工业控制系统

示意图清单

1.0 范围

本数据册包含对工业控制系统（简称工控系统或 ICS）的防损建议，使用系统论方法来评估场所全域内的工控系统，包括 ICS 通信网络和网络安全威胁。本文的目标是从财产保护和业务连续性的角度提供风险降低解决方案。

为便于论述，工控系统在本文中定义为硬件系统和软件程序的组合，其用于为工业和非工业设施中的流程、生产、制造和相关活动提供控制、保护和监控。以下列出了可接入工控系统网络（工控网络）的部分硬件资产：

- 监控与数据采集系统（SCADA）
- 分布式控制系统 (DCS)，包括历史数据服务器
- 可编程逻辑控制器 (PLC)
- 可编程自动化控制器 (PAC)
- 外部设备网关
- 远程终端测控单元 (RTU)
- 网络，包括交换机、防火墙和其它联网设备
- 智能现场设备（例如智能仪表、阀门、继电器和过程变送器）
- 仪表总线
- 人机界面 (HMI)
- 工程师工作站（工程师站）
- 工业控制面板，包括设备和仪表柜、输入/输出（I/O）柜等。
- 楼宇自动化/管理系统
- 智能设备或工业物联网 (IIoT)

本数据册提供有关工控系统的总体性指导。如果存在针对特定设备或流程的更详细的数据册，它们将取代此处提供的指南。

本数据册未涉及以下内容：

- 工控设备或通信/网络的详细设计或运行
- 软件的性能、兼容性或功能
- 安全仪表系统的设计、操作、检查、测试和维护（参见数据册 7-45《安全控制、报警和联锁装置》）
- 用于一般业务的信息技术系统（例如用于收发电子邮件的系统、可访问互联网的系统）

1.1 危害分析

如果工控系统未得到适当的管理和维护，小故障即可能引发重大事故，从而导致产能下降和/或潜在的重大财产损失。以下情况可能引发控制系统的故障：

A. 设备检查、测试、维护和补丁管理上的不足

B. 缺乏操作经验，包括未能提供充分的上岗培训和巩固培训。

C. 员工、供应商或第三方承包商的意外行为

D. 故意的破坏行为，旨在打乱 ICS 流程和/或旨在损坏 ICS 设备

E. 与网络有关的行为，旨在破坏 ICS 流程和/或旨在损坏设备

F. 位于第三方场所内的 ICS 软件或服务发生了中断。

G. 缺乏应付 ICS 中断的适当的事件响应和恢复预案

1.2 变更

2024年1月，中期修订。作少许编辑修改。

2.0 防损措施建议

2.1 引言

取决于所应用的行业，各类工控系统的功能不同，因此没有两个工控系统是相同的。工控系统是由控制器、逻辑解算器、电机、泵、执行器、监控和传感设备等组成的复杂系统，所有这些都由通信网络来连接。工控系统依赖于多种软件包、应用程序和配方程序来控制相关的过程。工控系统设备、软件、应用程序或配方需要定期进行修改和更新以提高性能。

工控系统涵盖发电、化工和工业制造等行业的复杂控制系统，也包括仓储业或用于医院和办公场所的楼宇自动化（例如暖通空调）等不太复杂的系统。

负责全厂工控系统的员工必须全面了解整个系统，包括操作要求和保护需求、通信网络和软件需求，并应紧密协作以识别与 ICS 相关的风险和隐患。

2.2 建筑结构和位置

2.2.1 过程控制室和相关的重要设备室应位于有爆炸危险的区域之外。如果无法做到这一点，则应提供其设计符合数据册 1-44《限损结构》要求的抗压结构，假定超压施加于控制室的外表面。为满足窗户的抗撞击和所需超压性能，应采用分别符合 ANSI Z97.1（ASTM E1886 和 E1996，或 FBC TAS 201 和 203 都是符合要求的替代品）和 ASTM E1300 要求的夹层玻璃。

2.2.2 过程控制室和相关设备室的定位，应使其不会受到腐蚀性或可燃液体、易燃蒸气或机械设备（如桥式起重机）的损坏。

2.2.3 位于高处的过程控制室和相关设备室如有暴露于火灾风险，则其钢构支架需具备相应防火性能（至少为 1 小时阻火）。

2.2.4 使用不燃材料来建造过程控制室、控制中心和配套的工控仪表设备间（比如 I/O 柜）和/或工控面板。这包括但不限于吊顶、架空地板、隔墙、室内陈设、管道和 HVAC 保温材料以及 HVAC 过滤器。

如要使用塑料，应采用符合以下适用标准的 FM 认证产品或符合必要规格要求的经测试的材料：

A. FM 认证标准 4882：用于烟敏感场所的 1 类内墙和吊顶材料或系统

B. FM 认证标准 4884：数据处理中心热通道和冷通道封闭系统中使用的面板

C. ANSI/FM 认证标准 4910：洁净室材料可燃性测试规范

2.2.5 在过程控制室与附近区域之间应设置至少 1 小时阻火隔断（包括设备室和低压开关室）。本建议不适用于位于过程控制室外的独立设备。

2.2.6 如果过程控制系统有冗余配置，则应将每个系统的控制、设备和电缆安排在单独的防火分区内。

2.2.7 更衣室、餐厅、厨房、会议室、办公室等等应各有其单独的区域。

2.2.8 防火地板和墙壁上的管线穿口应使用 FM 认证或要求的穿口封堵材料来密封，且其防火等级与地板或墙壁防火等级相当。

2.2.9 屋顶排水管、生活用水管和其它液体管线的布置需要避绕过程控制室和相关的设备室。在多层建筑中，其上面的地板应进行不透水处理。如管道布置无法绕开相关区域，则应设置阻断（如利用同心管）或集水箱并安装 FM 认证的检漏器，检漏报警信号接入始终有人值班的处所。有关详细信息，请参阅数据册 1-24《液体损害防护》。

2.2.10 如水或其它液体可能汇集则应在架空地板下方安装地漏。

2.2.11 使用不燃建筑材料构建工业控制面板，包括门和/或检修口板。遵守公认的国际标准。

2.3 保护措施

2.3.1 根据数据册 1-20《防范外来火险》，保护过程控制室、配套设备室和工业控制面板免于外部火灾风险。

2.3.2 在过程控制室、过程控制中心和相关设备室内安装经 FM 认证的烟雾探测器，并把报警信号接到始终有人值守的工作站或其它地点。

2.3.3 如果关键业务系统和/或安全系统需要更高标准的探测，则可在设备室和/或工控面板内安装极早期火灾探测报警 (VEWFD) 系统，并把报警信号接入始终有人值守的房间。根据封闭空间内的配置情况，可使用经 FM 认证的吸气式或智能高灵敏度 VEWFD 点式探测系统。

2.3.4 架空地板下方和吊顶上方的空间如有电缆，则应安装经 FM 认证的烟雾探测器。

2.3.5 按照数据册 5-48《自动火灾探测》要求安装烟雾探测器。

2.3.6 过程控制室、控制中心或工控仪表设备间的消防保护要求如下：

2.3.6.1 建筑材料可燃的房间

A. 安装湿式或预作用自动喷淋灭火系统，采用自动、快速响应 (QR) 喷淋头。应根据数据册 3-26《非仓储场所的消防保护》确定以下情况的消防设计需求、软管供水要求和持续时间要求：

B. 安装专为数据处理机房配置的经 FM 认证的细水雾自动喷淋系统，并按照数据册 4-2《细水雾系统》要求以及 FM 认证产品规格清单下给出的制造商的设计、安装、操作和维护手册进行安装。细水雾系统的供水时长应为 60 分钟。

对于上面的 A 和 B 项：

- 过程控制室和控制中心的天花板或室顶的高度不超过 30 ft (9 m) 的，应基于火险 1 级 (HC-1) 来设计
- 工控仪表设备室或过程控制室和控制中心的天花板或室顶高度超过 30 ft (9 m) 的，应基于火险 2 级 (HC-2) 来设计

2.3.6.2 建筑材料不可燃的房间

应安装卤化碳或惰性气体（洁净气体）灭火系统，其设计和安装需符合制造商说明书和数据册 4-9《卤化碳和惰性气体（洁净气体）灭火系统》的要求。可接受的安装选项包括：湿式或预作用自动喷淋系统或细水雾系统（据上文 2.3.6.1 节）。

