



DELTA ELECTRONICS, INC.

DIView X 安全指南

台达官方网站: www.delta-china.com.cn

网络安全公告: [产品网络安全公告](#)

网络安全上报: [产品网络安全上报](#)

网络安全策略: [产品安全漏洞处理策略](#)

漏洞反馈邮箱: Delta.PSIRT@deltaww.com

文档版本控制.....	2
1 概述.....	2
1.1 目的	2
1.2 适用范围	2
1.3 使用情景	2
1.4 使用环境	3
1.5 安全假设	3
1.6 文档关系	3
1.7 术语与定义.....	4
1.8 参考文档	5
2 部署环境安全要求	5
2.1 安全域划分.....	5
2.2 边界防护	8
2.3 物理与终端安全.....	8
2.4 纵深防御	9
3 安全安装	11
3.1 安装包与组件校验	11
3.2 最小化安装与组件收敛	11
3.3 初始加固	11
3.4 安装异常处理	12

4 安全配置基线	12
4.1 安全威胁与缓解措施	12
4.2 DIAView X 原生安全配置	13
4.2.1 工程密码配置	13
4.2.2 账号与用户权限配置	14
4.2.3 HMI Server 安全配置	15
4.2.4 组态脚本安全限制	15
4.2.5 操作审计与日志管理	15
4.2.6 通信与数据安全	16
5 运维安全管理	19
5.1 纵深防御实践	19
5.1.1 网络层防御	19
5.1.2 主机层防御	20
5.1.3 数据层防御	20
5.1.4 物理层防御	21
5.1.5 人员与流程防御	21
5.2 操作系统与网络环境适配加固	22
5.3 运维安全基线	23
5.4 账号与权限管理	23
5.5 运维红线	24

5.6 版本与补丁管理.....	24
5.6.1 常规更新	24
5.6.2 更新异常处置	25
6 退役与数据销毁	25
6.1 业务迁移与下线.....	25
6.2 权限与授权清理.....	25
6.3 数据与工程销毁.....	26
6.4 残余风险处置	26
7 事件与漏洞上报	26
7.1 应急处置	26
7.2 漏洞上报	27
7.3 漏洞披露	27
8 第三方元件及产品漏洞管理.....	27
8.1 第三方元件漏洞管理.....	27
8.2 产品漏洞管理	27
9 最终用户责任	28
10 文档维护	28

文档版本控制

版本号	修订日期	修订说明
1.0	2026-09-30	首次编制

1 概述

1.1 目的

本指南的制定遵循工业控制系统安全开发流程，并参考了网络安全相关法规的要求，界定 DIAView X 的威胁应对范围，指导 DIAView X 的安装、调试、验证及维护工作；同时本文档配合《DIAView X 1.0 用户手册》提供配套指引，供系统集成商及最终用户参考使用。

1.2 适用范围

本文的适用对象包含设备和人员两部分：

适用组件：实时数据库、Runtime、组态开发终端、Web 监控服务端、IO 通信套件

适用人员：系统集成商、资产所有者、运维人员

本文适用于 DIAView X v1.0 及后续兼容版本，PLC/下位机固件自身安全加固不在本指南范围内。

1.3 使用情景

DIAView X 系统用于工业生产现场自动化监控与运维管理，用于设备数据采集、工艺画面监控、生产状态展示、报警提示、参数查看与工程组态维护。典型使用情景：

1. 组态工程师在内网工作站编辑、上传、更新工程组态文件
2. 现场操作员实时监控生产画面、查看报警、查询历史数据
3. 系统管理员进行账号权限配置、系统安全参数维护、日志审计
4. 服务端持续和现场控制器通信，完成实时数据采集与状态同步

1.4 使用环境

1. 网络环境

产品可部署于工业控制局域网；经用户配置边界安全设备后，支持外网 Web 访问。

内网场景：服务端与 Web 客户端在工控内网交互，内网和办公网络之间建议逻辑隔离。

外网访问场景：服务端不直接暴露于公网，外网接入需要由用户前置部署安全网关（VPN、反向代理等）。

2. 硬件环境

服务端部署于机房工控机 / 工业服务器；Web 客户端可在操作站、办公 PC、远程终端浏览器运行。

3. 软件环境

服务端宿主操作系统为 Windows/Linux，对外提供 HTTPS、WebSocket 服务，用于 Web 画面交互、工程文件管理；客户端使用主流浏览器访问 Web 页面。

1.5 安全假设

本产品安全能力生效基于以下安全假设：

1. 系统按指南完成安全域划分与网络边界防护，落实物理与终端安全，采用纵深防御架构
2. 安装前校验安装包完整性，执行最小化安装与初始系统加固
3. 遵循 DIAView X 原生安全基线配置账号、权限、日志、通信等安全参数
4. 运维阶段持续落地网络、主机、数据、物理、人员流程多层纵深防御措施
5. 建立版本与补丁管理机制，开展常规更新并处置更新异常

1.6 文档关系

本文依据工业控制系统安全标准，旨在帮助使用者了解 DIAView X 的威胁防护能力，并指导软件的安全部署、配置与运维操作。

《DIAView X 1.0 用户手册》为软件基础参考文档，用于功能学习与工程组态开发指导，该手册对软件界面布局、通信配置、画面组态、变量词典、报警系统、历史数据、配方管理、用户权限等核心功能的配置方法进行详尽说明，提供完整的软件操作指引。

