the field controller, completing real-time data collection and status synchronization

1.4 Usage environment

1. Network environment

The product can be deployed on industrial control local area networks; After users configure boundary security devices, it supports external web access.

Intranet scenario: Server and web client interact within the industrial control intranet, with logical isolation recommended between the intranet and office network.

External network access scenarios: The server side is not directly exposed to the public network; external access requires users to pre-deploy security gateways (VPNs, reverse proxies, etc.).

2. Hardware environment

The server is deployed in the data center industrial control computer/industrial server; The web client can run on operation stations, office PCs or remote terminal browsers.

3. Software environment

The server host operating system is Windows/Linux, providing HTTPS and WebSocket services to external systems for web interface interaction and project file management; Clients access web pages using mainstream browsers.

1.5 Security assumptions

The effectiveness of this product's security capability is based on the following security assumptions:

1. The system completes security domain division and network boundary protection according to guidelines, implements physical and terminal security, and adopts a Defense in depth architecture.
2. Before installation, verify the integrity of the installation package and perform minimal installation and initial system hardening.
3. Configure security parameters such as account, permissions, logs, and communication according to DIAView X's native security baseline.
4. During the operations and maintenance phase, continuous implementation of multi-layered in-depth defense measures for networks, hosts, data, physical, and personnel processes.
5. Establish a version and patch management mechanism to carry out routine updates and handle update anomalies.

1.6 Document relationships

This article is based on industrial control system security standards, aiming to help users understand DIAView X's threat protection capabilities and guide software security deployment, configuration, and operation and maintenance operations.

The "DIAView X 1.0 User Manual" is a fundamental software reference document used for functional learning and engineering configuration development guidance. It provides detailed explanations for core functions such as software interface layout, communication configuration, screen configuration, variable dictionary, alarm system, historical data, recipe management, and user permissions, providing a complete software operation guide.

1.7 Terms and definitions

Terminology	Definition
Admin	Built-in user with administrator privileges.
Administrator	Roles with administrator privileges.
RBAC	Role-based access control core idea: permissions are assigned to roles, roles are assigned to users, and users obtain permissions through roles rather than direct authorization.
DIASudio	Provides integrated selection and setting software tools for equipment and system integration, including commonly used programmable controllers (PLCs), human-machine interfaces (HMI), servo drive systems, and frequency converters. Completes product selection, PLC programming, product parameter setting, equipment setup, and HMI planning for customers on a single platform, simplifying and accelerating the system development process.
Authentication	Verify the declared identity of the entity.
Cybersecurity	Ensuring the confidentiality, integrity, and availability of information in cyberspace.
Defense in Depth	A design that employs multiple independent protective measures to resist various system attacks.
Least Privilege	Basic security principle: Users (personnel, software processes, devices) should be assigned minimum permissions matching the tasks and functions they undertake.
Threat	It may adversely affect business operations (including tasks, functions, image, or reputation), assets, control systems, or personnel through unauthorized access, destruction, information leakage, data tampering, and/or denial of service.

Vulnerability	1. Defects or weaknesses present in system design, implementation, operation, and management that can be exploited to compromise system integrity or violate security policies. 2. Weaknesses present in the functions, processes, internal controls, or implementations of the Industrial Automation Control System (IACS); These weaknesses can be exploited or triggered by threat sources. Weaknesses can be intentionally implanted by computer components (such as remote port access) or accidentally introduced at any stage of the product lifecycle.
DMZ	An isolated area located between the internal trusted network and the external untrusted network is used to place servers that need to provide external services, allowing external access while preventing direct contact with the internal network.
Zone	Purdue model security zoning
Conduits	Communication channels between partitions, including firewalls, gateways, and other boundary devices
Jump Server	Operations and maintenance redirect to the server
Data Diode	One-way data transmission hardware device
HMI	Human-machine interface
IPC	Industrial computers

1.8 Reference documents

Terminology	Definition
IEC 62443-2-1	Establish safety procedures for industrial automation and control systems
IEC 62443-3-2	Security risk assessment for system design
IEC 62443-3-3	System safety requirements and safety levels
IEC 62443-4-1	System security development process

2 Deployment Environment Security Requirements

This paper follows the relevant standards for regional and pipeline safety models, and combines the ISA-95 standard model for enterprise system and control system integration. Based on asset significance, core business functions, and risk impact scope, the DIAView X industrial control monitoring system is comprehensively configured with network security protection configurations such as secure zone division, security boundary isolation, and network port convergence, while also implementing physical security measures such as anti-prying and anti-extraction for equipment.

2.1 Division of security domains

Figure 1 shows engineering practices for dividing control systems into zones and interconnecting them through Conduits. Viewing your control system from this perspective helps focus on the security protection of each channel, prevents unauthorized intrusions, and facilitates assigning various devices to appropriate zones. The concepts related to zones and channels, as well as the process for evaluating them in system design, are explained in detail in the Zone and Pipeline Safety Model Standard. For compliance security assessments of systems under construction, please refer to this standard. This section only provides a brief overview of some basic concepts to help understand the following content of this document. Within the same region, devices have unified security requirements, and there is a certain degree of mutual trust between devices, but there is no trust in devices within other regions. Channels between zones establish trust between interconnected areas through isolation mechanisms, cross-zone network traffic control, and provision of network traffic monitoring points. The specific deployment details for each region are as follows:

1. Factory site area

Each network area in the factory is interconnected using firewalls and routers, which not only enables access to I/O devices but also distributes data collected from a specific area I/O point to other business areas.

The factory area in this diagram includes I/O devices and their corresponding control units. In practical engineering scenarios, RTUs and PLCs are usually not deployed in the SCADA equipment area but are installed on remote sites. In this scenario, RTU/PLC should be divided into independent security domains, with dedicated controlled communication channels configured to facilitate data exchange with the SCADA domain, ensuring communication process security.