对于卤化碳或惰性气体（洁净气体）灭火系统，确保满足以下条件：

1. 应安装 VEWFD 探测系统或设置在检测到烟雾时使房间和设备（应急照明除外）自动断电，前提是要进行过程危害分析或等效评估，以证实自动断电不会损坏受控设备（即过程设备）和/或构成其它危险。
   a. 在设置自动断电时，请按数据册 5-32 有关数据处理设备和 HVAC 系统的电源隔离要求进行安装。
   b. 调整断电延迟时间，使过程设备进入安全状态的延迟时间应不超过卤化碳或惰性气体（洁净气体）灭火系统的浓度保持时间（安全系数为 2）。
2. 应安装带有监控告警/信号的极早期火灾探测报警 (VEWFD) 系统，以便在洁净气体系统喷放之前让操作者或应急响应人员有充分时间查看情况。
3. 设备外壳由金属制成。
4. 房间内尽量不使用纸张和其它可燃材料。
5. 房间内不存放任何包装材料或塑料盒。**注：**这包括所有可燃的介质（如卷筒磁带）。
6. 使用回流或补充空气的通风系统应有关机和/或风门设置。

2.3.7 为场所内的过程控制设备提供必要的保护。这种保护应基于相关工艺/过程的重要性，以及过程控制系统因火灾而损失所造成的影响。请参阅 3.1 节中有关工控设备消防的支持信息。采取以下任一措施（A 或 B）：

A. 不可燃材质的机柜，设有隔断，以使损失尽可能限于更小空间。

B. 在房间内安装卤化碳或惰性气体（洁净气体）灭火系统，前提是机柜本身通风和/或设置使该系统直接在机柜内部喷放。请遵循上面 2.3.6.2 节中的指导。

2.3.8 根据数据册 3-26《非仓储场所的消防保护》，在控制室和控制中心附近的所有建筑空间内（包括但不限于办公室、休息区、文件室、许可区、会议室、培训室、盥洗室等）提供自动喷淋保护，并基于相关空间的火险类别来设计。

2.3.9 按照数据册 2-0《自动喷淋灭火系统安装指南》和适用的特殊保护系统数据册安装消防系统。

2.3.10 根据数据册 5-32《数据中心和相关设施》要求，保护与过程控制室相关的数据中心。在使之自动关闭之前，对控制设备执行工艺/过程危害分析 (PHA)。

2.3.11 根据数据册 5-23《应急和备用电力系统的设计和保护》的要求来保护应急发电机。

2.3.12 根据数据册 5-31《电缆和母线》保护成组的电缆和电缆桥架。

2.3.13 为保护电子设备，应配置用于电气火灾的二氧化碳或洁净气体便携式（三类）灭火器，如数据册 4-5《便携式灭火器》所要求。

2.3.13.1 不得在内有电子设备的区域使用干粉灭火器。

2.3.13.2 对于普通可燃材料，需根据数据册 4-5《便携式灭火器》要求配置适当类型或多类组合便携式灭火器。

2.3.14 为过程控制室、控制中心、相关工业控制仪表设备室和/或工业控制面板制定火灾和电气响应的事前预案。

2.3.14.1 验证相关电工人员能与消防队员同时做出反应，接受过培训，能安全地断电或隔离受影响的过程控制面板并展开救火工作。

2.3.14.2 在不可对工控设备室内全部电气仪表设备和工控面板进行断电的情况下，应确保火警响应预案的内容包括对相关人员的培训，以能对受影响区域的火情和烟雾状况作出判断并根据事前预案采取适当行动，实施局部、区域或相关场所整体的手动断电。

2.4 人为因素

2.4.1 变更管理程序

2.4.1.1 工控系统的管理和 ICS 安全程序的执行，应与变更管理程序相结合。

2.4.2 工控系统的管理

管理层的意志是工控系统监督和管理程序能够得到成功执行的基石。如管理层对工控系统的管理缺乏强有力的意愿，良好的程序可能会被忽视或受其它因素影响（例如产能压力）而削弱。管理层的坚定决心是工控系统在包括资金和人员配备各方面得到必要重视的保证。

2.4.2.1 工控系统监督组

2.4.2.1.1 从总公司到属下工厂应组建 ICS 监督小组，负责 ICS 的维护工作。ICS 监督小组的职责可能包括但不限于以下内容：

- 全面了解场所内的仪表和控制系统
- 了解工艺流程详情
- 知晓 OT/IT 屏障
- 明了操作员职能
- 了解设备和/或 ICS 维护
- 熟知 ICS 网络安全和 OT 网络安全
- 采纳并落实公司政策（包括但不限于网路安全策略）

根据工厂的规模、复杂性和人员配置，ICS 监督小组可能还应包含公司和厂方管理层、ICS 供应商以及其他第三方服务提供商的人员。

2.4.2.2 资产管理计划

2.4.2.2.1 制定并实施工控系统的检查、测试和维护计划。有关制定资产完整性计划的指导，请参见数据册 9-0《资产完整性》。资产管理计划中应包括以下适用的要素：

A. 制定并及时更新接入工控网络的硬件清单，内容包括厂商、型号、序列号，及已安装的固件、软件和应用程序，包括版本号。纳入与跟踪技术过时相关的信息（即生命周期管理）。定期执行检查以识别 ICS 环境中是否有未经授权的设备或恶意设备。

B. 确保资产清单中包括 ICS 资产的关键性评估，以便确定安全工作的优先次序，及时更新安全事项。

C. 保留 ICS 的图纸和文档（如电气/控制图、网络图纸以及相关的系统、管道和仪表图 (P&ID)）。工控系统的变动应在这些文件中反映出来。

D. 有关设备清单、图纸和详细说明工控系统设计和功能的文档，应存储在受控和受限的场所。仅根据需要授予访问权限。如果这些文件是电子档文件，应使用密码对其进行保护，并在受信任网络上保存其备份副本。如有可能，对这些文档进行加密处理。ICS/OT 环境之外的所有网络都应被视为不受信任的网络，包括本地 IT 网络。

E. 制定并适时更新相关政策和/或程序文件。

F. 定期审查资产管理计划，且频次与风险相配。根据需要更新程序，以保持其有效性。

2.4.2.3 供应链管理程序

2.4.2.3.1 供应链管理程序中应包括以下适用的内容：

A. 将系统/应用程序或设备的网络安全要求作为供应商招标文件的组成部分。在合同签署/续签之前，重新评估经核准的厂商（包括第三方服务供应商）的安全策略和程序。

B. 对网络安全要求进行测试，包括出厂前执行的工厂验收测试 (FAT)、现场验收测试 (SAT)，及验收前的最后调试。

C. 制定、维护成文的政策和/或程序。

D. 定期审查供应链管理程序，且频次与风险相配。根据需要更新程序以保持程序的有效性。

2.4.3 工控系统的安全

工控系统在任何生产流程中都必不可少。有效的 ICS 安全策略对确保工控系统安全发挥着关键作用。

2.4.3.1 访问权限管理程序

2.4.3.1.1 访问权限管理程序中应包括以下适用的规定：

A. 仅限授权人员访问工控系统，包括硬件和 I/O 机柜。请参阅数据册 9-1《财产的监管》中有关内部访问权限的建议。

B. 管理承包商对工控系统的访问。请参见数据册 10-4《承包商管理》和数据册 9-1《财产的监管》。

C. 按下述要求管理用于访问工控系统的密钥：

1. 对于工控设备机柜、I/O 室或其它 ICS 设备相关区域，以及配备物理密钥的逻辑控制器（例如安全 PLC 或控制器），应遵循数据册 9-1《财产的监管》中的密钥控制建议。另见下文 2.4.3.2.1 D 节。
2. 对于配备数字密钥（即密码）的逻辑控制器（例如安全 PLC 或控制器），请遵循以下 E 项中的指南和下文 2.4.3.2.1 D 节。

D. 使用 ICS 权限凭证来控制对 ICS 的访问（即基于职责而授予对人机界面/操作员站和工程师站的访问权限）。此外，仅限有权更改流程的人员访问工程师站。为确保对工控系统访问的控制，需遵守以下规定：

1. 人机界面/操作员站的登录权限凭证可共享使用。如果相关处所/控制室始终有人值守并遵循上述 A、B 项的指导，则无需对人机界面/操作员站进行空闲会话超时设置。
2. 工程师站则应规定每次都要使用每个用户特定的唯一登录名和密码才能访问系统，并且空闲会话超时设置约不超过 15 分钟。工程师站安装有用于对逻辑控制器和人机界面进行编程的供应商程序，因此需要强化访问控制。