1.7 术语与定义

术语	定义
Admin	拥有管理员权限的内置用户。
Administrator	拥有管理员权限的角色。
RBAC	基于角色的访问控制，核心思想：权限分配给角色，角色分配给用户，用户通过角色获得权限，而不是直接给用户授权。
DIASudio	为设备和系统整合常用的可编程器 (PLC)、人机界面 (HMI)、伺服驱动系统、变频器等，提供一体化选型设定软件工具。在单一平台上为客户完成产品选型、PLC 程序编程、产品参数设定、设备调机与 HMI 规划，简化并加速系统开发流程。
身份鉴权(Authentication)	对实体所声明身份进行核验。
网络安全(Cybersecurity)	保障网络空间中信息的保密性、完整性和可用性。
纵深防御(Defense in Depth)	采用多种相互独立的防护手段抵御系统各类攻击的防护思路。
最小权限(Least Privilege)	基础安全原则：应当为用户（人员、软件进程、设备）分配与其承担任务和功能相匹配的最少权限。
威胁(Threat)	可能通过未授权访问、破坏、信息泄露、数据篡改和 / 或拒绝服务，对业务运行（包括任务、功能、形象或声誉）、资产、控制系统或人员造成不利影响。
漏洞(Vulnerability)	1. 系统在设计、实现、运行与管理中存在的缺陷或弱点，可被利用来破坏系统完整性或违反安全策略。 2. 工业自动化控制系统（IACS）功能、流程、内部控制或实现中存在的弱点；该弱点可被威胁源利用或触发。弱点既可以是计算机组件有意植入的（例如远程端口访问），也可以是产品生命周期任意阶段意外引入。
DMZ	位于内部可信网络与外部不可信网络之间的一个隔离区域，用于放置需对外提供服务的服务器，既允许外部访问，又避免其直接接触内部网络。
Zone	普渡模型安全分区

Conduits	分区之间的通信通路，含防火墙、网关等边界设备
Jump Server	运维跳转服务器
Data Diode	单向数据传输硬件设备
HMI	人机界面
IPC	工业计算机

1.8 参考文档

术语	定义
IEC 62443-2-1	建立工业自动化和控制系统安全程序
IEC 62443-3-2	系统设计的安全风险评估
IEC 62443-3-3	系统安全要求和安全等级
IEC 62443-4-1	系统安全开发流程

2 部署环境安全要求

本文遵循区域与管道安全模型相关标准，并结合 ISA-95 企业系统与控制系统集成标准模型，基于资产重要等级、业务核心功能及风险影响范围，对 DIAView X 工控监控系统整体开展安全区域划分、安全边界隔离、网络端口收敛等网络安全防护配置，同时配套落实设备物理防撬、防拔等物理安全防护措施。

2.1 安全域划分

图 1 展示了将控制系统划分为若干区域（Zones）、通过通道（Conduits）实现互联的工程实践。以该视角审视你的控制系统，有助于重点关注各通道的安全防护，防范非授权入侵，同时便于将各类设备划分至合适的区域。区域与通道的相关概念，以及在系统设计中二者开展评估的流程，在区域与管

道安全模型标准中有详细说明。如需对在建系统开展合规安全评估，请参阅该标准。本节仅对部分基础概念做简要概述，帮助理解本文档后续内容。在同一个区域内，设备具备统一的安全要求，设备之间存在一定程度的互信，但不信任其他区域内的设备。区域之间的通道通过隔离机制、管控跨区域网络流量、提供网络流量监测点，在互联区域之间建立信任关系。各区域具体部署内容如下：

1. 工厂现场区域

工厂各网络区域借助防火墙、路由器完成互联，一方面实现对工厂 I/O 设备的访问能力，另一方面将从某一区域 I/O 点采集得到的数据分发至其余业务区域。

本示意图中的工厂区域包含 I/O 设备以及对应的控制单元。在工程实际场景下，RTU 与 PLC 通常并不部署在 SCADA 设备所在区域，而是安装在远端现场。该场景下，应当将 RTU/PLC 划分为独立安全域，配置专用受控通信通道完成与 SCADA 域的数据交互，保障通信过程安全。

即便 RTU、PLC 部署于 SCADA 本地区域，通向工厂现场区域的通信通道仍需要实施防护与持续监测，及时识别具备入侵特征的异常网络流量。访问工厂区域的通信链路执行严格访问管控，仅放行业务必需的网络报文。除网络防护之外，还需要落实工厂区域对应的物理安全防护手段，例如门禁刷卡、密码键盘等方式对人员出入权限进行管控

2. SCADA 监控区域

部署 DIAView X 核心服务器及实时数据库，实现生产线实时监控、过程报警管理以及现场过程数据存储。本层仅负责设备级监控与监督控制。

3. 控制区域

控制区域部署用于控制系统维护、部分场景下也用于系统操作的设备。出入口由防火墙防护，按需允许访问 SCADA 区域及其他区域。

注意：该区域与更高区域之间，仅能经由防火墙和工厂隔离区（Plant DMZ）建立连接，不存在直连通道。

4. 工厂隔离区域

工厂隔离区内的服务器，用于实现高区域与低区域之间的隔离。工厂隔离区可部署监控服务器、网络流量服务器、外部设备网关。跳板机 (Jump Server) 一般用作身份认证与权限授权节点，供企业区域、DMZ 隔离区访问低区域。可部署 Data Diode，实现数据从 SCADA 区域单向流向 DMZ 中面向互联网的服务器。结合防火墙一同使用，能够实现网络监测，抵御 DMZ 服务器或企业区域设备被攻陷带来的风险。

