产品安全使用手册

UM024004C_20241004

1. 安全指南

1.1 文件目的

为了使人机界面与其相关软件在使用时能提供安全正确的安装、操作、维护及淘汰等操作，本文件将参考 IEC 62443-4-1 标准，列举出使用人机界面时会遇到的配置与工程档案的设计相关的安全强化机制，强烈建议用户参考本文件的步骤操作，在应用正式运行之前落实最大限度的安全防范措施，并在运行过程中持续维护，以确保应用不会受到负面影响，直至产品被安全淘汰为止。
注意: 文件中的 SG-X 代表对应 IEC62443-4-1 SG 对应的指引。

1.2 文件架构

本文件将围绕产品生命周期，从初始配置、到软硬件设置，最后到产品停用后的处置，详细探讨以下各主题领域机器对应的安全策略。

- 初始配置：最大限度地减少与防止配置过程中的操作风险
- 编辑程序：分析程序编辑软件中存在的风险
- 产品运行：规范管理者与操作员的权限管理
- 远端维护：采取适当的保护措施防止非必要的远程访问
- 硬件相关：管控外部储存设备的使用安全
- 产品生命终止：明确安全淘汰规则

1.3 纵深防御

纵深防御的概念就是，不单单仅依靠单一的安全措施，而是在各个层级都部署相应的安全防护机制，藉此大幅降低信息外泄与黑客攻击等潜在风险，并提升产品在安装、操作、维护及淘汰时的安全保护。

1.3.1 外部环境 (SG-2/SG-3a)

针对产品安全的外部环境防护主要包含现场安全、网络环境安全以及系统整合安全三道防线，以下分别说明：

现场安全

通过系统排查，确保人员对人机界面的安全使用。

- 在校园或工厂等场所设置带有门禁控制的围栏。
- 在实验室或服务器机房中采用生物识别技术访问控制或锁定机制。
- 安装报警系统或视频监控设备。

网络环境安全

为确保网络通讯不被轻易渗透，请简化网络环境。

- 在办公室网络与工厂网络间部署防火墙，监控通信接口。
- 将网络通讯架设于路由器后端，避免能直接通过公开 IP 就能访问到产品。
- 若是产品上有两个以太网端口，建议将 LAN 1 连接外部网络，LAN 2 连接内部设备，实现通信数据与外部网络的物理隔离。

系统整合安全

确保系统整合过程中，内部防护功能（如杀毒软件、白名单机制等）正常运行。

- 定期系统维护与更新。
- 工厂或人机操作员的用户进行身份验证。

1.3.2 产品操作 (SG-1/SG-3c)

人机界面的系统配置通常皆为制作文件与系统整合的人员来操作，在用户操作过程中应避免参数被修改而造成无法正常使用的情况，因此一般建议采取以下措施：

- 隐藏系统设置。
- 修改默认登录密码。
- 通过网页设置页面访问时，须采用 HTTPS 加密通讯。

1.4 一般安全性维护 (SG-3h)

本节说明维护产品安全性的准则与建议，帮助用户有效地规划和执行日常信息安全维护工作。

- 定期更新产品版本，确保软件和韧体都维持在最新的版本，包括应用程序、操作系统等。这样既能防范已知漏洞被利用，也能获取新的安全功能。
- 针对安全漏洞定期进行测试，包括漏洞扫描、渗透测试等，以确保产品的安全性。及时发现并修复潜在的安全漏洞。
- 借助产品自带的监控功能，实时监控产品的运行状态、检测异常行为和安全事件。同时，储存所有的安全事件记录，以便日后分析和调查。
- 采用适当的加密机制处理敏感数据和通信，确保资料在传输和储存过程中都能保持机密性和完整性。
- 制定应急预案，有效应对可能发生的安全事件，并迅速采取应对措施。建立漏洞管理流程，定期开展漏洞评估、追踪和修复。
- 若本产品向外部服务供应商开放访问权限，需确保其遵循相同的安全标准，并定期评估其安全性。可参考外部供应商的管理国际标准。(e.g. ISO 28000 / ISO 27001)

1.5 风险分析与回报机制 (SG-3g)