3. 对于具有 ICS 接口的偏远和无人处所的人机界面/操作员站和/或工程师站，其应受到用户名、密码和约不超过 15 分钟的空闲会话超时设置的保护。

4. 访问工控系统的权限凭证应独立于用于访问 IT 系统的权限凭证进行管理。在 OT 环境中及时更新的用户信息库中，保存好工控系统用户的权限凭证，定期评估这些访问权限，并删除不再需要的人员访问权限。或者，也可采用非联网的本地登录。

E. 更改所有系统、硬件和软件上的默认出厂用户名和密码。定期更新密码，或在发生重大和/或关键人员或供应商变动时更新密码。避免使用常见用户名和弱密码。

F. 使用身份验证和加密手段来保护无线通信。

G. 对于连接到 ICS 的便携设备，请采取以下预防措施：

1. 在允许进入场所之前，为临时进入场所的承包商及其他访客提供 ICS 网络安全培训。培训的内容应包括熟悉相关场所的规则和程序，如 2.4.3.1.1 节 G.2 至 G.5 所述。

2. 对于在 ICS 环境中使用的笔记本电脑（包括第三方笔记本电脑、平板电脑等）等设备，禁用无线连接，保留/检查当前的安全补丁和防病毒软件，并在每次连接到 ICS 之前进行病毒扫描。

3. 对于内存卡、U 盘、移动硬盘等，在每次连接到 ICS 之前进行病毒扫描。

4. 不得允许手机或任何启用移动网络的设备连接到 ICS。

5. 尽可能禁用与 ICS 相连的设备上的未使用端口（USB、RJ45、串行等）。

H. 制定并适时更新相关政策和/或程序文件。

I. 定期审查访问权限管理程序，且频率与风险相配。根据需要更新程序，以保持其有效性。

2.4.3.2 组态管理程序

2.4.3.2.1 安装的固件、软件和应用程序（以及每台数字设备的版本号）是确定哪些特性/功能可用的关键属性。

组态管理程序中应包括以下适用内容：

A. 对接入工控系统的所有数字设备的特性/功能和流量进行限制（即物理和逻辑硬化），仅保留支持工控系统运行和流程所需的那些特性/功能。应考虑进行物理与逻辑硬化的设备包括作为 ICS/OT 网络组成部分的设备。这包括有多种设置并进行数字通信的现场设备；执行基本控制和安全控制的逻辑解算器和控制器；监控设备、HMI 和工程师工作站；历史数据库；服务器（即应用程序、文件、数据库、打印服务器）；网络设备，例如网关、交换机和路由器；防火墙等保护设备，包括安装在工控系统 DMZ 内的所有设备。

B. 确认工控系统监督组会按照变更管理程序要求，对接入工控系统的任何数字设备所发生的全部变更都进行分析、验证和核准，了解其安全影响。

C. 使用系统监控来检查是否有对基本控制设备、安全控制设备和 OT 网络设备的任何未经授权的更改。所有网络设备和大多数工控系统组件如 PLC、DCS、IED 和智能仪表，应有系统监控选项，在启用后会提供日志、审计和告警，用以检出任何未经授权的活动。

D. 在启用系统和运行 ICS 之前，确保作为基本过程控制系统和安全系统一部分的逻辑解算器、PLC 或控制器的工作模式（即运行/编程/遥控等）为 OEM 推荐的设置选项。把对该工作模式的更改，也纳入上面系统监控建议中。

E. 制定并适时更新相关政策和/或程序文件。

F. 定期审查组态管理程序，且频次与风险相配。根据需要更新程序，以保持其有效性。

2.4.3.3 补丁管理程序

2.4.3.3.1 补丁管理程序中应包括以下适用内容：

A. 除了为逻辑解算器等实际控制设备打补丁外，厂方还应确保补丁管理程序涵盖支持和通信设备，包括但不限于远程访问服务器、跳转服务器、历史记录器、病毒防护、虚拟专用网络以及防火墙等其他网络组件。

还应包括用于检修 ICS 的任何设备，如笔记本电脑或手持设备，以及用于检查便携式设备的扫描设备如 USB kiosk 等。

B. 监测来自系统和设备制造商、ICS 集成商、政府机构及其他组织的网络安全漏洞公告与警报。重要的是，ICS 监督小组的人员需要掌握是否有会影响工厂 ICS 的漏洞。

C. 收到网络安全通知后，ICS 监督小组应根据其关键性和风险程度，确定所需采取的保护行动。例如，在安装软件补丁之前，可能需要针对系统漏洞采取额外的保护措施。

D. 安装补丁前应核实 ICS 监督组已与工控系统供应商进行了咨询。验证补丁的来源，并在安装前进行病毒检测。如有可能，请于安装前在模拟或虚拟系统中进行测试。

E. 由于缺乏 OEM 的支持，应为陈旧设备和/或软件提供额外保护措施，以抵御网络安全漏洞。

F. 制定并适时更新相关政策和/或程序文件。

G. 定期审查补丁管理程序，且频次与风险相配。根据需要更新程序，以保持其有效性。

2.4.3.4 网络保障

2.4.3.4.1 确保使用安全的对工控系统/运行技术 (OT) 环境的远程访问。ICS/OT 环境之外的所有网络都应被视为不受信任的网络，包括本地 IT 网络。采用以下适用的预防措施：

A. 按以下要求核实对 ICS 的远程访问：

如果是来自内网（连接源自场所内），例如本地 IT 网络，则使用多因素身份验证 (MFA)，通过位于工业 DMZ 中的跳转服务器（参阅 2.4.3.4.2 B 节）。

2. 如果来自任何外部网络（连接源自场所之外），例如公司总部或供应商，则应使用安全的虚拟专用网络 (VPN) 和多因素身份验证 (MFA)，利用公司的系统通过专用路径到达中间系统（工业 DMZ 中的跳转主机），然后才允许进入 ICS/OT 环境。

3. 对远程 SCADA 控制中心的工程师工作站作出限制，不允许其直接地接入本地 SCADA 服务器或 RTU。当远程 SCADA 控制中心需要工程师工作站的服务时，应使用安全虚拟专用网络 (VPN) 和多重身份验证 (MFA)，利用公司系统上的专用路径到达上述第二项中确定的中间系统。

4. 个人计算机或任何其它个人外设不用于远程访问 ICS/OT 环境。

5. 不需要时则禁用远程访问。在不稳定的情况下，限制可信来源和合同义务供应商的远程访问。

B. 不能允许远程接入安全系统。

C. 不允许长时间远程接入 ICS/OT 环境。远程监控、数据收集和诊断而且数据流为单向限制时则是可以的，对与工控系统的连接没有时间限制。

D. 用安全的现代通信方法代替拨号调制解调器。如果这无法实现，请执行下列操作：

1. 不用时则关闭和/或使拨号调制解调器断电。

2. 为有源拨号调制解调器增加保护措施（例如：回拨设置到指定电话号码、来电显示过滤、禁用自动应答）。

3. 如果公司人员发生变动和/或第三方访问相关要求发生了变化，则应更改硬件密钥或电话号码。

2.4.3.4.2 采取以下适用的网络保全措施：

A. 通过隔离（物理隔离或接口架构）或分段（集成或通用架构）在基本过程控制系统 (BPCS) 网络和安全控制网络之间设置分离。保护安全网络免受外部信号和/或活动的影响，包括来自安全网络外部的可能阻碍安全系统的恶意尝试。有关安全系统的更多指导，请参见数据册 7-45《安全控制、报警和联锁装置 (SCAI)》。

B. 采用所谓非军事区或屏蔽子网 (DMZ) 把 ICS/OT 网络与 IT 或其它业务网络隔开，并使进出工控系统的所有通信均通过 DMZ。从 ICS/OT 环境内部管理 DMZ 的一座防火墙。

C. 确保有联网和网路安全经验的员工对防火墙规则（打开的端口、允许的协议等）定期审查。对防火墙规则的更改需在 ICS/OT 环境中实施，在工控系统监督组的指导下通过 MOC 程序进行管理。

D. 基于其功能，采取对基本工艺控制系统网络进行分割和/或隔离的措施。

E. 在 ICS 环境中应尽可能使用应用程序允许名单。在采取此方案时应谨慎从事。

F. 为检出未经授权的活动，应尽可能利用网络监控和工控网络活动日志（也称为入侵侦测系统或 IDS），以及安全信息事件和管理 (SIEM) 软件。在可能的情况下，应从安全管理平台 (SOC) 来监控 OT 环境。

G. 在 ICS 和 OT 环境（包括 SCADA 系统）中使用防病毒保护软件。与 ICS 供应商或服务提供商合作，审慎选择、部署防病毒解决方案。

2.5 运行和维护

提振对工控系统按预期运行的信心，对于防止可能导致长期停机的设备和/或财产的重大损失至关重要。为最大限度地减少工控系统相关的故障和长期停机的概率，应充分利用监控和告警程序、有效的应急响应/复产方案和工控应急预案，并确保操作人员有充分培训、经验丰富，按标准和紧急操作程序工作。