5. 企业区域

企业区域由非控制系统类设备组成，例如办公台式机、笔记本电脑。从 SCADA 区域或控制区域导出到企业服务器的控制系统数据与报表，可在此区域查看、分析。

请注意：该图并非供你系统直接使用的设计方案。

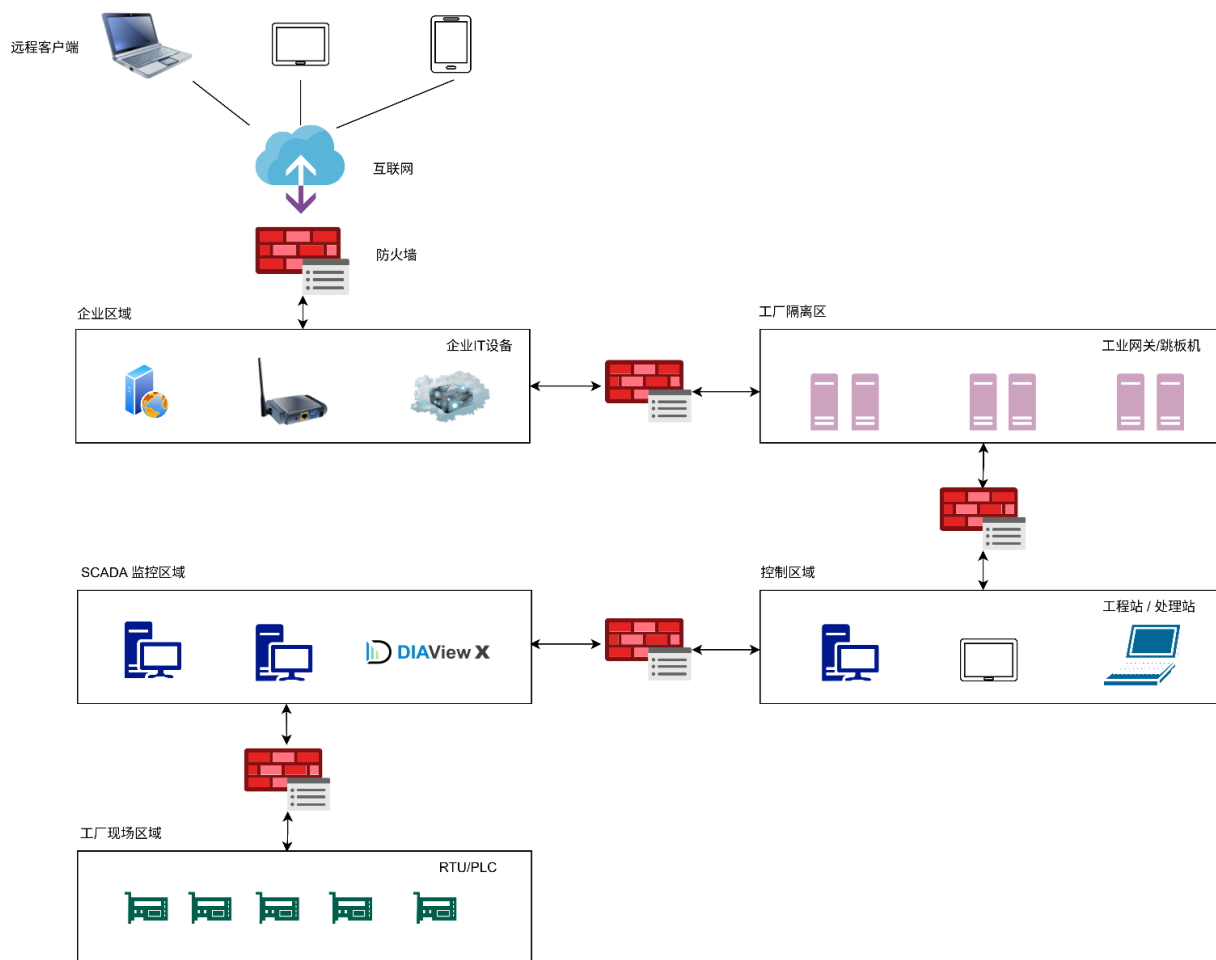


图 1

2.2 边界防护

本系统遵循最小权限原则规划跨区域通信通道，在区域边界防护设备上执行端口收敛策略，仅开放 DIAView X 系统及 PLC 通信所需的必要协议与端口。DIAView X 常用通信协议、服务、默认端口及对应功能说明如下所示。

协议/服务	默认端口	说明
Server Manager / HMI Server	10090 / 8090	客户端与 DIAView X Server 组态/运行通信端口
DIAView X Config Web Server	6070	DIAView X Web Config Server，用于开发时配置用户、角色、权限，强制使用 HTTPS (TCP / 6070)
Modbus TCP	502	Modbus Service 为 DIAView X 内置的 Modbus Slave 服务模块，对外提供 Modbus TCP 服务，接收外部 Modbus 主站的读写请求，实现数据交互。

▲ 安全建议：关闭所有未使用 TCP/UDP 端口，禁用 Telnet、FTP、HTTP 等高风险通用协议。

2.3 物理与终端安全

在落实网络逻辑隔离的基础上，还需开展物理层安全加固，作为纵深防御体系的底层防护措施，具体要求如下：

1. 机房环境防护

DIAView X 运行宿主机与 PLC 控制柜应放置于独立专用机房，机房配置出入门禁及视频监控，实现访问可控、行为可追溯。

2. 外设接口管控

对工控机闲置 USB、串口接口进行物理封堵，不允许随意接入 U 盘等移动存储介质，如需使用请确认扫描无病毒后启用。使用防拆标签记录设备开启状态，防止非法接入。

3. 网络端口物理防护

DIView X 运行宿主机、核心交换机的业务网口应配置网线锁、端口防盗防尘锁扣，防止网线被非法拔除、端口被违规占用。

4. 端口准入控制

交换机端口必须同时启用 IEEE 802.1X 认证与 Port Security 端口安全功能，防止未授权设备接入网络。

5. 资产台账管理

建立并维护针对现场的可连接设备清单，包括但不限于：工程师站、HMI、IPC、PLC 等，定期盘点与审计。

6. 人员接触管理

核心控制硬件仅限授权运维人员接触。外部厂商人员开展现场调试工作时，应执行专人全程陪同制度。

2.4 纵深防御

虽然 DIView X 在开发时遵循了多层安全设计原则，但真正的安全性更体现在产品的实际部署中。部署后的系统必须提供多重防御层，以确保即使某一层被攻破，其余的防御层仍能继续保护系统，抵御试图进一步渗透系统的攻击者。这些防御层可以采取多种形式，包括物理控制（例如控制对设备的访问权限）、技术控制（例如加密和身份验证）或管理控制（例如审计日志和监控）。每一层都在系统的整体安全中发挥着作用，以抵御各类威胁。