Even if RTUs and PLCs are deployed in the SCADA local area, communication channels to the factory site area still require protection and continuous monitoring to promptly identify abnormal network traffic with intrusion characteristics. Communication links accessing the factory area are strictly controlled

and only allow network packets necessary for business operations. In addition to network protection, physical security measures corresponding to the factory area must be implemented, such as access control, card swiping, password keypads, and other methods to control personnel access permissions

2. SCADA monitoring area

Deploys the DIAView X core server and real-time database to achieve real-time production line monitoring, process alarm management, and on-site process data storage. This layer is only responsible for device-level monitoring and supervision control.

3. Control area

Control areas are equipped with devices used for system maintenance and, in some scenarios, system operations. Entrances and exits are protected by firewalls, allowing access to SCADA areas and other areas as needed.

Note: This area can only be connected to higher areas via firewalls and Plant DMZ; there is no direct connection channel.

4. Factory isolation zone

Servers within the factory isolation zone are used to isolate between high and low areas. The factory isolation area can deploy monitoring servers, network traffic servers, and external device gateways. Jump servers are generally used as authentication and permission authorization nodes, allowing enterprise and DMZ isolation areas to access lower areas. Data Diodes can be deployed to enable data to flow unidirectionally from SCADA areas to internet-facing servers in the DMZ. When used together with firewalls, network monitoring can be achieved to mitigate risks caused by DMZ servers or enterprise zone devices being compromised.

5. Corporate area

The enterprise area consists of non-control system devices, such as office desktops and laptops. Control system data and reports exported from the SCADA or control area to the enterprise server can be viewed and analyzed in this area.

Please note: This diagram is not a design plan intended for direct use by your system.

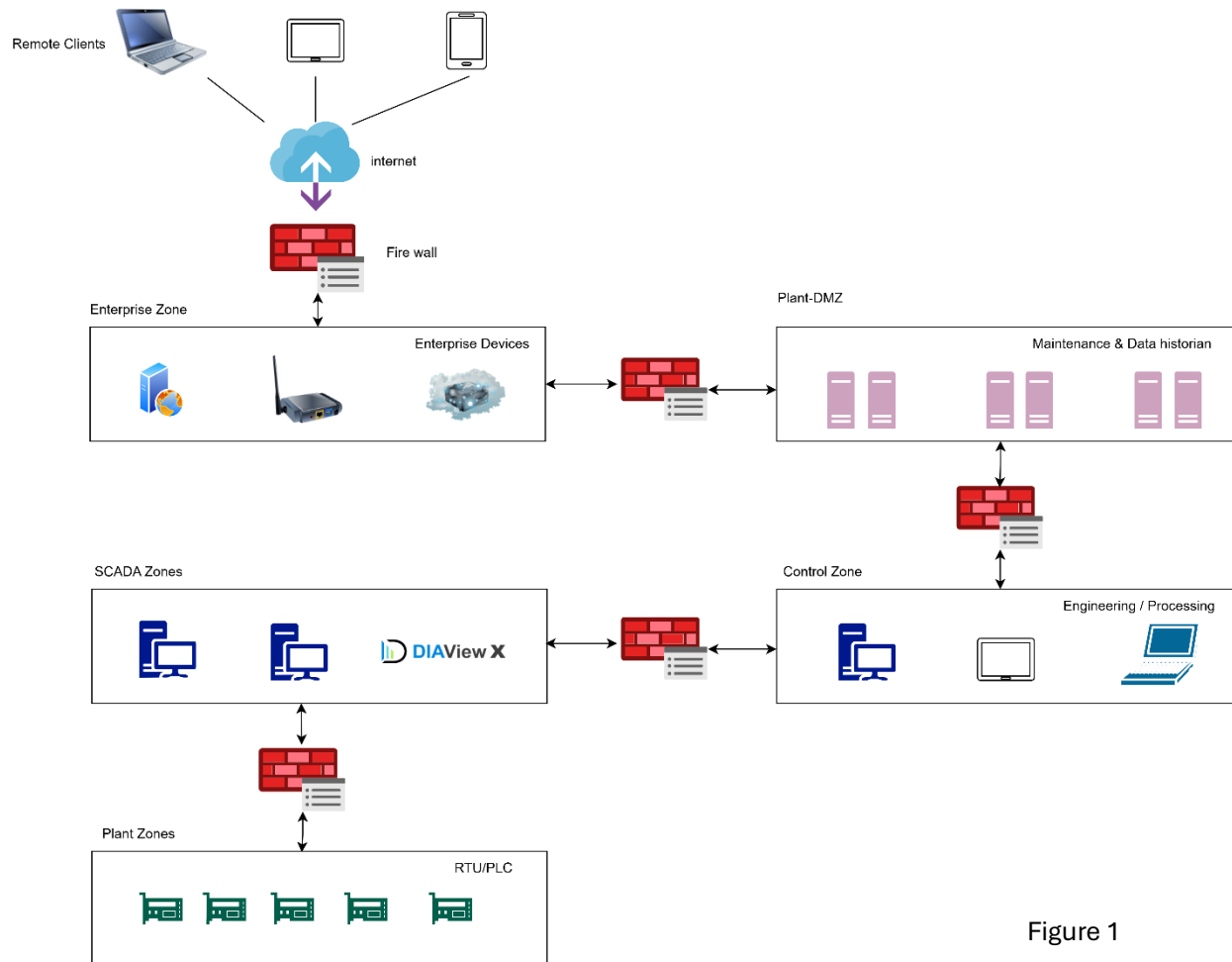


Figure 1

2.2 Boundary protection

This system follows the principle of least privilege when planning cross-area communication channels, executes port convergence policies on regional boundary protection devices, and only opens the necessary protocols and ports required for communication between the DIAView X system and PLC. Common communication protocols, services, default ports, and corresponding functions of DIAView X are described below:

Agreement/Service	Default port	Explanation
Server Manager / HMI Server	10090 / 8090	Configuring/running communication ports between client and DIAView X Server
DIAView X Config Web Server	6070	DIAView X Web Config Server is used to configure users, roles, and permissions during

		development, and to enforce HTTPS (TCP/6070)
Modbus TCP	502	Modbus Service is the built-in Modbus Slave service module of DIAView X, providing Modbus TCP services externally, receiving read/write requests from external Modbus masters and enabling data exchange.