2.5.1 工控系统的运行

2.5.1.1 报警管理程序

2.5.1.1.1 把对 ICS 设备和 OT 网络设备的系统监控作为警报管理程序的一部分（如果在组态管理建议 2.4.3.2.1 C 下确定是可行的）：

A. 利用系统监控来设置相关报警，用于工控设备（包括安全系统）的组态设置发生未经授权更改的监控。

B. 利用系统监控来触发报警，用于监控 OT 网络设备的组态设置发生了未经授权更改。

注：上述 A 和 B 中提到的报警不宜由现场制程操作人员来处理。相反，这些报警应上达负责监控 OT 网络设备和工控设备的人员。

C. 制定并适时更新相关政策和/或程序文件。

D. 定期审查报警管理程序，且频次与风险相配。根据需要更新程序，以保持其有效性。

有关报警管理的更多指导，请参阅数据册 10-8《操作员》。

2.5.1.2 紧急操作程序

2.5.1.2.1 工控系统的网络安全紧急操作程序是否成功的关键是如何进行计划和准备，包括安排能对网络入侵事件作出响应、有所需技能的员工以及（如果需要）第三方顾问或其他专家。

A. 验证是否确定了针对各类事件的岗位与职责，包括负责联网和网络相关事件的人员。

B. 保留关于被授权/负有合同义务在网络事件期间提供支持的供应商的信息。

2.5.1.2.2 网络/工控系统的紧急操作程序应包括以下相关内容：

A. 制定一项程序和/或策略，用以降低企业资源计划 (ERP) 系统或制造执行系统 (MES) 的损失对 ICS 和生产造成的影响。

B. 提供相关指导，说明若 ICS 的控制出现可疑行为或停止运作，应如何关闭系统和/或流程（即对系统操作使其到达一个安全状态）。这应涵盖已知或可疑的网络事件，包括但不限于以下情况：

- 黑屏/HMI 屏幕冻结
- 不明原因的机组跳闸
- 工作站出现勒索软件信息
- 工作站的光标在无操作的情况下自动移动
- 无法识别的组态变更

• 在配置或测试校准 ICS 的某些部分时出现问题

C. 验证是否存在手动模式下操作关键设备的程序。

D. 验证是否按照 ICS 监督小组确定的频率定期在桌面练习中对 EOP 进行了演习。

E. 定期审查网络/ICS 紧急操作程序，且频率与风险相当。根据需要更新程序，以保持其有效性。

2.5.1.3 应急预案

2.5.1.3.1 设备应急预案

如果 ICS 强迫停机会造成对持续运营至关重要的工厂流程和系统的计划外中断，则应根据数据册 9-0《资产完整性》制定和维护一份书面的工控系统应急预案。可行的工控系统的应急预案，其制定和维护过程的指南请参见该数据册的附录 C。另请参阅该数据册中有关备件、租赁设备和冗余设备的减损策略指南。

此外，工控系统特有的应急规划过程中应包括以下内容：

A. 应把管控意外停机和从 ICS 停机事件中恢复所需采取的行动纳入事件响应和恢复程序中（见 2.5.1.4 节）。

B. 对该预案进行测试和预演，频率由资产所有者确定并与风险相配。

C. 基于硬件清单（见 2.4.2.2.1），包括组件的关键性和生命周期管理预案，评估 ICS 设备故障备件的需求和范围。

D. 对关键业务控制系统或者工控安全系统，应给出其功能说明和布局设计。

2.5.1.3.2 每年审查工控系统应急预案来应对和管理现场风险的变化，包括工艺流程、收入流等的变化，以确保预案的可行性和有效性。

2.5.1.4 事故恢复计划

2.5.1.4.1 工控系统应急预案中，应在事件响应和恢复计划下包括以下适用内容：

A. 在试图重新启动 ICS 之前，确定意外关闭的根本原因。

B. 若发生意外关闭的情况，应尽可能保留电子记录，以便进行取证评估。

C. 为所有的 ICS 组态文件（例如，已知最新的可靠组态、基线组态）和整个功能系统所需的文档保留一份最新的可用副本。在有密码保护的实体安全地点保存备份文件的历史记录。如有可能，请使用加密保护。

1. 如果备份文件是不可变的（例如，一次写入/多次读取，不能被覆盖），那么：

   a. 不可变的备份文件应储存在不同于数据来源网络的可信网络驱动器上。

   b. 当系统发生变更及在系统更新后，应创建新的备份文件。

   c. 在上一个不可变文件的保留期结束之前，应创建新的备份文件。

2. 如果备份文件不是不可变的（例如，可以写入覆盖），则应：

   a. 使用密码保护所有备份文件。如有可能，则对这些文档进行加密处理。

   b. 对所有备份文件，其应有至少一份副本被离线储存在一个安全地点。

   c. 当系统发生变更及在系统更新后，应创建新的备份文件。

D. 审核与 OEM 和/或供应商签署的服务合同，明确组件的交付期限，以确定最佳恢复期和设备故障备件策略。

E. 制定并适时更新相关政策和/或程序文件。

F. 采用与风险相当的频率定期审核事件响应与恢复程序，但至少每年一次。根据需要更新程序，以保持其有效性。

有关事故前计划和恢复响应的更多指导，请参阅数据册 9-1《财产的监管》、数据册 10-1《事前和应急响应规划》和数据册 10-5《灾难恢复计划》。

有关事故调查的更多指导，请参阅数据册 10-8《操作员》和数据册 7-43《工艺安全》。

2.6 培训

2.6.1 在工厂的操作培训方案中，应针对安全策略和程序来加强工控系统的安全培训和安全意识。内容包括行业网络安全标准和最佳实践。

2.6.2 对与 ICS 互动的操作员和其它关键人员，在提供 ICS 访问权限前应先进行重点培训。对系统管理员或具备特权/高级访问级别人员进行额外培训（即岗位培训），以便其履行工作职责。

2.6.3 所有 ICS 人员都应接受工控系统的网路安全培训，包括初始培训和进修培训且每年都有。

2.6.4 应审查有关 ICS 安全的培训方案，审查频率取决于具体风险的大小。根据需要更新方案。

2.6.5 对消防应急人员进行过程控制室火灾的灭火培训。请参阅数据册 5-32《数据中心和相关设施》第 2.7.1 节。

有关操作员的更多指导，请参阅数据册 10-8《操作员》。

2.7 公用设施（动力设备）

2.7.1 购置不间断电源 (UPS) 和应急电源系统，使工控系统可在安全断电之前保持运行。这应包括为任何配套系统提供 UPS 电源，例如仪表供气系统（如有使用）和暖通空调（HVAC）等，这些设备在安全断电期间可能需要 UPS。

2.7.2 应按资产完整性计划中的要求对与工控相关的动力设备和配套系统（如电池、不间断电源 [UPS]、发电机和恒温空调）执行检查和维护。如需更多指导，请参阅数据册 5-28《直流电池系统》和数据册 5-23《应急和备用电力系统的设计和保护》。

2.7.3 提供使用气动空气控制装置的可靠的仪表供气系统（例如有 N+1 备用配置或设计确当的空气接收器的独立仪表空气压缩机）。

2.7.4 提供可靠的暖通空调（HVAC）系统，以维持工控系统设备正常运行所需的空间环境条件。这主要涉及对运营至关重要的 ICS 设备。

3.0 相关建议的技术支持

3.1 工控设备的消防保护

我们应认识到，提供自动喷淋保护主要是为保护房间的结构及其附近设施。在一个小房间里，即使火灾被喷淋灭火系统或细水雾系统控制了，内部所有设备也可能都损失了。因此，如果目标是保护设备本身，卤化碳或惰性气体（洁净气体）灭火系统可能是更好的选择。