最终用户有责任对部署系统中存在的威胁进行妥善评估，确定所需的安全控制措施，并对这些威胁进行缓解。由于威胁环境并非一成不变，这一过程需要持续不断地进行。

本文档旨在明确 DIAView X 的安全能力，以协助用户评估系统的安全能力、威胁及缓解措施，从而帮助实现安全的系统设计。

纵深防御层级包括但不限于：

1. **网络层防御**：本层实施安全区域划分，构建网络隔离防线。依托防火墙、VLAN、VPN、IDS/IPS 等设备实现网络边界防护。通过网络分段、访问控制、异常流量监测，降低非授权访问、端口探测扫描、网络层面恶意攻击、横向渗透等风险。
2. **主机层防御**：本层重点保障运行 DIAView X 组件的服务器、工程师站、HMI 工控主机安全。关键措施包含最小化安装、关闭闲置服务与端口、文件目录权限管控、禁用不安全加密套件、终端防护等。通过操作系统层面加固，防范未授权本地访问、拒绝服务、数据篡改破坏、会话劫持、恶意代码执行等威胁。
3. **数据层防御**：本层保障工程文件、配置参数、历史工艺数据等静态数据的保密性与完整性。主要手段包含加密存储、完整性校验、关键目录权限限制、定期备份与版本管控。通过对敏感数据保护，抵御数据窃取、非授权篡改、数据损坏丢失、勒索加密等威胁。
4. **物理层防御**：本层通过管控物理访问权限，保护工作站、控制室、PLC、网络交换机等硬件基础设施。防护措施包含物理访问控制、门禁及视频监控系统。对关键资产实施严格物理访问管控，可应对设备失窃、硬件接线恶意篡改、未经授权外接设备等安全威胁。
5. **DIAView X 应用加固**：本层充分启用软件自身内置安全能力，例如强制 HTTPS 发布、安全访问策略、强身份认证、RBAC 权限控制、访问流量控制、组态脚本安全限制等。依托应用层安全能力，抵御中间人攻击、XSS 攻击、资源耗尽、路径遍历、越权操作等面向业务应用的恶意攻击。
6. **人员与流程防御**：技术防护无法完全抵消人为风险，配套管理制度、人员培训、职责分离、审计与供应商管理，作为技术防护的重要补充，降低误操作、内部恶意操作、流程管控缺失带来的安全风险。

3 安全安装

3.1 安装包与组件校验

DIAMView X 软件下载、安装及升级操作由官方工具 DIAMInstaller 统一管理，全程规范化、标准化执行。

DIAMInstaller 操作流程：

1. 预先完成 DIAMInstaller 工具的安装部署
2. 启动 DIAMInstaller，登录台达 DIAMStudio 官方账号
3. 在【所有应用程序】列表中勾选 DIAMView X 产品
4. 点击下载并安装，完成软件部署

3.2 最小化安装与组件收敛

为降低系统受攻击风险，在安装过程中遵循以下原则：

1. 按需安装

仅安装业务运行所必须的功能组件、数据库服务和系统依赖。严禁将 DIAMView X Builder、Demo 工程和相关数据库部署在生产环境。

2. 收敛攻击面

每增加一个组件都意味着引入潜在漏洞和维护成本。安装完成后，识别系统内未使用的组件、插件、服务，对闲置组件执行卸载，暂时不用的服务予以禁用。

3.3 初始加固

软件安装完成后，需严格执行以下安全配置操作，夯实系统运行安全基线：

1. 确认软件为最新版本

安装完成后，应校验软件版本，确认当前安装的为官方发布的最新正式版本：

- 1) 访问软件官方网站，查询当前最新版本号

- 2) 打开已安装的 DIAView X Builder，进入【帮助-关于】页面，查看当前软件版本号，并与最新版本号比对
- 3) 如检测到当前已安装版本非最新，必须通过官方正规渠道升级至最新版本
- 4) 升级完成后，再次确认版本号为最新版本并检查安装包文件是否有 DELTA ELECTRONICS, INC. 数字签名

2. 修改管理员账户密码并启用密码安全策略

安装完成后，须立即修改 DIAView X 内置管理员密码，并统一配置密码安全管控策略：

- 5) 启用密码强度
- 6) 设置密码最大生命周期
- 7) 强制开启密码历史记录
- 8) 设置密码错误次数阈值。

修改账户密码请参阅《DIAView X 1.0 用户手册》第 14 章—用户。

3.4 安装异常处理

安装过程中若出现报错、安装中断或提示缺失依赖组件（包括 .NET Framework、Visual C++ Runtime 等），严禁忽略异常继续安装。需立即终止当前安装流程，逐项排查安装权限、依赖库完整性、依赖库版本匹配度等问题，待故障完全修复后重新执行安装。若问题排查完毕仍无法正常安装，请联系官方技术支持团队协助处理。

4 安全配置基线

4.1 安全威胁与缓解措施

DIAView X 提供了丰富的安全机制，但工业控制系统的安全性取决于“产品能力”与“部署环境”的结合。下表梳理了 DIAView X 运行环境中可能面临的安全威胁，并指引您通过配置后续章节的安全功能来构建纵深防御体系。

威胁类别	潜在风险描述	缓解措施
身份与权限滥用	使用默认密码或弱口令、越权操作、内部人员误操作导致系统被接管。	见 4.2.1
通信窃听与篡改	中间人攻击 (MITM)、网络嗅探导致敏感数据泄露或被篡改。	见 4.2.4
主机层恶意攻击	勒索病毒、恶意软件感染、操作系统漏洞被利用，导致系统瘫痪或数据丢失。	见 5.2
审计与追溯失效	发生安全事件后无法溯源、日志被攻击者篡改或删除，导致责任无法界定。	见 4.2.5
网络层拒绝服务	网络泛洪攻击、端口扫描、非授权设备接入，导致合法用户无法访问服务。	见 2.2
特权功能滥用	生产环境中非法修改工程逻辑、调试工具未受控使用，导致生产中断。	见 4.2.2
物理访问威胁	违规外接设备、硬件破坏、未经授权的物理接触，绕过软件层面的防御。	见 2.3
工控协议层攻击	攻击者利用工控协议的漏洞，绕过应用层直接向 PLC 下发恶意指令。	见 4.2.4
供应链与第三方风险	第三方开源组件或底层库存在已知漏洞，被利用进行供应链攻击。	见 第 8 章
系统退役数据泄露	系统下线或硬盘报废时，工程数据未被彻底销毁，导致商业机密泄露。	见 第 6 章

4.2 DIAView X 原生安全配置

4.2.1 工程密码配置

1. 工程密码

为了防止工程被未经授权修改，DIAView X 提供工程密码功能。用户对当前工程设置密码，设置密码后，再次打开该工程时需要输入正确的密码。

2. 下载/上载密码配置

工程下载是 DIAView X 组态软件中完成工程本地设计与配置后，将编辑好的工程文件及相关配置数据，从设计端传输至目标运行设备或控制器的操作过程；工程上载是将目标运行设备或控制器中已生效的工程文件、配置参数及相关运行数据，传输至本地设计端的操作过程。DIAView X 支持设置工程上载/下载密码，防止未经授权的上载和下载操作。