▲ Security recommendation: Close all unused TCP/UDP ports and disable high-risk general protocols such as Telnet, FTP, and HTTP.

2.3 Physical and endpoint security

On the basis of implementing network logical isolation, physical layer security reinforcement should also be carried out as a foundational protection measure of the Defense in Depth. The specific requirements are as follows:

1. Data center environment protection

The DIAView X host computer and PLC control cabinet should be placed in an independent dedicated computer room, equipped with access control and video surveillance to achieve controllable access and traceable behavior.

2. Peripheral interface control

Physically block idle USB and serial ports of industrial computers; do not arbitrarily connect USB drives or other removable storage media. If needed, please confirm that the scan is virus-free before activating. Use tamper-evident tags to record device activation status to prevent unauthorized access.

3. Physical protection of network ports

The service network ports of DIAView X running host machines and core switches should be equipped with cable locks and anti-theft and dustproof locks to prevent unauthorized cable unplugging and ports being illegally occupied.

4. Port access control

Switch ports must have IEEE 802.1X authentication and Port Security port security features enabled simultaneously to prevent unauthorized devices from accessing the network.

5. Asset ledger management

Establish and maintain a list of connectable devices for the site, including but not limited to: engineer stations, HMI, IPC, PLC, etc., with regular inventory checks and audits.

6. Personnel contact management

Core control hardware is limited to authorized operation and maintenance personnel. When external vendor personnel conduct on-site commissioning, a dedicated person must accompany the entire process.

2.4 Defense in Depth

Although DIAView X was developed following multi-layered security design principles, true security is more evident in actual product deployment. After deployment, the system must provide multiple layers of defense to ensure that even if one layer is breached, the others can continue to protect the system against attackers attempting to infiltrate further. These layers of defense can take various forms, including physical controls (such as controlling device access), technical controls (such as encryption and authentication), or administrative controls (such as audit logs and monitoring). Each layer plays a role in the overall security of the system to defend against various threats.

End users are responsible for properly assessing threats present in deployment systems, determining necessary security controls, and mitigating these threats. Since the threat landscape is not static, this process must be ongoing.

This document aims to clarify the security capabilities of DIAView X to help users assess the system's security capabilities, threats, and mitigation measures, thereby supporting secure system design.

The Defense in Depth Tier includes but is not limited to:

1. **Network layer defense:** Implement security zone division at this layer to build a network isolation defense line. Relying on firewalls, VLAN, VPN, IDS/IPS, and other devices to achieve network boundary protection. Through network segmentation, access control, and abnormal traffic monitoring, risks such as unauthorized access, port probing scanning, malicious attacks at the network level, and lateral infiltration are reduced.
2. **Host layer defense:** This layer focuses on ensuring the security of servers, engineer stations, and HMI industrial control hosts running DIAView X components. Key measures include minimizing installation, shutting down idle services and ports, file directory permission control, disabling insecure encryption suites, and endpoint protection. Operating system layer hardening to prevent threats such as unauthorized local access, denial of service, data tampering, session hijacking, and malicious code execution.
3. **Data layer defense:** This layer ensures the confidentiality and integrity of static data such as engineering files, configuration parameters, and historical process data. Main methods include encrypted storage, integrity verification, key directory permission restrictions, regular backups, and

version control. By protecting sensitive data, it resists threats such as data theft, unauthorized tampering, data corruption and loss, and ransomware encryption.

4. **Physical layer defense:** This layer controls physical access permissions to protect hardware infrastructure such as workstations, control rooms, PLCs, and network switches. Protective measures include physical access control, access control, and video surveillance systems. Strict physical access control is implemented for critical assets, enabling countermeasures against equipment theft, malicious tampering with hardware wiring, unauthorized external devices, and other security threats.
5. **DIASView X Application Hardening:** This layer fully enables built-in software security features, such as forced HTTPS release, secure access policies, strong authentication, RBAC permission control, traffic control, and configuration script security restrictions. Relying on application layer security capabilities, it defends against man-in-the-middle attacks, XSS attacks, resource exhaustion, path traversal, unauthorized operations, and other malicious attacks targeting business applications.
6. **Personnel and process defense:** Technical protection cannot fully offset human risks. Supporting management systems, personnel training, separation of responsibilities, audits, and supplier management server as important supplements to technical protection, reducing security risks caused by maloperations, internal malicious operations, and lack of process control.

3 Secure Installation

3.1 Installation package and component verification

The download, installation, and upgrade operations of DIASView X software are managed uniformly by the official tool DIAInstaller, with the entire process standardized and executed.

DIAInstaller Operation Process:

1. Pre-deploy the DIAInstaller tool
2. Launch DIAInstaller and log in to the official Delta DIASstudio account
3. Check the DIASView X product in the [All Applications] list
4. Click Download and Install to complete the software deployment

3.2 Minimize installation and component convergence

To reduce the risk of system attacks, follow these principles during installation:

1. Install as needed

Only install functional components, database services, and system dependencies necessary for business operation. Deploying DIAView X Builder, demo projects, and related databases in production environments is strictly prohibited.

2. Reduce the attack surface

Each additional component means introducing potential vulnerabilities and maintenance costs. After installation, unused components, plugins, and services in the system are identified, idle components are uninstalled, and services temporarily unused are disabled.