在使用产品的过程当中，若发现安全相关风险，请执行以下的流程并尝试强化产品安

全来达到风险管理的需求。

- 风险分析
- 产品安全使用手册
- 评估风险是否消除
- 若无法独立解决此问题，请使用提供的 URL 地址报告此问题。

2. 编辑程序时的风险

2.1 安装文件确认

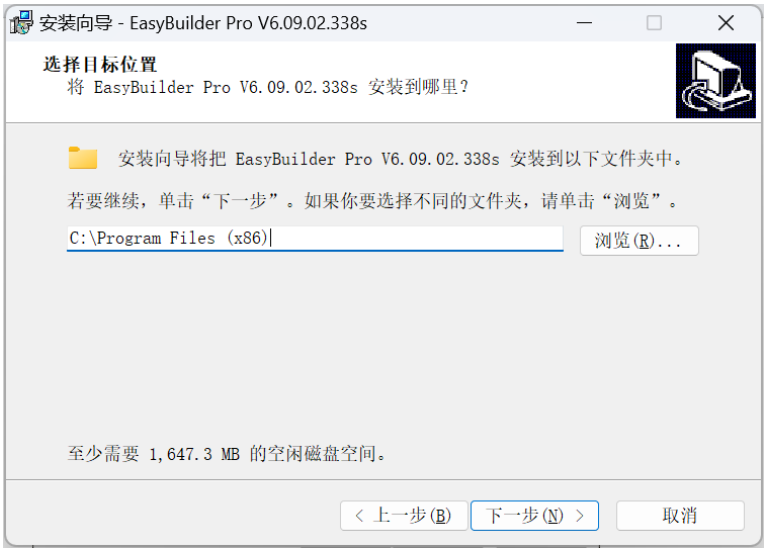
2.1.1 数字签名

在安装 EasyBuilder Pro 前，请确认安装文件(setup.exe)是否有数字签名，且签名没有被破坏。在安装文件时可使用右键进入数字签名的属性，点击“详细信息”确认数字签名是否为正常。

数字签名

2.1.2 安装路径

安装 EasyBuilder Pro 至访问权限受限的文件夹中 (e.g. C:\Program Files (x86)) 。



安装路径

2.1.3 启用自动更新

开启 EasyBuilder Pro 自动更新，确保可及时升级至修复安全漏洞的最新版本。

进入 EasyBuilder Pro 之后，点击上方菜单栏 [文件] 开启 [偏好设置] 页面，在 [其他] 选项页中，勾选“当新版本的 EasyBuilder Pro 推出时通知”选项。

当新版本的 EasyBuilder Pro 推出时通知

2.2 软件安全设定 (SG-3d)

2.2.1 启用安全通讯

开启安全加密通讯确保 HMI 与其他设备通讯时采用加密数据传输。

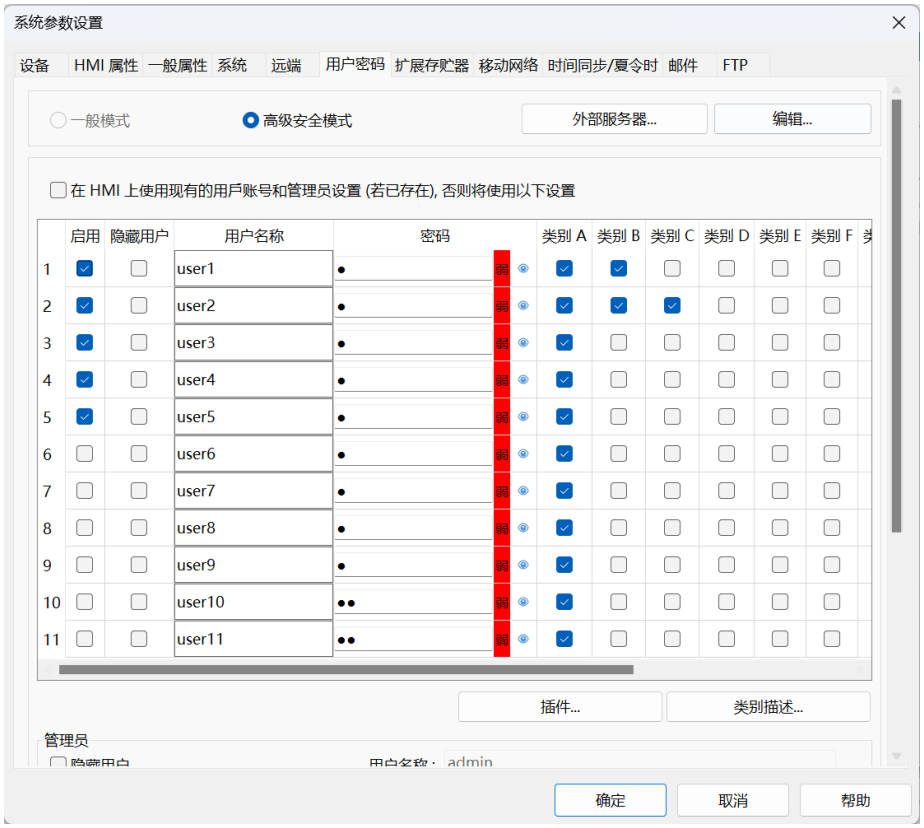
进入 EasyBuilder Pro 之后，点击上方菜单栏 [常用] 开启 [系统参数] 页面，在 [设备] 选项页，点选 HMI 并进入 [设置/保护] 窗口即可启用安全通讯，如下图。