工程密码和下载/上载密码的默认配置存在安全隐患，安全建议如下：

功能模块	安全风险	安全建议
启用密码强度	默认启用密码强度，且启用全部密码复杂度规则。用户可手动取消部分密码复杂度规则或不启用密码强度。	禁止取消密码强度，且必须启用全部密码复杂度规则。
工程密码	默认未启用	启用工程密码，且配置高复杂度的密码。
下载/上载密码	默认未启用	启用下载/上载密码，且配置高复杂度的密码。

4.2.2 账号与用户权限配置

DIAMView X 支持精细化权限配置，可针对用户账号定制分配操作权限，严格管控用户可执行的系统操作。系统采用 RBAC 的权限管理机制：将多项单一权限整合为专属角色，用于匹配岗位所需的权限集合，通过为用户分配对应角色，快速赋予其匹配业务场景的操作权限。

系统账号与用户权限的默认配置存在一定安全隐患，为规避权限滥用、越权操作等安全风险，本指南给出以下安全配置建议：

功能模块	安全风险	安全建议
权限配置	内置 Administrator 角色拥有所有权限	禁止直接使用 Administrator 角色, 依据最小权限原则新增定义角色。
账号配置	内置账号 Admin 使用默认随机密码，在开发时对用户可见	在组态工程时，必须修改内置 Admin 账号的默认密码。
	新增账号使用默认随机密码，在开发时对用户可见	新增用户后必须修改用户的初始随机密码。
	账号默认永不自动注销	设置自动注销时长
	默认未启用密码安全策略	开启全套密码安全策略

账号与权限配置方法，请参阅《DIAMView X 1.0 用户手册》第 14 章—用户。

4.2.3 HMI Server 安全配置

DIView X Manager Server 的安全配置包括 HTTP 最大并发连接数、单个 IP 最大并发请求数、请求内容大小。下述并发、请求大小参数配置对象为 HMI Server，并非 Manager Server。

功能模块	安全风险	安全建议
HTTP 最大并发连接数	默认 256，用户可自定义修改，存在资源总量耗尽的风险	根据服务器性能和实际使用场景设置合理的值。
单个 IP 最大并发请求数	默认 240 请求数/5 秒，用户可自定义修改，存在高频请求风险。	根据实际使用场景设置合理的值。
请求内容大小	默认 30Mb，用户可自定义修改，存在大包攻击、缓冲区溢出的风险。	根据实际使用场景设置合理的值。

4.2.4 组态脚本安全限制

DIView X 内置可编程扩展模块，依托 JavaScript 语言，作为基础可视化组态的补充，支持配置控件事件脚本和排程后台脚本。

在 DIView X 中执行的脚本严禁通过以下方式与操作系统交互：

1. 调用操作系统命令行解释器（如 cmd.exe、powershell.exe、wscript.exe、cscript.exe）
2. 启动或调用任何外部第三方可执行程序（.exe .bat .cmd .msi 等）
3. 读写操作系统关键路径下的文件（如 C:\Windows\System32、C:\Windows\SysWOW64、C:\Windows\System32\drivers、注册表关键键值等）

4.2.5 操作审计与日志管理

DIView X 提供操作日志与报警日志功能。操作日志与报警日志数据存储于外部第三方数据库。

针对操作日志及报警日志功能，给出如下安全配置建议：

功能模块	安全风险	安全建议
------	------	------

操作日志	默认未开启	强制手动开启。操作日志开启方法请参阅《DIAView X 1.0 用户手册》第 8 章 Action
	存放于数据库中，存在被删除、篡改的风险	预设日志保存期限、磁盘容量阈值、磁盘空间不足策略,设置方法参阅《DIAView X 1.0 用户手册》第 11 章 11.4 数据库
报警日志	存放于数据库中，存在被删除、篡改的风险	同上

▲ 安全建议：日志存储与实体数据库文件，运维人员应根据实际情况从操作系统层面设定访问权限，避免数据库被删除/修改破坏。

4.2.6 通信与数据安全

OPC UA Client 通信

为保障 OPC UA Client 数据传输的机密性与完整性，DIAView X 内置多项强制安全配置，如下：

1. 强制开启 OPC UA Client 安全访问策略，禁止无安全策略通信；
2. 默认采用 Basic256Sha256 加密算法及 SignAndEncrypt（签名并加密）安全模式；
3. 启用账号身份核验机制，严格禁止匿名接入；
4. 强制启用 OPC UA Client 证书校验，与 OPC UA Server 实现双向身份认证，拦截并拒绝不受信、已过期的非法证书。

▲ 安全建议：系统支持手动切换为无安全（None）通信模式，该模式下数据无加密、报文明文传输，存在极大数据泄露与篡改风险，严禁在正式生产环境使用。

Web/App 远程发布

HTTP 明文传输存在请求参数被窃取、数据被篡改的安全风险。DIAView X 默认强制开启 HTTPS 发布，采用 TLS 1.2 及以上加密协议，该安全策略对全部 Web 界面与 API 接口统一生效。

▲ 安全建议：用户可手动关闭 HTTPS 发布功能，关闭后通信将采用 HTTP 明文传输，会引入严重安全风险，生产环境不建议关闭。

RabbitMQ Client

RabbitMQ Client 支持匿名认证、用户名密码认证、证书认证三种身份认证模式，用于和 RabbitMQ 服务端完成身份鉴权。默认启用 SSL/TLS，使用证书认证模式，数据加密传输。

▲ 安全建议：用户可手动关闭 SSL/TLS，关闭后数据采用明文传输，存在被恶意截获的风险，生产环境必须搭配 SSL/TLS 使用。

Modbus Service

Modbus 协议本身规范不内置身份认证、报文鉴权与加密机制，无法在协议 PDU 内携带身份凭证，本系统未内置 IP 过滤、Modbus 报文 DPI 校验等安全控制逻辑，存在未授权访问、非法写入风险。