3.3 Initial reinforcement

After software installation is complete, the following security configuration operations must be strictly followed to solidify the system's operational safety baseline:

1. Confirm that the software is the latest version

After installation, verify the software version and confirm that the current installed version is the latest official release released by the official source:

- 1) Visit the official software website to check the latest version of the number
- 2) Open the installed DIAView X Builder, go to the [Help - About] page, check the current software version number, and compare it with the latest version
- 3) If it is detected that the currently installed version is not the latest, you must upgrade to the latest version through official channels
- 4) After the upgrade is complete, confirm the version number is the latest official release again and check whether the installation package files have DELTA ELECTRONICS, INC. digital signatures

2. Change the administrator account password and enable password security policies

After installation, immediately change the DIAView X built-in administrator password and uniformly configure the password security control policy:

- 5) Enable password strength
- 6) Set the maximum lifecycle of the password
- 7) Force unlock password history
- 8) Set a threshold for password errors.

To change your account password, please refer to Chapter 14 — Users of the DIAView X 1.0 User Manual.

3.4 Installation exception handling

If errors, installation interruptions, or missing dependencies (including .NET Framework, Visual C++ Runtime, etc.) occur during installation, ignoring the exception and continuing installation is strictly

prohibited. The current installation process must be terminated immediately, and issues such as installation permissions, dependency library integrity, and dependency version matching must be checked item by item. Install again after the fault is fully resolved. If installation still cannot be completed after troubleshooting, please contact the official technical support team for assistance.

4 Safety Configuration Baseline

4.1 Security threats and mitigation measures

DIASView X offers a rich set of security mechanisms, but the security of industrial control systems depends on the combination of "product capability" and "deployment environment." The table below summarizes the potential security threats faced in the DIASView X operating environment and guides you in building a defense-in-depth system by configuring the security features in subsequent chapters.

Threat categories	Potential risk description	Mitigation measures
Abuse of identity and authority	Using default passwords or weak passwords, unauthorized operations, or internal maloperation can lead to system takeovers.	Refer to 4.2.1
Communication eavesdropping and tampering	Man-in-the-middle (MITM) attacks and network sniffing can lead to the leakage or tampering of sensitive data.	Refer to 4.2.4
Malicious attacks on the console layer	Ransomware, malware infections, and operating system vulnerabilities are exploited, causing system paralysis or data loss.	Refer to Section 5.2
Audit and retrospective failures	After a security incident occurs, traceability is impossible, and logs are tampered with or deleted by attackers, resulting in inability to define responsibility.	Refer to 4.2.5
Network layer denial of service	Network flooding attacks, port scanning, and unauthorized device access prevent legitimate users from accessing services.	Refer to Section 2.2
Abuse of privileged functions	Illegal modification of engineering logic and uncontrolled use of debugging tools in the production environment led to production interruptions.	Refer to 4.2.2
Physical access threats	Unauthorized external device access, hardware damage, and unauthorized physical contact bypass software-level defenses.	Refer to Section 2.3
Industrial control protocol layer attack	Attackers exploit vulnerabilities in industrial control protocols to bypass the application layer and directly issue malicious commands to PLCs.	Refer to 4.2.4
Supply chain and third-party risks	Third-party open-source components or underlying inventory are exploited through known vulnerabilities to carry out supply chain attacks.	Refer to Chapter 8
System retirement data leaks	When the system goes offline or the hard drive is scrapped, engineering data is not completely destroyed, leading to the leakage of trade secrets.	Refer to Chapter 6

4.2 DIAView X native security features

4.2.1 Project password configuration

1. Project code

To prevent unauthorized modifications to projects, DIAView X provides a project password feature. Users set a password for the current project, and after setting it, the correct password must be entered when reopening the project.

2. Download/upload password configuration

Project download is the process in DIAView X configuration software where the edited project files and related configuration data are transmitted from the design side to the target operating device or controller after completing local design and configuration; Project upload is the process of transferring the project files, configuration parameters, and related operational data that have been active on the target operating device or controller to the local design side. DIAView X supports setting project upload/download passwords to prevent unauthorized upload and download operations.

The default configuration of project passwords and download/upload passwords poses security risks.

Security recommendations are as follows:

Functional modules	Security risks	Safety advice
Enable password strength	Password strength is enabled by default, and all password complexity rules are enabled. Users can manually disable some password complexity rules or disable password strength.	Password strength is prohibited, and all password complexity rules must be enabled.
Project code	Not enabled by default	Enable engineering passwords and configure high-complexity passwords.
Download/upload password	Not enabled by default	Enable download/upload passwords and configure highly complex passwords.

4.2.2 Account and user permission configuration

DIAView X supports refined permission configuration, allowing users to customize and assign operational permissions based on their accounts, strictly controlling the system operations they can execute. The system adopts RBAC's permission management mechanism: multiple single permissions are integrated into dedicated roles to match the set of permissions required by positions. By assigning corresponding roles, users are quickly granted operational permissions that match business scenarios.

The default configuration of system accounts and user permissions poses certain security risks. To avoid risks such as permission abuse and unauthorized operations, this guide provides the following security configuration recommendations:

Functional modules	Security risks	Safety advice
Permission configuration	The built-in Administrator role has all permissions	Direct use of the Administrator role is prohibited; define roles according to the principle of least privilege.
Account configuration	The built-in Admin account uses a default random password and is visible to users during development	During configuration engineering, you must change the default password for the built-in Admin account.
	New accounts use default random passwords, which are visible to users during development	After adding a new user, you must change the user's initial random password.
	By default, the account will never be automatically canceled	Set the auto-logout duration
	By default, password security policies are not enabled	Activate a full set of password security policies

For account and permission configuration methods, please refer to Chapter 14 — Users of the DIAView X 1.0 User Manual.

4.2.3 HMI Server secure configuration

The security configuration of DIAView X Manager Server includes the maximum number of HTTP concurrent connections, the maximum number of concurrent requests per IP, and the size of the request content. The following concurrency and request size parameters are configured for HMI Server, not Manager Server.