过程控制设备机柜在布置时如果有很好的隔断，火灾可能只对起火的机柜造成火损，而附近机柜则损失有限。相反，过程控制设备机柜如果没有适当隔断，火舌会沿着机柜整体蔓延开来。过程控制设备损失的影响将取决于火损程度、相关过程的关键性、是否有替换零件等等。

3.2 工控系统的管理

资产所有者和工控系统监督组应制定网络安全策略来保护全厂的工控系统。可行的业务连续性计划应包括以下内容：

A. 根据公司政策确定的支持和评估网络安全活动的程序。

B. 检测威胁以及保护本厂工控系统免受来自内外部威胁的策略。

C. 尽快使工控系统和生产流程恢复并减轻影响的响应预案。

业务连续性计划包括灾难恢复、工控系统应急预案和应急响应。

3.2.1 工控系统监督组

工控系统面临的风险由于自动化本身变得更加复杂、不同系统及网络的互连、以及用于业务分析的数据采集等趋势而增加网络安全风险（也称网路风险）。为确保工厂的连续运转，工控系统需要支持小组来保护其免于网路安全风险，他们应了解网路安全方法以及产品和系统可能如何影响 ICS 的性能。

3.2.2 资产管理计划

为使工控系统能够防范网路安全风险，监督组必须知道与工控网络相连的设备。如无这些知识就无法识别将工控系统暴露于网路安全风险的设备。

接入工控网络的数字设备是需要纳入资产管理计划的资产。这包括人机界面/操作员站、工程师站、网络交换机、调制解调器、路由器、防火墙、应用服务器、打印机、DCS、PLC 和其它逻辑控制器，以及联网的智能现场设备。操作系统（例如 OT 网络“普渡模型”第 3 层上的设备）也应纳入资产跟踪。此层中的重要组件包括工厂的历史数据服务器、操作调度系统、报警和其它应用程序服务器、业务所需 IT 服务（如 DHCP、LDAP、DNS 和文件服务器）。此外，还应考虑工控网络中可能错误地接入工业物联网 (IIoT) 甚至是基本的物联网 (IoT) 设备的情况。

在识别接入工控网络的设备后，了解每个设备的固件、软件和应用程序至关重要。如无这些附加信息，就无法知道每台设备可用的功能和服务，给工控系统留下未知的漏洞。

市场上有许多供应商提供自动化的主动和被动工控识别/网络映射解决方案。在可能的情况下，采用被动式工控识别解决方案优于手动资产管理技术。

3.2.3 供应链管理方案

良好的供应链管理程序不仅有助于确保交付的设备和软件无漏洞风险，而且还考虑来自不同利益相关者的意见，使新设备和系统具备最新标准和保障优势，利于有效管理风险并确保工控系统的持续运行。

供应链是工控系统被攻击的主要途径之一。数字设备在硬件和软件两方面都使网路安全问题更加棘手。

在为工控系统安装任何新的数字控制器或其它数字设备或软件和/或应用程序之前，监督组需要确信该设备的产销监管链绝对可靠，包括开发商、制造商、供应商、运输和存储及调试和验收测试阶段。

3.3 工控系统的安全

3.3.1 访问权限管理程序

非安全接入点是工控系统上最易发生的攻击路径之一。这些接入点容易受到蓄意和无意的网络入侵。网路罪犯知道工控系统必须支持远程访问，会寻找简单的接入点来破坏系统。最坏的情况是，非经批准的第三方通过某个接入点漏洞在很长一段时间内访问工控系统，据此了解工厂工控系统和流程的重要信息，从而有时间来计划和发起网路攻击。

3.3.2 组态管理程序

数字/电子设备通过其安装的固件和/或软件，具备许多性能及通信能力上的选项和功能。为减少可能的网路攻击面，相关设备（基于设备关键性或网路安全风险分析 [cyber PHA]）需接受“硬化”处理，即仅为数字/电子设备保留工控系统运行所需的选项和功能。

一旦进行所需组态的设定并且系统工作正常，其应保存为基线组态或已知最新的可靠组态。该基线可用于在发生中断或扰乱时重建系统，无论是由于物质损坏还是固件/软件问题造成的中断。

在完成安全 PLCs 或其它控制器的组态设置后，应将 PLCs 或控制器置于制造商建议采用的工作模式（运行、编程、遥控等）。可通过移除物理密钥或设置数字密钥来将此组态配置（包括其设定和运行模式）锁定到位。这使访问管理程序得到强化，仅允许有权调整安全设置的人员访问。

监控该组态配置将能在工控系统发生未经授权的更改时及时发现问题。这种监控对于识别甚至是防止工控系统的内外部威胁很有用。

工厂人员为追求生产力会定期修改相关配置，成为日常操作的一部分。这些修改可能涉及到控制器的调整或警报限制的更改。它们还可能涉及添加新的控制方案，或重新设计现有的控制方案。市场上有自动化的软硬件解

决方案，可用于持续监控实际的组态配置，包括日常运行的变化，并将它们与记录副本（基线）进行比较。这些自动化解决方案可快速识别出任何差异并提供整改步骤，允许用户接受更改的组态或恢复到以前曾使用的良好组态。

3.3.3 补丁管理程序

在 ICS/OT 环境中打补丁，不能是有了任何新的补丁就立即实施更新。打补丁需系统地进行，应考虑 ICS/OT 环境中的漏洞和/或风险，以及是否影响生产流程等因素。成功的补丁管理程序在很大程度上取决于成功的资产管理计划和成功的组态管理程序。识别 ICS/OT 环境中的关键设备，并全面了解这些关键设备所需的功能，是成功修补程序的重要组成部分。

在安装任何补丁之前，核实和验证软件的完整性非常重要，以确保其为原始形态，未被篡改。软件的来源也很关键；在下载任何软件之前，必须确认来源是否可信。

安装补丁后需要验证系统的组态，因为补丁可能会将所有组态配置改回到出厂设置和/或给更新的设备添加新功能。

如果补丁从网路安全或性能方面来说没有好处，则可能无需安装该补丁。工控系统监督组应与 ICS 供应商合作完成在 ICS/OT 环境中部署补丁的工作。

3.3.4 网络安全保障

过去工控系统的网路安全一直不是问题，因为这些类型的系统对攻击者几乎没有价值，所以对其连接几乎没有管理或控制。现在已不再是这种情况。由于工控系统上有未知连接，以及在旧设备上运行有已知漏洞的非支持软件等问题的存在，工控系统瘫痪和流程中断已成为不可忽视的风险。

远程访问已成为供应商提供非现场支持的常用方法，也为员工访问 ICS/OT 环境提供了便捷渠道。源自外部并希望访问 ICS/OT 环境的通信应通过安全 VPN 进行，先通过公司环境下和 DMZ 下的 MFA 验证，再登录可访问 ICS/OT 环境的远程访问服务器/跳转服务器。源自公司内网并希望访问 ICS/OT 环境的通信应通过 DMZ 进行 MFA 验证，再登录可访问 ICS/OT 环境的远程访问服务器/跳转服务器。

非军事隔离区 (DMZ) 是指位于受信任网络外围的子网，在此可为不可信网络（例如因特网）提供可用资源。这样，来自不受信任区域的用户所需的服务，将不会接触到被认为是安全的网络。测试、实验室或访客网络通常采用 DMZ 来确保卓越的安全级别。在安全性方面，DMZ 可归类为半可靠，因其不是完全开放，必须在网络层级及通过“硬化”处理为其提供保护。工业 DMZ （位于 ICS/OT 网络和任何不受信任的网络之间）将根据访问权限为不同类型的用户提供多种服务。这些服务可以是网页/Web 服务器、电子邮件、文件传输协议 (FTP)、域名系统 (DNS)、IP 语音 (VoIP)、虚拟专用网络 (VPN) 和数据记录器等等。简而言之，企业希望在安全的基础上提供的服务。但是，DMZ 也用于分隔或屏蔽可靠网络中的环境和系统。因此，它成为外部世界与企业关键资产之间的屏障。在某些环境中，这种逻辑分离可能意味较低的性能水平，而这通常是工业环境中一个相关的标准，因为各种环境之间的通信受到监控和过滤。DMZ 存在于 IT 网络和工业环境 (OT) 之间是正常的，因为 IT 网络是更频繁的攻击目标，如果与 OT 通信，它们可作为工业环境的入口。