▲ 安全建议：工业防火墙 / 网关配置可信 IP 白名单，非授权 IP 在 TCP 握手阶段直接阻断，配套防 ARP 欺骗与设备生命周期管理；生产环境 502 端口严禁直接暴露至非可信网络；定期维护网关策略与白名单、核验网关运行状态。

报警邮件通知

SMTP 明文发送邮件时，报警信息存在被第三方截获的风险。DIAView X 报警通知的电子邮件服务器配置默认强制启用 SSL/TLS 加密传输，报警通知邮件将以加密方式发送，避免报警信息遭到恶意窃取。

▲ 安全建议：用户可手动关闭 SSL/TLS 加密传输，关闭后邮件将以明文方式传输，会带来相应安全风险，生产环境请勿关闭该配置。

系统加固

1. Windows 操作系统

为落实密码安全合规要求，规避弱加密算法、老旧 TLS 密码套件带来的中间人攻击、数据篡改、加密降级等安全风险，依据欧盟网络安全局（ENISA）发布的《ECCG Agreed Cryptographic Mechanisms Version 3 (Draft)》基线要求，针对 Windows、Linux 服务器操作系统开展 TLS 密码套件专项加固工作，按照基线要求建议禁用以下密码套件：

名称
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

运行 DIAView X 服务的主机，需要通过 Windows 组策略、注册表或 Powershell，禁用 TLS 相关密码套件。

方法一：组策略

1. 按下 Win+R，运行 gpedit.msc 打开本地组策略编辑器；
2. 依次导航至路径：计算机配置 → 管理模板 → 网络 → SSL 配置设置
3. 双击打开 SSL 密码套件顺序，选择 已启用
4. 在 SSL 密码套件配置框中，清理移除所有不安全得密码套件
5. 点击【确定】保存配置，重启服务器使策略永久生效。

方法二：Powershell

验证：列出当前启用的套件中是否包含 建议移除的密码套件

```
Get-TlsCipherSuite | Where-Object { $_.Name -match "密码套件名称" }
```

禁用密码套件（如包含情形下再执行禁用操作）

Disable-TlsCipherSuite -Name "密码套件名称"

▲ 安全建议：在禁用相关密码套件之前，请充分评估并检查该操作是否会对系统其他业务功能产生兼容性影响，确认无业务异常后再执行禁用操作；相关配置细则请查阅微软官方操作系统文档。

2. Linux 操作系统

Linux 环境下已通过程序代码层面禁用不安全加密套件；其中 Ubuntu 20.04 及以上操作系统版本，已默认关闭不安全的密码套件。

OPC UA Client · RabbitMQ 证书管理说明

产品仅提供证书加载、证书校验的应用层能力。证书签发、管理、吊销列表维护、定期巡检、到期通知属于现场管理员运维责任。

5 运维安全管理

5.1 纵深防御实践

为在产品全生命周期内有效落地并持续执行纵深防御策略，企业应当落实下述部署运维安全控制措施。本节覆盖物理层、网络层、主机操作系统层、数据层、人员与流程管理域五大域；DIAView X 应用层为产品原生安全能力，配置要求参见第 4 章节安全配置基线。本节聚焦五大域的部署与运维实践。

5.1.1 网络层防御

1. 网络分段：借助防火墙、VLAN 或专用物理基础设施对 IT 网络与 OT 网络实施物理或逻辑隔离，仅放行业务必需流量。
2. 防火墙规则：在 OT 网络边界部署防火墙，配置严格的入站、出站访问规则，仅开放 DIAView X 工程师站、SCADA 服务、HMI 客户端与现场 PLC/RTU 设备之间必要的通信端口与 IP 地址。

3. 入侵检测 / 防御系统 (IDS/IPS)：在关键网络节点部署 IDS/IPS，监测异常流量模式与已知攻击特征；检测到异常时触发告警或自动阻断。
4. 虚拟专用网络 VPN：若需要对 DIAView X 工程师站或 SCADA 系统进行远程维护，必须使用高强度加密 VPN 并启用多因子认证 MFA。
5. MAC 地址过滤：在交换机层面配置访问限制，仅允许预先登记 MAC 地址的设备接入 OT 控制网络。

5.1.2 主机层防御

1. 操作系统加固：对运行 DIAView X 组件 (SCADA 服务器、工程师站、HMI 客户端) 的工作站与服务器执行最小化安装，移除无用服务，关闭闲置端口，安装最新安全补丁。
2. 杀毒软件 / 终端检测响应 EDR：部署正规杀毒软件或高级 EDR 终端防护方案，定期更新病毒特征库，持续监测主机异常行为。
3. 应用白名单：仅允许预先审批通过的程序运行，例如 DIAView X 运行组件、工程工具以及经过授权的辅助软件，拦截其余未授权程序。
4. USB 端口管控：禁用闲置 USB 接口，执行严格 USB 使用策略；仅允许 IT/OT 安全团队审批的加密 U 盘用于 SCADA 工程文件传输。
5. 主机防火墙：配置 DIAView X 所在主机的系统内置防火墙，限制应用层面的网络连接。
6. 定期漏洞扫描：使用自动化工具定期扫描 DIAView X 服务器、工程师站、HMI 工作站，识别并修复操作系统及应用程序漏洞。

5.1.3 数据层防御

1. 加密存储：DIAView X 工程文件、配置数据库、历史数据本地存储时，采用操作系统级加密 (BitLocker) 或第三方加密软件对关键文件实施保护。
2. 数据备份与恢复：将 DIAView X 工程、配置库、历史归档定期异地备份；建立严格备份管理制度，定期开展恢复测试，应对数据损坏以及勒索病毒事件。

3. 版本控制系统：使用 Git 或者工控专用版本控制系统管理 DIAView X 工程文件，完整记录每一次工程修改，实现操作可追溯、版本比对以及故障回滚。

5.1.4 物理层防御

1. 限制物理访问：DIAView X SCADA 服务器、工程师工作站、HMI 人机面板、现场 PLC/RTU 及配套网络设备需要放置在受管控的安全区域，例如带锁机柜、监控机房。
2. 访问控制系统：使用刷卡读卡器、生物识别等手段管理并记录关键区域人员出入。
3. 视频监控 CCTV：关键机房部署监控摄像头，录像留存并定期复核。
4. 物理锁机制：机柜、设备机箱、服务器机架加装物理锁，防范非授权接入硬件、篡改接线。