Functional modules	Security risks	Safety advice
Maximum number of concurrent HTTP connections	The default is 256, which users can customize and modify, posing risks of exhausting total resources	Set reasonable values based on server performance and actual usage scenarios.
Maximum number of concurrent requests per IP	Default is 240 requests per 5 seconds; users can customize and modify them, but there is a risk of frequent requests.	Set reasonable values based on actual usage scenarios.
Maximum request payload size	The default is 30Mb, which users can customize and modify as needed, but there are risks of large packet attacks and buffer overflow.	Set reasonable values based on actual usage scenarios.

4.2.4 Configuration script security limits

DIASView X has built-in programmable extension modules based on JavaScript, serving as a supplement to basic visualization configurations, supporting configuration of control event scripts and scheduling backend scripts.

Scripts executed in DIASView X are strictly prohibited from interacting with the operating system in the following ways:

1. Invoke the operating system command-line interpreter (e.g., cmd.exe, powershell.exe, wscript.exe, cscript.exe)
2. Starting or invoking any external third-party executable programs (.exe .bat .cmd .msi, etc.)
3. Read and write files under the operating system key path (e.g., C:\Windows\System32, C:\Windows\SysWOW64, C:\Windows\System32\drivers, registry key values, etc.)

4.2.5 Audit Log Management

DIASView X provides operation log and alarm log functions. Operation log and alarm log data are stored in an external third-party database.

Based on the operation log and alarm log functions, the following security configuration recommendations are provided:

Functional modules	Security risks	Safety advice
Operation log	Disabled by default	Manual activation is forced. For how to enable operation logs, please refer to Chapter 8, Action in the DIASView X 1.0 User Manual
	Stored in databases, there is a risk of deletion or tampering	Preset log retention periods, disk capacity thresholds, and disk space insufficient strategies. For setting methods, refer to Chapter 11, Section 11.4 Database of the DIASView X 1.0 User Manual
Alarm log	Stored in databases, there is a risk of deletion or tampering	Same as above

▲ Security recommendation: For log storage and physical database files, operations personnel should set access permissions at the operating system level based on actual conditions to avoid database deletion or modification damage.

4.2.6 Communication and data security

OPC UA Client Communication

To ensure the confidentiality and integrity of OPC UA Client data transmission, DIAView X has multiple mandatory security configurations built in, as follows:

1. Forcibly enable OPC UA Client secure access policies to prevent communication without security policies.
2. By default, it uses the Basic256Sha256 encryption algorithm and SignAndEncrypt (signature and encryption) security mode.
3. Enable account identity verification and strictly prohibit anonymous access.
4. Forcing OPC UA Client certificate verification to achieve two-way authentication with OPC UA Server to intercept and reject untrusted, expired illegal certificates.

▲ Security recommendation: The system supports manual switching to the "None" communication mode. In this mode, data is unencrypted and transmitted in plaintext, posing significant risks of data leakage and tampering. It is strictly prohibited for use in formal production environments.

Remote web/app publishing

HTTP plaintext transmission carries security risks such as request parameter theft and data tampering. DIAView X forcibly enables HTTPS publishing by default and uses TLS 1.2 or above encryption protocols. This security policy applies uniformly to all web interfaces and API interfaces.

▲ Security recommendation: Users can manually disable HTTPS publishing. After turning it off, communication will use plaintext HTTP, which introduces serious security risks. It is not recommended to disable it in production environments.

RabbitMQ Client

RabbitMQ Client supports three authentication modes: anonymous authentication, username-password authentication, and certificate authentication, used to complete identity authentication with the RabbitMQ server. SSL/TLS is enabled by default, using certificate authentication mode for encrypted data transmission.

▲ Security recommendation: Users can manually disable SSL/TLS. After turning it off, data is transmitted in plaintext, posing a risk of malicious interception. Production environments must be used in conjunction with SSL/TLS.

Modbus Service

The Modbus protocol itself does not have built-in identity authentication, message verification, or encryption mechanisms, so identity credentials cannot be carried inside the protocol PDU. The system

lacks built-in IP filtering and Modbus message deep packet inspection (DPI) security control logic, posing risks of unauthorized access and unauthorized writing.

▲ Security recommendations: Industrial firewall/gateway configuration with trusted IP allowlist, unauthorized IPs directly blocked during TCP handshakes, supported by ARP spoofing prevention and device lifecycle management; Production environment port 502 strictly prohibited from direct exposure to untrusted networks; Regularly maintain gateway policies and allowlists, verify gateway operating status.

Notification email

When sending emails in plaintext SMTP, there is a risk that alarm information may be intercepted by third parties. The DIAView X alarm notification email server configuration is by default to require SSL/TLS encrypted transmission, sending alarm notification emails in encrypted form to prevent malicious theft of alarm information.

▲ Security recommendation: Users can manually disable SSL/TLS encrypted transmission. After turning it off, emails will be sent in plaintext, posing corresponding security risks. Do not disable this configuration in production environments.

System reinforcement

1. Windows operating system

To implement cryptographic security compliance requirements and avoid security risks such as man-in-the-middle attacks, data tampering, and encryption degradation caused by weak encryption algorithms and outdated TLS cryptographic suites, a special strengthening of TLS cryptographic suites will be carried out for Windows and Linux server operating systems according to the baseline requirements of the European Union Cybersecurity Agency (ENISA) "ECCG Agreed Cryptographic Mechanisms Version 3 (Draft)." It is recommended to disable the following cryptographic suites according to the baseline requirements:

Name
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_3DES_EDE_CBC_SHA

Hosts running the DIAView X service need to disable TLS-related password suites via Windows Group Policy, Registry, or PowerShell

Method 1: Group strategies

1. Press Win+R, run gpedit.msc to open the local Group Policy Editor;
2. Navigate to the path: Computer Configuration → Management Template → Network → SSL Configuration Settings
3. Double-click to open the SSL password suite sequence and select Enabled
4. In the SSL password package configuration box, clean and remove all insecure password packages
5. Click [OK] to save the configuration, then restart the server to make the policy permanently effective.