启用安全通讯

2.2.2 使用高级安全模式 (SG-6)

建议启用高级安全模式操控 HMI。工程设计人员可针对不同的用户提供不同的类别权限，藉此来控制特定元件的访问权限。

进入 EasyBuilder Pro 之后，点击上方菜单栏 [常用] 开启 [系统参数] 页面，在 [用户密码] 选项页中，选择高级安全模式，如下图。详细设置请参考使用手册第 10 章。



高级安全模式

2.2.3 高强度的用户密码

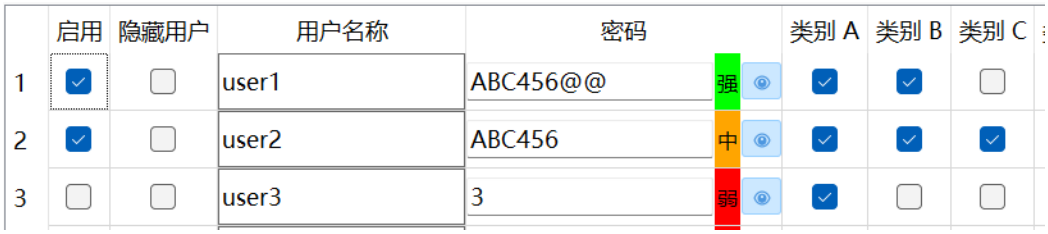
越复杂的用户密码越不容易被恶意破解，在设置用户密码时，窗口中会通过颜色及强度来告知该用户密码的安全等级。

主要分成大写英文字母、小写英文字母、数字与符号四种类型。规则如下：

强：上述类型三种以上且长度大于 8 个字符。(请参考下方建议)

中：上述类型两种以上且长度大于 6 个字符。

弱：其余类型。



用户密码强度

(建议)如何设置高强度的的用户密码？

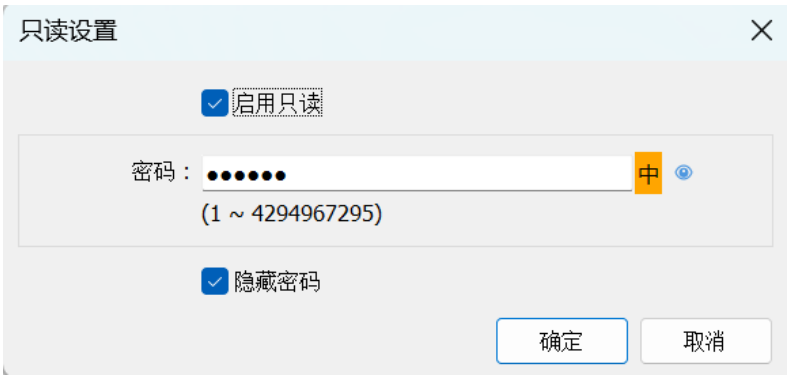
- 字符长度至少大于 8 个；
- 请不要只使用一种类型，建议将大、小写英文字母、数字与特殊符号混合使用；
- 请不要使用字典中常见的词汇 (例如: Mouse)；
- 请不要使用键盘上连续排列的字符组合 (例如: 123456 或是 asdfgh)；

- 请不要使用重复的字符 (例如: AAAA)。

2.2.4 用户密码安全设置防护

启用“只读”模式后，即便他人取得原始工程文件，也能防止未经授权的用户进行安全设置。在只读模式中，安全设置无法被变更，且密码将以隐藏形式显示，以防止密码泄露。必须使用原始设置的密码才能重新取得管理权限。