5.1.5 人员与流程防御

1. 安全意识培训：对所有接触 DIAView X 的人员（工艺工程师、操作员、运维人员、IT 人员）开展常态化安全培训，覆盖 OT 威胁、安全制度、运维最佳实践。
2. 安全策略与操作规程：制定可落地的安全策略与操作流程，覆盖 SCADA 软件部署、工程组态变更、口令管理、事件响应、备份恢复等内容。
3. 职责分离：对 SCADA 高危任务做权限拆分，例如工程修改与工程下装上线、现场硬件维护分配不同人员执行，消除单人高危操作带来的单点风险，抑制恶意操作。
4. 安全审计与合规：定期开展内部或外部安全审计，核查制度执行情况，满足 IEC 62443 等行业标准以及监管要求。
5. 供应商安全管理：评估 SCADA 与现场设备供应商安全能力，要求产品遵循安全设计理念，保障 DIAView X 及配套硬件能够及时获取安全更新与漏洞补丁。

5.2 操作系统与网络环境适配加固

DIAMView X 自身安全能力存在边界，部分威胁需要依托操作系统、边界网络设备做补偿防护。本节是对 5.1 纵深防御的场景化补充，聚焦 DIAMView X 所在工控环境的特殊落地注意事项，包含杀毒软件性能适配、白名单落地配置、以及面向下位机 PLC 的业务流量深度监测。

工控机防病毒软件部署

1. 安装适配工控机操作系统的防病毒软件，实时更新病毒特征库；
 2. 合理配置扫描策略，避免全盘实时扫描对业务性能造成影响；
 3. 针对 DIAMView X 的程序目录、数据存储目录，按需配置合理排除项，防止病毒软件误拦截；
- 定期执行病毒查杀，及时处置病毒、恶意程序告警。

工控机软件白名单

采用可信应用白名单，仅放行授权程序，拦截未授权程序。

示例：使用系统内置的 AppLocker 配置软件白名单

无需额外安装，规则灵活，支持针对发布者、路径、哈希值设置规则。适用于 Windows 10/11 企业版/教育版、LTSC 版、Windows Server。

网络侧异常写指令监听

在网络边界/工控网络侧，应部署流量审计、入侵监测类设备，对流向本工控机的网络报文进行监测。

1. 非授权时段对 PLC/下位机的写操作指令；
2. 异常写指令、异常文件写入请求、异常配置修改指令；
3. 异常频率写入、异常批量写、未授权的写操作；
4. 非白名单 IP/设备的写入请求；

运维人员定期查看网络监测告警，发现可疑写指令行为及时排查来源，开展阻断与溯源处置。

5.3 运维安全基线

DIAMView X 正式投入生产运行后，需执行常态化安全巡检，及时发现生产中断、访问异常、证书失效、漏洞风险、日志异常等安全隐患，保障生产环境业务连续性与数据安全。

巡检工作由运维人员负责执行，不建议普通用户执行安全巡检。

巡检应分为日常巡检、周度巡检、月度巡检及专项巡检：

日常巡检（每日）：DIAMView X 服务进程运行状态、CPU/内存/磁盘使用率、登录失败、权限变更、日志异常

周度巡检：账户与权限复核、工程备份有效性、日志抽查

月度巡检：证书有效性、工程备份恢复演练、漏洞扫描、安全策略有效性验证

专项巡检：版本升级、配置变更、安全事件发生后，立即开展专项安全复核巡检

巡检需形成巡检记录，由负责人定期审阅巡检报告，监督问题闭环，为安全整改提供资源保障

5.4 账号与权限管理

1. 分级用户权限管理

DIAMView X 通过“用户-角色-权限”的关联模式，实现权限的批量分配与灵活调整。用户与权限必须基于最小权限原则，仅为用户分配完成其工作所必须的资源，防止单人权限过大。

建议运维人员通过灵活分配权限实现分级用户权限管理：

管理员：拥有最高权限；

工程师：拥有配置权限，但不能管理账户；

操作员：运行时面向固定流程操作，严禁修改组态工程逻辑；

2. 账号定期清理

应建立账号定期清理机制，降低因闲置、过期、离职人员账号未及时处置而带来的安全风险：

- 1) 定期开展账号巡检，及时禁用、回收或删除闲置、过期、离职人员账号

- 2) 核对账号的权限，及时收回不再需要的权限
- 3) 做好账号处置记录，留存账号禁用、删除、变更的操作日志，便于审计和追溯

5.5 运维红线

1. 严禁在未经授权的情况下进行远程连接
2. 严禁私自将 U 盘等移动存储介质插入工控机（确需使用时必须经过病毒扫描）
3. 严禁在生产环境中使用默认密码或弱口令

5.6 版本与补丁管理

5.6.1 常规更新

DIView X 软件已在正式生产环境中使用，安装软件补丁是封堵软件漏洞的核心手段，保障生产系统稳定运行；但补丁部署属于高风险操作，补丁更新失败极易引发非计划停机，必须建立一套严格、受控、可回退的流程：

DIView X 团队内部验证

补丁生成后，DIView X 团队需对补丁做功能性、兼容性测试验证。

提交与审批

补丁文件必须有公司认可的数字签名，明确修复的漏洞、新增功能。由负责人审批同意软件更新。

生产环境验证

禁止在生产系统上直接测试。需要准备一台与生产环境软硬件配置完全一致的验证机。校验补丁文件的完整性，使用系统管理员账号在验证机上执行安装。安装完成后，重启系统，测试完整的核心业务流程，确认无报错，无性能下降。

制定补丁更新计划

明确软件更新的时间，预计影响时长，停机范围和责任。更新前必须将生产系统全盘备份，校验哈希值，暂时关闭白名单和防火墙，以便安装程序能顺利执行。

补丁更新

正常停止 DIAView X 服务及后台相关进程，以系统管理员账号运行补丁文件或安装包。安装完成后立即恢复白名单和防火墙，运行 DIAView X 并测试核心功能。

观察与回退预案

软件更新后，运维人员必须第一时间到现场保障生产系统正常运行，加强巡查，持续监控安全事件日志。如发现生产异常中止、异常停机，立即启动回退方案，用“5.6.1 常规更新 –制定补丁更新计划”中做的全盘备份镜像覆盖恢复。