入侵侦测系统 (IDS) 可以提升安全级别。虽然 IDS 可有效识别可疑网络活动，但在工控网络内实施 IDS 有一定程度的复杂性，对于某些网络或工厂来说其部署较为困难：

- 非原设备厂家的 IDS 解决方案可能与原始软件或系统不兼容，例如会在系统中引入不可接受的延迟。
- 来自 ICS 的告警需要传给 SOC。

基于印迹的 IDS 侧重于搜索印迹（即攻击模式）来侦测入侵。这些印迹需要定期更新，以便识别最新的攻击模式。

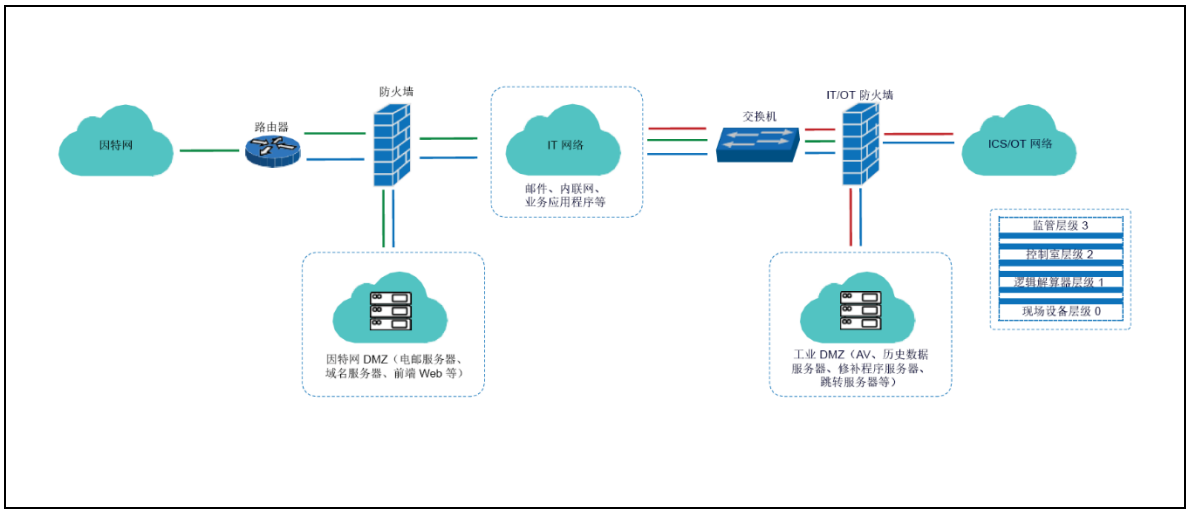

图 1. 显示企业/互联网 DMZ 和工控系统/工业 DMZ 的通信路径示例

基于异常现象的 IDS 专注于意外活动模式来侦测入侵。例如，网络活动激增、多次登录尝试失败、被标记为可疑活动的异常网络端口活动。这些告警会定期转到安全运营中心 (SOC)。

3.4 损失事故举例

3.4.1 乌克兰电网

崩溃覆盖（Crash Override）恶意软件。2015 年 12 月 23 日，乌克兰发生了备受关注的工控系统无授权入侵事件，导致多次非计划性停电，给大约 22.5万客户造成影响。停电是因为三个地区性配电公司遭受远程网络入侵。在努力恢复供电期间，相关公司继续在困境下运营。

据悉，这次网路攻击是在对相关的网络进行长期深入侦察后，同步和协调下进行的。一些报告表明，这发生在六个月的时间里。报告称，对各公司的网路攻击相继发生，彼此间隔不超过 30 分钟，多处设施受到冲击。在事件发生时，有多个外部人员使用操作系统层级的现有远程管理工具，或通过虚拟专用网络 (VPN) 连接的工控系统 (ICS) 远程客户端软件，对多个断路器进行了未经授权的远程操作。据悉，这些外部人员在网路攻击之前即获得远程访问所需的合法权限凭证。

这三家电力公司报告说，在网路攻击结束时有许多系统被 Kill Disk 恶意软件删除了。该恶意软件会擦除系统上的选定文件并破坏主引导记录，从而使系统无法运行。此外，据悉，远程终端测控设备中嵌入的基于 Windows 的人机界面也被 Kill Disk 覆盖。变电站的许多串口转以太网设备因固件损坏而无法运行。为干扰预期的恢复工作，攻击者通过 UPS 远程管理界面使不间断电源 (UPS) 断开了连接。

这三家公司报告说感染了名为黑色能量的恶意软件，但不确定其是否卷入这次网路攻击。据悉，该恶意软件是通过带有恶意附件的鱼叉式网络钓鱼电子邮件传递的。这尚未得到证实，但人们怀疑“黑色能量”可能被用于获取合法权限凭证。但是，应该注意的是，任何远程访问木马程序都可能被使用。

袭击发生后，公司无法远程重置断路器，因此不得不派遣员工去完成手动开关操作。这导致了持续四到六个小时的断电。需要指出的是，没有任何发电设施因该事件而造成损失的报告。

3.4.2 特里西斯（TRISIS）

2017 年 12 月，安全研究人员在中东的一家大型工业设施中发现了针对安全仪表系统 (SIS) 和分布式控制系统 (DCS) 的恶意软件攻击。该恶意软件被网路安全组织称为 TRITON 和 TRISIS，被国土安全部的 ICS-CERT 小组称为 HATMAN。该恶意软件影响了施耐德电气的 Triconex Tricon 安全控制器和 HMI，使攻击者可读取/修改控制器内存的内容（即通过远程网络连接覆盖现有程序）。

根据现有信息，攻击者在获得对 SIS 工程师站的远程访问权限后部署了该恶意软件：用于与安全控制器 (Triconex) 通信的基于 Windows PC 的可执行文件以及下载到控制器的恶意二进制组件。被要求调查此事的

FireEye 网路安全公司 Mandiant 在其报告 [1] 中表示，“该恶意软件可读写程序并查询控制器的状态。它还能使用 TriStation 协议与控制器进行通信，这是一种专有协议，TriStation 软件（Tricon 编程软件）用之于与 Triconex 安全系统进行通信。攻击者似乎熟悉 Triconex 系统，并在攻击前测试了该恶意软件。”

根据 Mandiant 的分析，有证据表明攻击者也获得了对工厂 DCS 的访问权限，但决定破坏安全系统。攻击者在试图重新编程控制器以造成物理损坏时意外导致系统关闭。由于处理器之间的验证检查失败，系统随即进入故障安全状态，即系统自动关闭并向业主报警。正如 Mandiant 所说，“同时控制 DCS 和 SIS 可能使攻击者有能力造成重大损害。”

ICS-CERT 和 Dragos 表示，本次事件中受攻击的控制器属于旧控制器，其中使用的 TriStation 协议缺乏对后门帐户的身份验证或加密机制，而这在紧急状况下对于确保管理员级别的访问及对设备的控制至关重要。但是，较新版本的 Triconex 系统包含这些帐户的身份验证要求，不太容易受到此类攻击。施耐德电气下发的安全通知证实了该漏洞的存在，他们已开发一种工具来检测和删除 Tricon 控制器中的恶意软件。他们还表示，提供物理操作控制的硬件密钥开关被留在“编程”模式下，这在不对控制器进行编程时被认为是不符合要求的做法。

Triconex 系统是市场上享有高度评价的安全系统。Tricon 奠基于三重模块化冗余 (TMR) 技术。TMR 采用三个隔离的并行控制系统和广度诊断工具并集成于一个系统。Tricon 系统提供高整体性、无差错、不间断的过程运行，没有单点故障。TMR 适用于输入、输出和逻辑。由于系统的占地面积和成本，它们主要用于关键的应用，例如涡轮控制（超速控制），有时也用于 DCS。尽管该恶意软件是专门为 Triconex 系统而设计，但网路安全组织认为该恶意软件的功能和攻击方式可由攻击者定制，以针对不同供应商的安全系统。此事件表明，人们对过程控制系统被侵入后安全系统也能防止损坏的信念发生了动摇。