在 [用户密码] 选项页，点击 [编辑] 进入 [只读设置]，启用只读后，即可保护用户密码信息，防止被恶意查看。



只读模式

2.2.5 启用自动注销

当 HMI 处于闲置状态(无人操作)时，为了避免前一位用户离开后忘记注销，导致后续使用者获取其使用权限，建议启用自动注销。

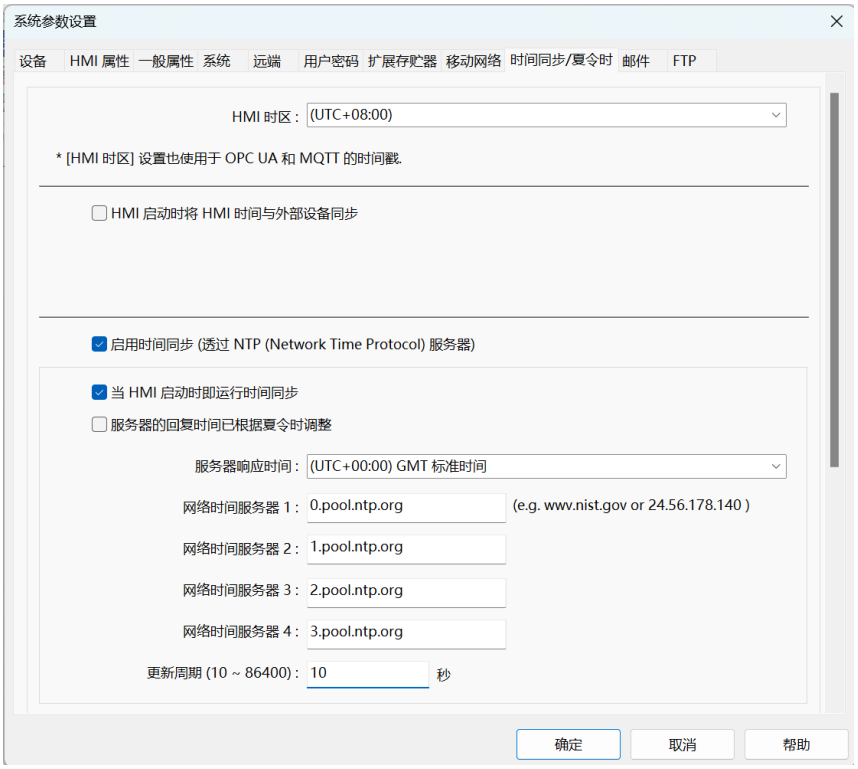
进入 EasyBuilder Pro 之后，点击上方菜单栏 [常用] 开启 [系统参数] 页面，在 [系统] 选项页中，启用自动注销，如下图。

自动注销

2.2.6 启用时间同步 (透过 NTP 服务器)

为了确保时间的正确性，建议将 HMI 的时间定期与 NTP 服务器同步。

进入 EasyBuilder Pro 之后，点击上方菜单栏 [常用] 开启 [系统参数] 页面，在 [时间同步/夏令时间] 选项页中，启用时间同步(透过 NTP 服务器)，如下图。



时间同步

2.2.7 元件安全

HMI 的基本操作元素为元件，针对每一个可操作的元件，建议用户启用安全控制，在实际发出命令之前提供再度确认的功能，另外也可以搭配用户密码的权限功能实现对元件的管控。