5.6.2 更新异常处置

当执行软件更新过程中，出现更新失败、软件启动失败、组态工程打不开、业务功能报错、与 PLC/下位机通信异常等现象，需立即终止更新，立刻启动回退，用“5.6.1 常规更新 –制定补丁更新计划”中做的全盘备份镜像覆盖恢复。记录更新异常现象、报错信息、日志内容，反馈给台达技术支持。

6 退役与数据销毁

6.1 业务迁移与下线

停止 DIAView X Runtime 服务，停止与 DIAView X 相关的所有 Windows 服务。执行数据备份，将 DIAView X 组态工程及历史数据、报警记录与事件日志归档留存，用授权的专用介质进行备份，并将备份文件妥善保管。

6.2 权限与授权清理

注销并回收 DIAView X 硬件加密狗或 WIBU 软授权。在防火墙策略中移除 DIAView X 相关的策略。在“计算机管理”中，删除为 DIAView X 创建的专用服务账号，并移除其所有用户权限分配。更新软件白名单，移除为 DIAView X 创建的所有规则。拔除物理网线。

6.3 数据与工程销毁

卸载 DIAView X 只会移除软件本体及其组件，组态工程文件(包含生产工艺配方、报警)、历史数据不会被删除，存在配方泄露和错误配方投产的风险。

安全建议：对数据与组态工程执行专项清除。简单删除或格式化是可以被恢复的，必须执行专业数据覆写。先卸载 DIAView X，再对残留的安装目录执行覆写删除。重点擦除工程文件(包含生产工艺配方、报警)、日志、缓存、上传文件、数据库文件等。

▲ 安全建议：清理与 DIAView X 相关的注册表和事件日志，避免留下操作痕迹。

6.4 残余风险处置

固态硬盘的磨损均衡机制使得覆写可能不完全，故障闪存卡无法通过软件彻底擦除。

▲ 安全建议：存储介质优先物理销毁。

7 事件与漏洞上报

7.1 应急处置

当发生非法登录、组态篡改、脚本异常、勒索攻击等安全事件，按以下步骤处置与复原：

1. 事件确认：核实告警信息，确认安全事件类型与影响范围。
2. 隔离止损：断开受影响工作站 / 服务器网络，锁定异常账号，阻断攻击链路。
3. 取证留存：保存日志、组态文件、进程快照，不修改现场原始数据。
4. 根源排查：分析审计日志，定位入侵入口、恶意操作点。
5. 系统复原：用干净备份组态 / 镜像恢复系统与工程文件，恢复前清理恶意程序、修复安全缺陷。
6. 验证上线：复原后校验工程数据完整性、权限配置，确认无异常再投入运行。
7. 事件复盘：记录事件全过程，更新防护策略。

7.2 漏洞上报

台达漏洞上报地址：[产品网络安全上报 - 台达](#)

台达漏洞反馈邮箱：Delta.PSIRT@deltaww.com

如果您发现我们的产品有潜在的网络安全漏洞，请根据漏洞上报地址中的选项完整填写，亦可透过 mail 连同补充资讯(例如：日志、crash dumps、packet captures、屏幕截图等)一起提供给我们。您的通报我们将进行确认，如果需要，将安排人员与您联系。若未提供完整产品网络安全漏洞资讯，我们将无法受理。

7.3 漏洞披露

遵循协同漏洞披露 (CVD) 机制。用户应通过官方渠道 (官网、邮箱) 反馈漏洞，厂商负责评估、复现、开发补丁并发布安全通告，严禁私自公开未修复的漏洞细节，相关国家针对私自披露负有刑法责任。

台达漏洞公告地址：[产品网络安全公告 - 台达](#)

8 第三方元件及产品漏洞管理

8.1 第三方元件漏洞管理

DIAGView X 集成了多种第三方元件 (如开源库、驱动程序等)，其安全性直接影响整个系统的稳固性。

资产清点：DIAGView X 建立并维护一份准确的第三方元件资产清单，进行漏洞管理和风险评估

主动监控：定期根据 SBOM 清单，主动跟踪其中第三方元件的公开漏洞信息

风险评估：一旦发现相关漏洞，立即评估其对系统的影响范围和严重程度

协同处置：关注台达官方发布的安全通告 (Security Advisory)

8.2 产品漏洞管理

1. 外部安全问题(客户、研究机构、第三方)

建立安全问题反馈入口接收外部提交的安全漏洞，收到反馈后及时回执并登记工单。组织安全、开发团队开展风险评估。

2. 内部重大安全问题(SAST、内部测试)

内部发现重大安全问题，评估后若漏洞存在客户侧可利用风险，按规范对外发布安全通告

本产品 SBOM 与自研漏洞管理，仅覆盖产品打包内置的自研代码与第三方组件。宿主操作系统、用户使用的独立外部中间件不属于本产品漏洞管理范围，相关漏洞监控、处置由现场运维方负责。

▲ 安全建议：具体漏洞上报和披露流程参考 7.2 & 7.3 章节

9 最终用户责任

本安全指南所载信息旨在为最终用户提供参考依据，便于用户结合自身需求，合理选择技术方案以达到预期安全等级。

保障 DIAView X 系统安全的基础前提：至少落实并持续维护 工业控制系统安全 规定的基线安全要求。同时建议同步实施并持续满足工业控制系统安全的合规要求。

最终用户同时负有以下责任：在持续演变的威胁环境下，确保整体工业自动化与控制系统（IACS）网络安全管理体系能够长期落地、持续运维，使网络安全水平稳定维持在预设目标等级。任何软件产品的安全能力，都依赖于部署现场落地的运维安全策略与管理制度。维护网络安全运行环境属于使用单位的责任。

10 文档维护

确保本安全指南的时效性与准确性，适应系统演进与标准变化。

定期复审：建立每个版本复审文档的机制。

动态修订：在发生以下情况时，必须立即启动文档的修订、审核与重新发布流程：

1. DIAView X 发生大版本跨越（如架构升级）

2. 相关国际或行业安全标准更新
3. 发生重大安全事件后，需总结经验教训并更新防护措施

更多资源访问：[台达 DIAView X 工业组态系统](#)