4.0 参考文献

4.1 FM Global

数据册 1-20《防范外来火险》
数据册 1-44，《限损结构》
数据册 2-0《自动喷淋系统的安装指南》
数据册 3-26《非仓库类场所的消防》
数据册 4-5《便携式灭火器》
数据册 4-9《卤烃和惰性气体（洁净气体）灭火系统》
数据册 5-11《电气系统的雷击和电涌防护》
数据册 5-23《应急和备用电力系统的设计和保护》
数据册 5-28《直流电池系统》
数据册 5-31《电缆和母线》
数据册 5-32《数据中心和相关设施》
数据册 7-43《工艺安全》
数据册 7-45《安全控制、报警和联锁装置》
数据册 9-0《资产完整性》
数据册 9-1《财产监管》
数据册 10-1《制定事前和应急响应预案》
数据册 10-5《灾难恢复计划》
数据册 10-8《操作员》

4.2 其它

国际自动化学会 (ISA)。ISA/IEC 62443 标准和技术报告系列。

美国国家标准与技术研究院 (NIST)。工业控制系统 (ICS) 安全指南。NIST SP 800-82，修订版 2。

北美电力可靠性公司 (NERC)。关键基础设施保护可靠性标准。

电力研究所 (EPRI)，《电厂网路安全》。

美国国土安全部，国家网路安全和通信集成中心 (NCCIC) 的 ICS-CERT。

附录 A 术语表

SCADA 控制中心：使用装有 SCADA 软件的计算机控制中心，用于对远离控制中心的地点之设备进行监控和操作。SCADA 控制中心通常位于无本地过程控制（如 DCS 或 PLC）的建筑中。这些 SCADA 控制中心具有双向数据流，并可对远程设备进行操作上的改动。

安全网络：连接安全仪表系统以进行安全相关信息通信的网络。

安全系统：用于实现一项或多项安全仪表功能的系统。它由传感器、逻辑解算器和执行器任意组合而成。

安全信息和事件管理 (SIEM)：为一种应用程序，用于从信息系统组件收集安全数据、规范化审计跟踪，以及用于针对一组相关规则来记录测试，这些规则在触发时会创建用于分析的事件并通过单个界面将该数据显示为可操作信息。

安全运营中心 (SOC)：包含人员、流程和技术的解决方案，包括 SIEM 解决方案，涉及保护性监控数字环境（即 IT 和 OT）、响应可转化为事故的事件、研究已知/尚不确定的威胁、事故响应和信息共享等等。

白名单：特定实体的列表，例如主机或应用程序，这些实体已知是良性的并被核准在组织和/或信息系统中使用。例如：iPhone 应用程序知道只能从 App Store 获取更新。

补丁（程序）：旨在修复操作系统或应用程序中的错误和安全问题的软件插件。通过补丁程序使软件保持最新，可将安全风险降到最低。

不可变的备份文件：不可变的备份文件是无法以任何方式再次写入或更改（一次写入/多次读取）的，并且在保留期结束之前无法删除的文件（在创建不可变文件时，需设置此保留期的结束日期）。由于不可变文件不能更改或删除，因此这些备份文件应该是可靠的，并且可用于部署到需恢复的系统中。

操作人员工作站（操作员站）：操作员站提供全部工厂流程的动态视像，具备操作现代控制系统所需的稳定性、性能和灵活性。它提供控制图、诊断、趋势、警报和状态显示。

操作系统（OS）：支持与计算机交互的底层软件。操作系统控制计算机存储、通信和任务管理功能。

策略：一组规则，用于管控某些程序的实施方式。

程序：为执行某项任务而采取的步骤。

传感器：

1. 一种能产生电压或电流输出的设备，且其输出代表了所测物理特性（如速度、温度、流量）。
2. 一种测量物理量并将其转换为观察者或仪器可以读取的信号的设备。
3. 一种能响应输入量并产生（通常以电或光信号的形式）功能相关的输出的设备。

单向数据二极管和单向网关：具有两个节点或电路（一个仅发送，一个仅接收）的基于硬件的设备，仅允许数据流来自一个方向，即从其源头抵达目的地。在一侧使用 LED 作为数据发送器，而在另一侧使用光接收器；因此，数据在物理上不可能从另一个方向传递。有些人可能将软件解决方案（例如通过防火墙设置）甚至交换机或路由器组态方案称为单向网关，但“真正的”单向网关使用单向数据二极管作为创建单向网关的组件。根据 NIST 800-82：“单向网关是硬件和软件的组合。所涉硬件允许数据从一个网络流向另一个网络，但在物理上根本无法将任何信息发送回源网络。所涉软件则复制数据库并模拟协议服务器和设备。

单向通讯：用于确保来自设备或跨不同网络/保护区的安全单向通信的策略，例如：

1. 仅向/从设备发送模拟信号（安培数或电压）而非数字信息。
2. 一个单向数据二极管/单向网关。
3. 使用防火墙或 DMZ 中的规则跨网络传递数据。

多因素身份验证 (MFA)：多因素身份验证涉及两个或多个身份验证因素（即所知道的东西，例如密码；所拥有的东西，例如基于时间的令牌/静态令牌，或能指示身份的东西，例如指纹）。双因素身份验证为多因素身份验证的一种特例，其仅涉及两个因素。

恶意软件：此为通用术语，用于描述恶意软件，例如病毒、特洛伊木马、间谍软件和恶意活动内容。

防毒软件：保护计算机免受病毒和恶意软件侵害的软件。一旦检测到恶意代码，防毒软件会试图清理、删除或隔离任何受影响的文件、目录或磁盘。

防火墙：防火墙是一种网络安全设备，它监控传入和传出的网络流量，并根据一组定义的安全规则决定是允许还是阻止特定流量。

访问（权限）：与系统通信或以其它方式与系统互动以利用系统资源的能力和手段。这种访问可能涉及物理访问（人身进入某区域的权限，拥有实物锁钥、PIN 码或门卡或基于生物特征的访问权限）或逻辑访问（通过逻辑和物理等组合手段登录系统和应用程序的权限）。

非军事化隔离区或称外围网或屏蔽子网（工业 DMZ）：

1. 路由防火墙上的接口，类似于防火墙受保护侧的接口。在 DMZ 和防火墙受保护侧的其它接口之间的流量仍会通过防火墙，并可应用防火墙保护策略。
2. 一个插入的主机或网段，存在于公司的专用网络和因特网之间的“中性地带”。
3. 逻辑上位于内部网络和外部网络之间的外围网段。其目的是强制执行内部网络的外部信息交换策略，并为外部、非信任的来源提供对可发布信息的有限制的访问，同时保护内部网络免受外部攻击。当接入“外部”业务或公司网络时，控制网络在工控系统中被视为“内部网络”。

分布式控制系统（DCS）：在控制系统中，DCS 是指通过智能和设备实现控制，且这些设备在物理或功能上分布在要控制的过程中，而非通过一个位于中心的控制单元来实现控制。请注意，术语“DCS 控制器”是指物理控制器组件，而术语“DCS”则指整个系统，包括应用服务器、HMI 等。

分段：将网络分隔成较小的部分，各部分仍然属于同一整体网络。在 ICS 中，通常是使用虚拟局域网 (VLAN) 或硬件防火墙来实现分段。这有助于减缓恶意软件的传播或有助于阻止攻击者。但是，使用 VLAN 并不是将 IT 与 OT 分开的合适方法。

分离：彼此间不信任的不同网络的适当分离。这通常是使用防火墙（最好是正式的 DMZ）或单向网关来完成。对工控网络来说与 IT 分离是关键。

隔离：将一个网络与其它网络完全断开（气隙方式）。大型设施的安全仪表系统 (SIS) 是隔离的，因为它们不受处理基本过程控制系统 (BPCS) 的工控网络控制。

工程师工作站（工程师站）：工程师站通常是指高端的非常可靠的计算平台，专为控制系统应用程序和其它控制系统设备的组态配置、维护和诊断而设计。它通常包含对设备进行编程所需的供应商特定软件，以及用于对设备和 HMI 进行编程的项目文件。

工控设备：请参阅工业控制面板。

工控仪表设备房：过程控制设备间，通常包括许多工业控制面板和物理过程运行所需的网络设备。

工控资产识别解决方案：

1. 被动监控：一种静默、非侵入式监控技术，用于通过复制流量（通常来自跨接端口或镜像端口或通过网络分流器）来从网络捕获流量。基于 OT 的 IDS 解决方案使用这种技术进行资产识别以及侦测未经授权的活动。
2. 主动监控：一种侵入式监控技术，以相关控制器的母语（协议）执行查询，各制造商的产品略有不同。主动监控方法包括向控制器询问详细信息（IP 和 MAC 地址、固件版本、背板配置等）。