进入元件的属性，在 [安全] 选项页中，启用安全控制以及用户密码的权限管控，如下图。

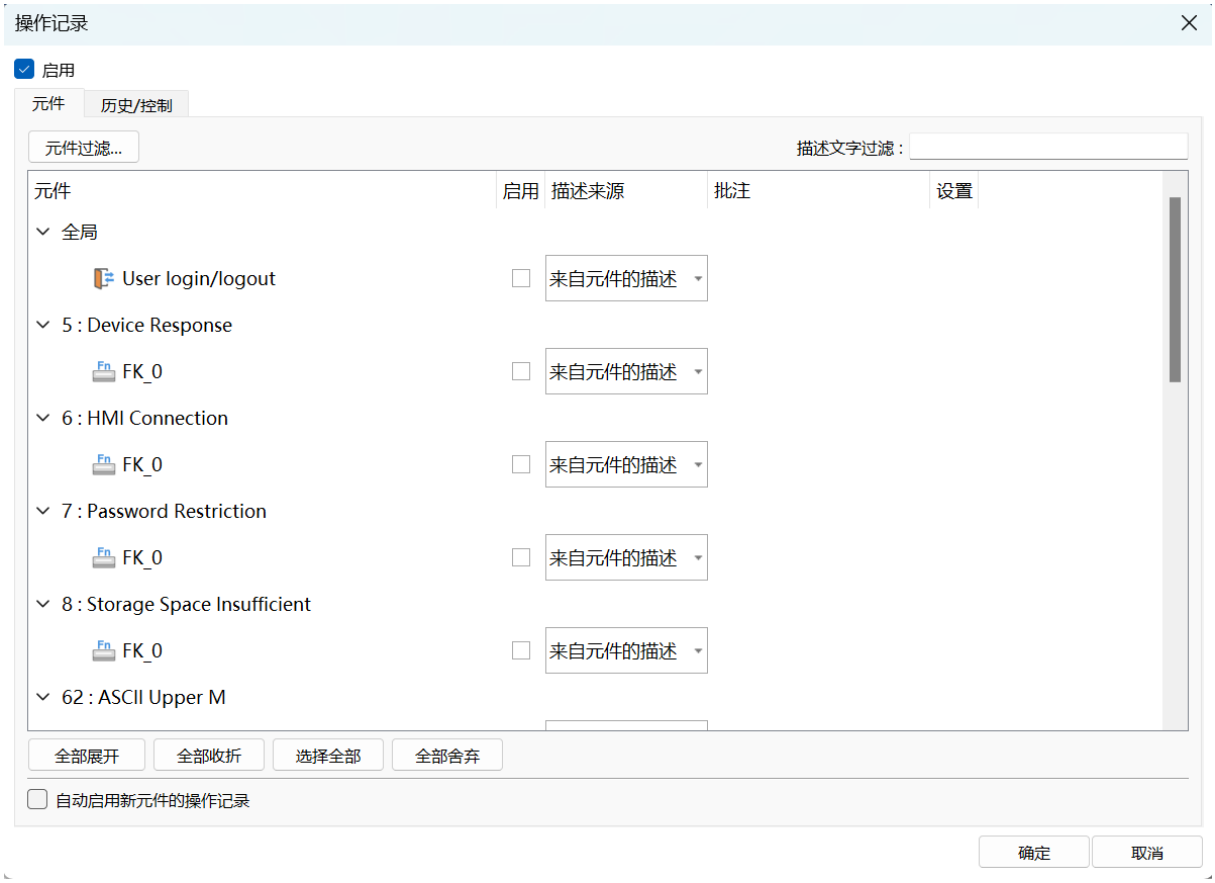
元件安全

2.2.8 操作记录

当对各类元件进行操作时，[操作记录]能记录所有关于该动作操作的信息，包括：日期/时间、用户名称、类别、窗口、元件名称、用户定义的描述、动作(元件类型)、地址、以及变更信息。

开始记录后，操作记录会预设以 SQLite 数据库格式储存在 HMI 内存中，也能备份至连接的外部装置中，例如 U 盘。

[元件] » [操作记录] » [操作记录设置] 启用操作记录功能。选择所有需记录操作过程的元件，并写下关于该元件执行动作的描述。这些描述也会一并记录在操作记录中。



操作记录设置

提示：点击元件过滤能指定欲检视的元件

用户务必需完成此页的详细设置，否则可能导致资料遗失。在将外部存储器的资料同步之前，请确认 HMI 存储器的最大记录笔数，以免超出上限。请同时将资料同步至外部装置中，以便在 HMI 空间不足时，作为备用，以防资料丢失。

操作记录使用控制地址，以便在 HMI 运行时，对操作记录下指令，或是确认与操作记录相关的状态报告。请谨慎使用控制地址，避免意外清除资料，或是关闭操作记录，并且尽可能报告所有执行结果。

如欲检视操作记录，可在画面上放置一个操作记录检视元件。

3. 产品运行时的风险 (SG-5)

3.1 登入权限

开启网络浏览器 (Windows Edge, Chrome, Firefox) 并输入 cMT X 系列人机的 IP 地址，此时即可进入 cMT X 系列人机的网页设置页面。若输入 IP 地址出现的是 Webview 界面，则需要输入 https://HMI_IP/admin 才会是 Easyweb 2.0 系统参数登入页面。

有设置，而登入 [Update] 时，可更改的设置项目则较少。基于安全考量，进入设置前须先进行密码确认。另外进入 [History] 前，须登入密码，登入后可备份历史资料。请分别设置管理者与操作者的密码，避免操作者拥有管理者的权限。

登入权限

3.2 历史档案安全

历史档案包含资料取样、事件记录以及操作记录元件所产生出的档案，可藉由本节的内容来加强与历史档案相关的安全性。

3.2.1 延长闪存存储器寿命

因为 HMI 内部的闪存存储器有写入次数的限制，若大量或频繁的写入历史资料，将缩短闪存存储器的寿命，导致历史资料无法读取而最终 HMI 可能无法启动。

因此建议闪存存储器的每分钟平均写入速度应小于 1200 KB/min。(此信息可以在 HMI 上的 System Setting 中取得)