Method 2: PowerShell

Verification: List whether the currently enabled packages contain the recommended password packages

```
Get-TlsCipherSuite | Where-Object { $_. Name -match "CipherSuite Name" }
```

Disable the password suite (if it is included, then perform the disable operation).

```
Disable-TlsCipherSuite -Name "CipherSuite Name"
```

▲ Security recommendation: Before disabling the relevant password suite, please thoroughly assess and check whether the operation will affect compatibility with other system business functions. Only disable the device after confirming no business anomalies; For detailed configuration details, please refer to Microsoft's official operating system documentation

2. Linux operating system

In Linux environments, the unsecure encryption suite has been disabled at the program code level; For Ubuntu 20.04 and above, the insecure password suite is disabled by default

OPC UA Client, RabbitMQ Certificate Management Specification

The product only provides application-layer capabilities for certificate loading and certificate verification. Certificate issuance, management, maintenance of revocation lists, regular inspections, and expiration notifications fall under the on-site administrator's operational and maintenance responsibilities.

5 Operations and Maintenance Security Management

5.1 Defense in Depth

To effectively implement and continuously implement defense in depth strategies throughout the product lifecycle, enterprises should implement the following deployment and operation and maintenance security control measures. This section covers five major domains: physical layer, network layer, host operating system layer, data layer, and personnel and process management domain; The DIAView X application layer is the product's native security capability; configuration requirements refer to Chapter 4 Security Configuration Baseline. This section focuses on deployment and operation and maintenance practices across these five domains.

5.1.1 Network layer defense

1. Network segmentation: Implementing physical or logical isolation between IT networks and OT networks using firewalls, VLANs, or dedicated physical infrastructure, allowing only essential business traffic.
2. Firewall rules: Deploy firewalls at the OT network boundary, configure strict inbound and outbound access rules, and only open the necessary communication ports and IP addresses between DIAView X engineer stations, SCADA services, HMI clients, and on-site PLC/RTU devices.
3. Intrusion detection/defense system (IDS/IPS): Deploys IDS/IPS at critical network nodes to monitor abnormal traffic patterns and known attack characteristics; Triggers alarms or automatically blocks anomalies upon detection.
4. Virtual Private Network VPN: If remote maintenance is needed for DIAView X engineer stations or SCADA systems, a high-strength encrypted VPN must be used and multi-factor authentication MFA enabled.
5. MAC address filtering: Configure access restrictions at the switch level so that only devices pre-registered with MAC addresses are allowed to access OT control networks.

5.1.2 Host-based Defense

1. Operating System Hardening: Minimize installation on workstations and servers running DIAView X components (SCADA server, engineer station, HMI client), remove unnecessary services, close idle ports, and install the latest security patches.
2. Antivirus Software / Endpoint Detection and Response (EDR): Deploy legitimate antivirus software or advanced EDR endpoint protection solutions, regularly update the virus signature database, and continuously monitor abnormal host behavior.
3. Application Allowlist: Only pre-approved programs are allowed to run, such as DIAView X runtime components, engineering tools, and authorized auxiliary software, intercepting other unauthorized programs.
4. USB port control: Disable idle USB ports and enforce strict USB usage policies; Only encrypted USB drives approved by the IT/OT security team are allowed for SCADA project file transfers.
5. Host Firewall: Configure the system built-in firewall on the host hosting DIAView X to restrict application-level network connections.
6. Regular vulnerability scanning: Automated tools are used to regularly scan DIAView X servers, engineer stations, and HMI workstations to identify and fix operating system and application vulnerabilities.

5.1.3 Data layer defense

1. Encrypted storage: When storing project files, configuration databases, and historical data locally, DIAView X uses operating system-level encryption (BitLocker) or third-party encryption software to protect critical files.
2. Data Backup and Recovery: Regularly backing up DIAView X projects, configuration libraries, and historical archives off-site; Establishing strict backup management policies, conducting regular recovery tests, and handling data corruption and ransomware incidents.
3. Version Control System: Use Git or industrial control dedicated version control systems to manage DIAView X project files, fully recording every engineering modification, enabling operation traceability, version comparison, and fault rollback.

5.1.4 Physical layer defense

1. Restricting physical access: DIAView x SCADA servers, engineer workstations, HMI human-machine panels, on-site PLC/RTUs, and supporting network devices must be placed in controlled secure areas, such as locked cabinets or monitoring data centers.

2. Access control system: Uses card readers, biometric identification, and other means to manage and record personnel entering and exiting key areas.
3. Video Surveillance CCTV: Surveillance cameras are installed in key data centers, with recordings retained and regularly reviewed.
4. Physical lock mechanism: Install physical locks on cabinets, equipment chassis, and server racks to prevent unauthorized hardware access and wiring tampering.

5.1.5 Personnel and process defense

1. Security Awareness Training: Regular security training is provided to all personnel who encounter DIAView X (process engineers, operators, operations staff, IT personnel), covering OT threats, security policies, and best practices for operations and maintenance.
2. Security Policies and Operating Procedures: Develop implementable security policies and operational processes, covering SCADA software deployment, engineering configuration changes, password management, incident response, backup and recovery, and more.
3. Separation of responsibilities: Separate permissions for high-risk SCADA tasks, such as project modification and deployment of engineering equipment, and assigning different personnel to perform on-site hardware maintenance, eliminating single-point risks caused by high-risk individual operations and suppressing malicious operations.
4. Security audits and compliance: Regularly conduct internal or external security audits to verify system implementation and meet industry standards such as IEC 62443 and regulatory requirements.
5. Supplier Security Management: Assessing the security capabilities of SCADA and field equipment suppliers, requiring products to follow security design principles to ensure that DIAView X and supporting hardware receive timely security updates and vulnerability patches.

5.2 Hardened for adaptation to operating systems and network environments

DIAView X's own security capabilities have boundaries, and some threats require compensation and protection by relying on operating systems and boundary network devices. This section is a scenario-based supplement to 5.1 Defense in Depth, focusing on special implementation considerations for the industrial control environment where DIAView X operates, including antivirus software performance adaptation, allowlist deployment configuration, and deep monitoring of business traffic for lower-level PLCs.