平均写入速度

降低闪存存储器写入速度的建议：

资料取样

- 若未有历史档案的需求，仅需要检视 HMI 开机后产生的资料，则不需要勾选储存历史资料。
- 设置较长的取样时间。
- 减少在控制地址下达同步命令(2 或 3)的频率。
- 若使用自定义文件管理，请减少切换文件的频率。若启用周期性自动同步，也可设置较长的同步时间。

事件记录

- 若未有历史档案的需求，仅需要检视 HMI 开机后产生的资料，则不需要勾选储存历史资料。
- 若非报警用途，只是希望在某些条件满足时，执行特定动作，不要勾选 [储存为历史资料]，或改使用动作触发元件。
- 减少在控制地址下达同步命令(2 或 3)的频率。
- 启用 Aggregate 模式。

操作记录

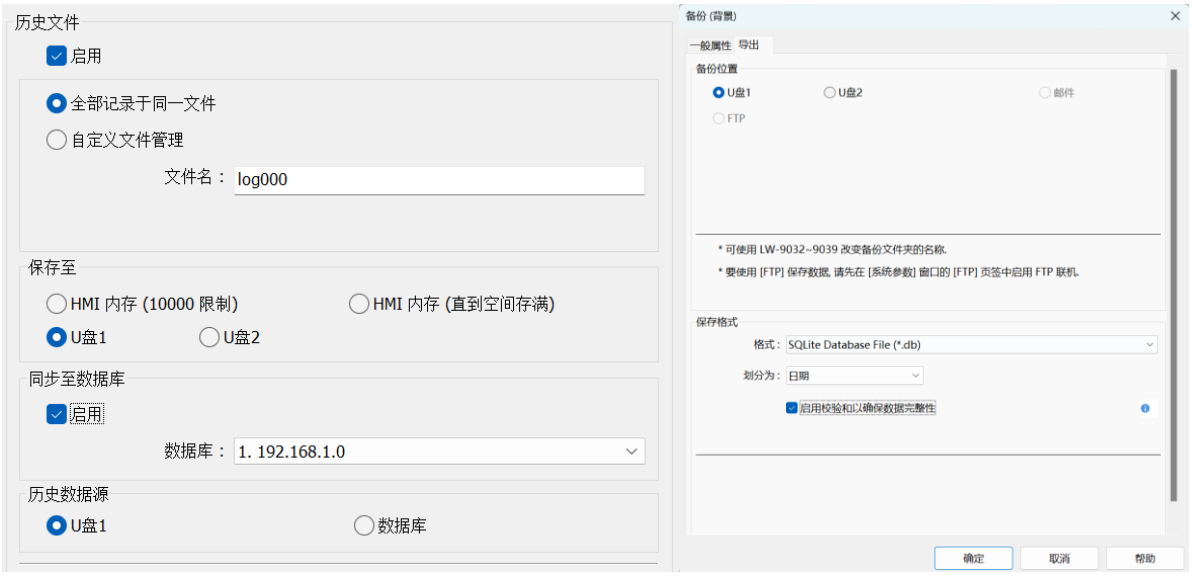
- 减少在控制地址下达同步命令的频率。
- 启用 Aggregate 模式。

Note

- 在 HMI 关机前，应将系统寄存器 LB-9034 设为 ON，以确保历史资料完整写入闪存存储器。

3.2.2 储存/备份历史文件到外部装置

建议将历史文件储存或备份到外部装置，例如：U 盘、SD 卡或是同步至数据库服务器，以便在 HMI 空间不足时，作为备用，以防止资料丢失。



储存/备份历史文件到外部装置(以资料取样为例)

外部装置选用 U 盘与 SD 卡的建议：

外部 U 盘与 SD 卡也有写入次数的限制，依照存储器种类不同，有不同的写入次数上限。若历史资料写入较为频繁，或希望历史档案能长久保存，建议尽量使用容量较大的 U 盘与 SD 卡 (e.g. 32GB) ，且定期 (e.g. 每年) 执行一次远程备份。

外部装置选用数据库服务器的建议：

启用 RAID，且定期 (e.g. 每年) 执行一次远程备份。

3.2.3 备份档案完整性

威纶通提供的 EasyConverter 工具能在计算机上开启 SQLite 档案，以显示备份文件资料，并支援将文档输出为 Excel/CSV 格式。若备份文件含有校验和(checksum)，EasyConverter 将验证校验和，确认资料的一致性。在产生备份文件时勾选 [启用校验和以确保资料完整性]，即可启用此功能。此功能只支援于 cMT/cMT X 系列。

备份元件校验和设置

EasyConverter 可用于检验备份文件内容的完整性。若检验时发现文档可能已被窜改，EasyConverter 将发出警示。

4. 远端维护时的风险

4.1 通讯安全

4.1.1 关闭不必要的功能 (SG-3b)

在使用 HMI 时，若未使用的情况下，尽量关闭不必要的功能，或是至少使用密码防护：

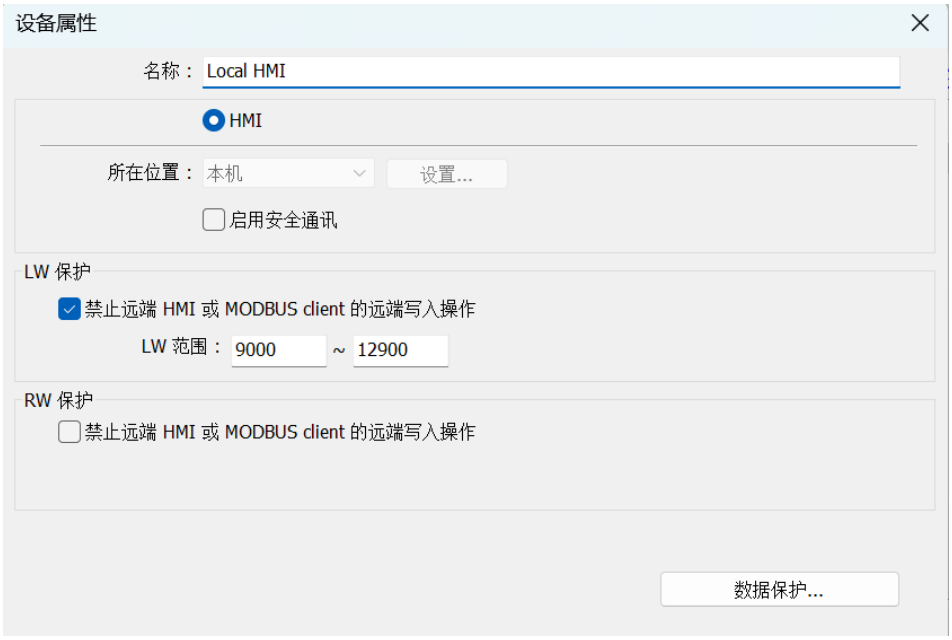
1. 远端 HMI
2. PLC 控制 (换页)
3. Modbus 服务器
4. VNC 服务器
5. cMT Diagnoser (cMT/cMT X 系列)
6. OPC UA 服务器 (部分 cMT/cMT X 系列)

此列表并非详尽无遗。

4.1.2 Modbus 服务器

HMI 程序若有使用 Modbus 服务器，请在 [系统参数] 的 [设备] 选项页中，选择 [设置/保护]，并勾选 [LW 保护]，以避免 HMI 与 Modbus client 端通讯时，系统寄存器的相关功能被任意调整，如下图。