Deployment of antivirus software for industrial computers

1. Install antivirus software compatible with industrial computer operating systems and update the virus signature database in real time.
2. Reasonably configure scanning strategies to avoid full-pan real-time scanning impacting business performance.
3. For the program directory and data storage directory of DIAView X, reasonable exclusion items are configured as needed to prevent accidental interception by virus software.

Regularly perform virus scans and removals, promptly handling viruses and malicious program alerts.

Industrial computer software allowlist

Uses a trusted app allowlist, allowing only authorized programs and blocking unauthorized ones.

Example: Use the system's built-in AppLocker to configure the software allowlist.

No additional installation required, flexible rules, supports setting rules for publisher, path, and hash value. Compatible with Windows 10/11 Enterprise/Education Edition, LTSC Edition, Windows Server.

Network-side exception write instruction monitoring

At the network boundary/industrial control network side, traffic auditing and intrusion monitoring devices should be deployed to monitor network packets flowing to this industrial control machine.

1. Write operation instructions to PLC/field device during unauthorized hours.
2. Exception writes instructions, exception file write requests, exception configuration modification instructions.
3. Abnormal frequency writes, abnormal batch writes, unauthorized write operations.
4. write requests for non-allowlist IPs/devices.

Operations and maintenance personnel regularly check network monitoring and alerts, promptly investigate the source of suspicious command writing behaviors, and carry out blocking and traceability measures.

5.3 Operations and maintenance security baseline

After DIAView X officially entered production and operation, regular security inspections were required to promptly detect safety hazards such as production interruptions, access anomalies, certificate invalidation, vulnerability risks, and log anomalies, ensuring business continuity and data security in the production environment.

Inspection work is carried out by operation and maintenance personnel; ordinary users are not recommended to perform safety inspections.

Inspections include daily, weekly, monthly, and special types:

Daily: DIAView X service process running status, CPU/memory/disk usage, login failures, permission changes, log anomalies.

Weekly: account and permission review, project backup validity, log spot checks.

Monthly: certificate validity, engineering backup and recovery drills, vulnerability scanning, and security policy validation.

Special: After version upgrades, configuration changes, or security incidents, special security review inspections are immediately carried out.

Inspections must record inspections, with responsible persons regularly reviewing inspection reports to supervise the closed loop of issues and provide resource support for safety rectification.

5.4 Account and permission management

1. Hierarchical user permission management

DIAView X achieves batch allocation and flexible adjustment of permissions through a "user-role-permission" association model. Users and permissions must be based on the principle of least privilege, allocating only the resources necessary for users to complete their work, preventing individual permissions from being too large.

It is recommended that operations personnel achieve hierarchical user permission management through flexible permission allocation:

Administrator: Has the highest permissions;

Engineer: Has configuration permissions but cannot manage accounts;

Operator: Runtime is focused on fixed workflows; modification of configuration engineering logic is strictly prohibited;

2. Accounts are cleaned regularly

A regular account cleanup mechanism should be established to reduce security risks caused by idle, expired, or resigned accounts not being handled in a timely manner:

- 1) Regular account inspections are conducted, and idle, expired, or resigned accounts are promptly suspended, recalled, or deleted
- 2) Check account permissions and promptly revoke permissions you no longer need
- 3) Keep records of account disposition, keeping operation logs of account disables, deletions, and changes for easier auditing and traceability

5.5 Operation and maintenance red line

1. Remote connection without authorization is strictly prohibited

2. It is strictly forbidden to insert USB drives or other portable storage media into industrial computers without authorization (if necessary, they must be scanned for viruses).
3. It is strictly forbidden to use default passwords or weak passwords in production environments

5.6 Version and patch management

5.6.1 Regular updates

DIASView X software is already in production environments, and installing software patches is the core method for fixing software vulnerabilities and ensuring stable production system operation; However, patch deployment is a high-risk operation, and patch updates can easily cause unplanned downtime. A strict, controlled, and rollable process must be established:

Internal verification by the DIASView X team

After patches are generated, the DIASView X team must conduct functional and compatibility testing to verify the patches.

Submission and approval

Patch files must have company-approved digital signatures clearly identifying fixed vulnerabilities and new features. Software updates must be approved by the person in charge.

Production environment validation

Direct testing on the production system is prohibited. A validator with exact matching hardware and software configurations for the production environment is required. Verify the integrity of patch files and perform installation on the validator using a system administrator account. After installation, restart the system and test the complete core business processes to confirm there are no errors or performance degradation.

Develop a patch update schedule

Specify the timing of software updates, the expected impact duration, downtime scope, and responsible personnel. Before updating, the production system must be fully backed up, hash values verified, and the allowlist and firewall temporarily disabled to ensure the installer can run smoothly.

Patch update

Normally stop the DIASView X service and related background processes, and run patch files or installation packages under the system administrator account. After installation, immediately restore the allowlist and firewall, run DIASView X, and test core functions.

Observation and rollback plans

After software updates, operations personnel must immediately arrive on-site to ensure the production system operates normally, strengthen inspections, and continuously monitor security event logs. If

abnormal production stoppages or shutdowns are detected, the rollback plan should be immediately initiated and the full disk backup image covered and restored using the full disk backup image described in "5.6.1 Routine Update – Developing Patch Update Plan."

5.7 Update exception handling

If during software update execution encounters update failures, software startup failures, configuration project launches, business function errors, or communication anomalies with PLC/subcomputers, the update must be terminated immediately, rollback started immediately, and the process should be used in "5. 6.1 Routine Update – Formulate a Patch Update Plan" to cover and restore the full disk backup image as described in the "Routine Update Plan." Record update anomalies, error messages, and log content, and report them back to Delta technical support.

6 Retirement and Data Destruction

6.1 Business migration and offline management

Stop the DIAView X Runtime service and discontinue all Windows services related to DIAView X. Perform data backup, archive and retain DIAView X configuration engineering and historical data, alarm records, and event logs, back up using authorized dedicated media, and properly safeguard backup files.