注意: 需设置保护的 LW 范围请查阅系统寄存器支援范围。



LW 保护

4.1.3 MQTT

HMI 程序若有使用 MQTT 功能，请使用 TLS 1.2 安全加密通讯，并导入服务器 CA 凭证、客户端凭证以及密钥文件。

选择 MQTT 服务器元件之后，在 [TLS/SSL] 选项页中，启用加密以及认证功能，如下图。

MQTT TLS/SSL 加密

4.1.4 OPC UA 服务器

HMI 程序若有使用 OPC UA 服务器功能，请取消勾选明文通讯，改使用安全加密通讯。

选择 OPC UA 服务器元件之后，在 [一般] 选项页中，取消勾选 [无] 的安全策略，强制客户端必须以加密的内容通讯，如下图。

OPC UA 服务器安全策略

4.1.5 数据库服务器

HMI 程序若有使用数据库服务器功能，请使用 TLS 1.2 安全加密通讯，并导入服务器 CA 凭证。

选择数据库服务器元件之后，在 [TLS/SSL] 选项页中，启用加密以及认证功能，如下图。

数据库服务器 TLS/SSL 加密

4.1.6 邮件功能

HMI 程序若有使用邮件功能，请使用需要认证的 SMTP 服务器并启用 TLS/SSL 安全加密类型连结。

在 [系统参数设置] 启用邮件功能之后，勾选 [SMTP 服务器需要认证] 与 [使用下列加密类型连结]，如下图。

邮件功能加密

4.1.7 cMT Viewer 远端监控

若 cMT/cMT X 系列 HMI 有远端监控的需求，用户可以透过 cMT Viewer 来监控画面。

建议在 HMI 的系统设置修改各个权限的密码，于 cMT Viewer 中使用各个权限的密码皆可登入监控画面，系统密码设置页面如下图。


设置
系统密码
系统设置
系统密码
进阶安全模式
VNC 设置
EasyAccess 2.0
语言
输入法
系统设置
更新工程文件
历史
用户
系统密码

4.2 网页安全

cMT/cMT X 系列 HMI 可透过网页登入设定页面 EasyWeb 2.0 并具备各种功能，包含设定网络 IP、上传下载工程文件、备份资料等至关重要的内容，所以网页的安全也是必须按照建议设定来进行保护。

4.2.1 启用 HTTPS 安全加密通讯

建议启用 HTTPS 加密通讯。

进入 EasyWeb 2.0 之后，从左方 [系统管理] 开启 [安全设定] 页面，启用 [强制使用 HTTPS] 选项，如下图。

强制使用 HTTPS

4.2.2 启用系统密码强度规则

建议启用系统密码强度规则。针对登入网页密码的长度、大小写、特殊字符进行强制使用的限制，可强化网页整体的安全性。

进入 EasyWeb 2.0 之后，从左方 [系统管理] 开启 [安全设定] 页面，在 [密码强度规则] 的范围进行设定，设定完毕请使用 [保存] 储存，如下图。

密码强度规则

4.2.3 启用系统密码有效期限

建议启用系统密码有效期限。在此可设定天数，若系统密码使用期限到期后建议强制更换新的系统密码。

进入 EasyWeb 2.0 之后，从左方 [系统管理] 开启 [安全设定] 页面，在 [密码过期] 的范围进行设定，设定完毕后请使用 [保存] 储存，如下图。

密码过期

4.2.4 启用登入失败锁定功能

建议启用登入失败锁定功能。用户在登入其网页时，若尝试 5 次密码登入失败的话，该系统将会停止 10 分钟。

进入 EasyWeb 2.0 之后，从左方 [系统管理] 开启 [安全设定] 页面，启用 [登陆失败次数达到上限时自动封锁] 选项，如下图。

登陆失败次数达到上限时自动封锁

4.2.5 修改出厂预设系统密码

经过上述网页设定的修改之后，请修改出厂预设系统密码，并变更至高强度密码。

进入 EasyWeb 2.0 之后，从左方 [系统管理] 开启 [系统密码] 页面，可在此重新设定系统登入密码，如下图。

修改系统密码

4.3 定期安全维护活动 (SG-3f)

定期的信息安全维护是确保系统和数据持续安全的核心工作。以下是建议的常态化安全维护措施：

- 定期更新软件：确保您的操作系统、应用程序和所有相关的软件都保持最新的安全补丁和更新程序。可以防止已知漏洞被恶意利用。
- 定期更换密码：建议定期更换用户账户的密码，且密码需符合高强度要求，包含大小写字母、数字和特殊字符。
- 定期备份数据：执行定期的数据备份，并确保备份存储在安全的位置。这可以保护您的数据免受潜在的故障风险或攻击。
- 定期强化防火墙和入侵防护系统：确保防火墙和入侵防护系统保持实时更新。这些工具可以阻止不明来源的网络侵入您的系统。
- 定期漏洞扫描和测试：定期执行系统漏洞扫描和安全测试，及时发现可能存在的安全漏洞并加以修复。
- 定期审查权限和访问控制：定期审查用户的权限和访问控制，确保只有授权的用户可以访问敏感数据。
- 定期监控日志：定期检查系统和应用程序的日志，以检测潜在的安全事件或异常活动。
- 定期进行安全稽核：定期进行内部或外部的安全稽核，以确保您的信息安全措施符合标准和最佳实践。

5. 产品安全淘汰指南 (SG-4)

本节阐述产品需安全处置是为确保设备停用或下线时，不会因其停用而造成信息安全问题。(e.g.敏感信息外泄等等)

5.1 安全处置建议

- 将产品从设备配置中拆除且不造成任何物理损坏。
- 透过重置 HMI 的方式来完整删除产品中的程序和配置数据。
- 安全删除产品与外部储存装置中留存的历史档案。
- 安全处置产品（物理销毁），以防止产品中包含的无法删除的数据可能被泄露。