6.2 Permissions and authorization cleanup

Log out and reclaim DIAView X hardware dongles or WIBU soft licenses. Remove DIAView X-related policies from firewall policies. In "Computer Management," delete dedicated service accounts created for DIAView X and remove all user permission assignments. Update software allowlists and remove all rules created for DIAView X. Unplug physical network cables.

6.3 Data and engineering destruction

Uninstalling DIAView X will only remove the software body and its components; configuration engineering files (including production process recipes, alarms), and historical data will not be deleted, posing risks of recipe leakage and incorrect recipe production.

Security Recommendation: Perform special clearing of data and configuration engineering. Simple deletion or formatting can be restored, but professional data overwriting is required. First uninstall DIAView X, then perform overwriting and deletion on the remaining installation directory. Focus on erasing engineering files (including production process recipes, alarms), logs, caches, uploaded files, database files, etc.

▲ Security recommendation: Clean the registry and event logs related to DIAView X to avoid leaving traces of operations.

6.4 Residual risk management

The wear-balancing mechanism of SSDs can cause incomplete overwrites, and faulty flash cards cannot be fully erased by software.

▲ Security recommendation: Prioritize physical destruction of storage media.

7 Incidents and Vulnerability Reporting

7.1 Emergency response

When security incidents such as unauthorized logins, configuration tampering, script anomalies, or ransomware attacks occur, the following steps are followed for handling and recovery:

1. Event Confirmation: Verify alarm information to confirm the type and scope of the security event.
2. Isolated Stop-Loss: Disconnect affected workstation/server networks, lock abnormal accounts, and block attack links.
3. Forensic Collection: Logs, configuration files, and process snapshots are saved, without modifying original on-site data.
4. Root Cause Investigation: Analyze audit logs to locate intrusion entry points and malicious operation points.
5. System recovery: Restore system and project files using a clean backup configuration/image, cleans up malicious programs and fixes security vulnerabilities before recovery
6. Verification online: After restoration, verify the integrity of engineering data and permission configuration, confirm no abnormalities, and then resume operation.
7. Event review: Records the entire event process and updates protection strategies.

7.2 Vulnerability reporting

Delta vulnerability reporting address: [Product Cybersecurity Reporting - Delta](#)

Delta vulnerability feedback email: Delta.PSIRT@deltaww.com

If you discover potential cybersecurity vulnerabilities in our products, please fill in the vulnerabilities in the reporting address as required, or provide them via email along with supplementary information (such as logs, crash dumps, packet captures, screenshots, etc.). We will verify your report and, if necessary, arrange for personnel to contact you. If you do not provide complete information about the product's cybersecurity vulnerability, we will not be able to process your request.

7.3 Vulnerability disclosure

Follow the Collaborative Vulnerability Disclosure (CVD) mechanism. Users should report vulnerabilities through official channels (website, email). Vendors are responsible for assessing, reconstructing, developing patches, and issuing security notices. It is strictly forbidden to privately disclose details of unresolved vulnerabilities. Relevant countries bear criminal liability for unauthorized disclosure.

Delta vulnerability bulletin address: [Product Cybersecurity Bulletin - Delta](#)

8 Third-Party Component and Product Vulnerability Management

8.1 Third-party component vulnerability management

DIAMView X integrates various third-party components (such as open-source libraries, drivers, etc.), whose security directly affects the overall system robustness.

Asset Inventory: DIAMView X maintains an accurate inventory of third-party components for vulnerability management and risk assessment.

Proactive monitoring: Regularly track publicly available vulnerabilities in third-party components based on SBOM lists.

Risk assessment: Once a relevant vulnerability is discovered, immediately assess the scope and severity of its impact on the system.

Collaborative Action: Pay attention to Delta's official Security Advisory.

8.2 Product vulnerability management

1. External Security Issues (Customers, Research Institutions, Third Parties)

Establish a dedicated channel to receive externally reported security vulnerabilities. Acknowledge receipt promptly upon feedback and register a ticket. Organize security and development teams to conduct risk assessments.

2. Critical Internal Security Issues (SAST, Internal Testing)

For critical security issues discovered internally, if the assessment indicates an exploitable risk on the customer side, issue a security advisory externally in accordance with standard procedures.

This product's SBOM and proprietary vulnerability management only cover the built-in self-developed code and third-party components in the product package. Host operating systems and independent external middleware used by users are not within the scope of vulnerability management for this

product; related vulnerability monitoring and handling are handled by the on-site operations and maintenance team.

▲ **Security recommendation:** For specific vulnerability reporting and disclosure processes, please refer to Sections 7.2 & 7.3.

9 End User Responsibility

The information contained in this safety guide is intended to provide a reference for end users, helping them select technical solutions reasonably based on their own needs to achieve the expected safety level.

The fundamental prerequisite for ensuring the security of the DIAView X system: at least implement and continuously maintain the baseline safety requirements specified in industrial control system security. It is also recommended to implement and continuously meet compliance requirements for industrial control system security

End users also bear the following responsibilities: ensuring that the overall Industrial Automation and Control System (IACS) cybersecurity management system can be implemented and maintained long-term under the ever-evolving threat environment, maintaining network security levels stably at preset target levels. The security capability of any software product depends on deployed, on-site operation and maintenance security policies and management systems. Maintaining a secure network operating environment is the responsibility of the user unit.

10 Document Maintenance

Ensure the timeliness and accuracy of this safety guide, and adapt to system evolution and changes in standards.

Regular Review: Establish a mechanism to review documents for each version

Dynamic revision: The process of document revision, review, and re-release must be initiated immediately in the following situations:

1. DIAView X undergoes major version leaps (such as architecture upgrades)
2. Updates to relevant international or industry safety standards
3. After a major safety incident occurs, lessons learned and protection measures must be summarized and updated

More resources available: [Delta DIAView X SCADA System](#)