工业控制面板（工控面板或 ICP）：包含两个或多个控制电路和电源电路部件的组件。控制电路组件包括可编程逻辑控制器（PLC）、输入和输出模块、电机驱动器、工业网络设备和现场通信协议接线。电源电路组件包括电源、不间断电源 (UPS) 设备、继电器、变压器和电压/电流转换器。通常，ICP 的工作电压为 600 伏或更低，尽管 UL 508A 和 IEC 标准允许使用 1,000 伏或以下的电压。

工业控制系统（ICS）：

1. 工业控制系统是包含多种控制系统的通用术语，包括监控与数据采集 (SCADA) 系统、分布式控制系统 (DCS) 和其它控制系统组态，例如可编程逻辑控制器 (PLC)、工业部门和关键基础设施中常见的安全逻辑

解算器。工业控制系统由各种控制部件（例如电气、机械、液压、气动）组合而成，这些组件共同作用以实现工业目标（例如制造、发电、物质或能源的运输）。

2. 可能促成或影响某个工业过程的安全和可靠运转的人员、硬件和软件的集合。

攻击路径或媒介：威胁源起方用以获取或侵害他人数据或计算机网络的方法或手段。攻击路径举例说来包括阻断服务 (DoS)、恶意软件、物理访问、勒索软件和社交陷阱。

攻击者：为犯罪或谋取经济利益而创建和/或修改计算机软件和硬件的人。攻击者通常会尝试访问计算机系统以获取用户名和密码。

广域网解决方案：广域网 (WAN) 是跨越较大地域、国家甚至世界的计算机网络。在跨越地理位置的网络间传输数据的方式有多种，这些 WAN 可由不同类型的连接来构建。有线解决方案包括：MPLS、T1 和永久虚拟电路。无线通信服务包括 4G 和 5G、Wi-Fi 和卫星网络。

过程控制室：一个隔断室和/或隔离室，在其中，人员从中央或远程位置可全天候（24/7）地操作流程。过程控制室通常是独立的，但与工业控制设备室又是集成的以达到方便控制设备的功能。过程控制在工业中得到广泛应用。它通常是实现不间断流程下规模生产所必要的，例如造纸、制药、化工和发电，以及其它工业流程如监控和数据采集 (SCADA) 系统。在某些情况下，过程控制室/技术室可能无人值守且是远程操作。

过程控制中心：参见过程控制室。

基本过程控制系统（BPCS）：基本过程控制系统 (BPCS) 是管理工厂内的设备、生产和过程的系统。基于一个或多个预设条件，BPCS 使用来自控制回路的反馈对所需条件、输出或流程进行自动化管控和维持。人们可定制 BPCS 以满足任何工艺过程的需求——从非常大型和复杂的系统（例如发电系统或化工过程控制）到只有一个输入和输出的非常简单的系统（例如运动检测器或照明系统）。

基线：经过正式评估和同意的规范或产品，此后作为进一步开发的基础，并且只能通过正式的变更控制程序来更改。

基于职责的访问控制：为一种基于身份的访问控制形式，其中被识别和控制的系统实体是在组织或流程中担负的职责。

加密：对数据进行加扰，使没有其解扰“密钥”的人无法读取。将明文加密转换为密文，隐藏数据的原始含义以防其被知道或使用。

监控与数据采集 (SCADA)：用于控制分散的资产，其中集中数据采集与之控制同样重要。SCADA 系统用于分布式系统，例如：

1. 配水和废水收集系统
2. 燃油和天然气管道
3. 电力输配系统
4. 铁路和其它公共交通系统

SCADA 系统集成了数据采集系统与数据传输系统和人机界面 (HMI) 软件，形成对众多过程输入和输出提供集中监测和控制的系统。SCADA 系统是用于收集现场信息并传输至中央计算机房，再以图形或文本的形式向操作员显示此类信息，从而允许操作员从中心场所近乎实时地对整个系统进行监控或操控。基于个体系统的复杂程度和设置情况，对任何系统、操作或任务的控制可以是自动的，或者可在操作员命令下执行。

局域网（LAN）：连接有限地理区域（通常小于 10 公里）内的计算机和其它智能设备的通信网络。

可编程逻辑控制器（PLC）：小型工业计算机，最初设计来实现由电气硬件（继电器、开关和机械定时器/计数器）执行的逻辑功能（开/关）。可编程逻辑控制器已经发展成为具有控制复杂过程能力的自动化控制器，被大量用于监控与数据采集 (SCADA) 系统和分布式控制系统 (DCS)。PLC 也用作较小系统组态中的主控制器。PLC 广泛用于几乎所有的工业过程。

可靠性：系统在规定的条件下在规定的时间段内执行所需功能的能力。

控制网络：时间关键型网络，通常接入控制物理过程的设备。控制网络可以细分为多个区域，单个企业或工厂内可有多个单独的控制网络。

控制中心：参见过程控制室。

勒索软件：一种恶意软件，它会禁止操作或阻止对数据的访问，直到业主或运营商答应付款要求。

历史数据服务器（数据记录器）：工控系统的历史数据服务器是一个专门的软件系统，可从工业设备和系统中收集点值、警报事件、批次记录和其它信息，并将它们存储于专门构建的数据库中，即可使用统计过程控制技术进行数据分析的集中式数据库。

流氓设备：流氓设备是指无权访问和操作网络的未经授权的设备。此类设备可能具有恶意性质，且可被用于绕过安全保护。

漏洞：系统设计、组建或操作和管理中的缺陷或弱点，可能被利用来破坏系统的完整性或其安全策略。

路由器：位于开放系统互联 (OSI) 第 3 层的两个网络之间的网关，用于传递和引导跨网络的数据包。最常见形式的路由器运行的是互联网协议 (IP) 数据包。

默认密码：系统首次交付或安装时提供的标准密码。用户一定要立即更改默认密码。

内部威胁：来自组织内的威胁（恶意或无意），例如心怀不满的员工、前雇员、承包商和业务伙伴，他们掌握有关组织安全实践、数据和计算机系统的内部信息。

企业资源计划 (ERP) 系统：商业环境中使用的软件。例如 SAP 和 Oracle/PeopleSoft，它们主要涉及生产订单流程、仓储和已完成订单的运输信息条目。

权限凭证：最低限度是指用户名和密码，但也可以是物理或人体生物特征，例如指纹。凭证用于在用户登录工控系统时对其进行身份验证。访问权限可与用户的凭证相关联。某用户的凭证可能只授予其对操作员站的访问权限，而其他用户则可能有更高级别的权限如访问工程师站的权限。

人机界面（HMI）：

1. 用于操作员与控制器互动的硬件或软件。HMI 设备既包括有按钮和指示灯的物理控制面板，也包括有运行专用 HMI 软件的彩色图形显示器的工业 PC。
2. 操作人员可通过这些软件和硬件来监控受控过程的状态、修改控制设置以更改控制目标，并在紧急情况下手动覆盖自动控制操作。工程 HMI 允许控制工程师或操作员在控制器中配置设定点或控制算法和参数。HMI 还向操作员、管理员、经理、业务合作伙伴和其它授权用户显示过程状态信息、历史信息、报告和其它信息。操作员和工程师使用 HMI 向现场设备发送命令。

入侵侦测系统：一种安全服务，用于监视和分析网络或系统事件，对以未经授权的方式访问系统资源进行侦测并提供实时或接近实时的告警。入侵检测系统可以侦测和告警，但不会阻止或拒绝不良流量。

输入/输出 (I/O) 设备：用于与计算机或控制系统通信的设备以及通信中涉及的数据的总称。

数据二极管/单向网关：请参阅下面的单向数据二极管。

完整性：指某个系统的品质，反映其操作系统的逻辑正确性和可靠性，实现保护机制的硬件和软件的逻辑完好性，及其数据结构和存储数据出现的一致性。

网关：一种中继机制，接入两个或多个具有相似功能但实现方式不同的计算机网络，使一个网络上的主机能够与另一个网络上的主机进行通信。

网络钓鱼：一种诱骗受害者泄露信息的网络攻击，通过伪造的电子邮件将收件人引诱到看起来与合法来源关联的网站。

威胁源起方：对影响安全的事件担负部分或全部责任的实体。威胁源起方例举如下：黑客活动分子、内部威胁、国家实体、有组织犯罪。

物理访问：人到现场操作计算机和网络硬件或网络装备的其它部分。

现场设备：接入工控系统现场侧的设备。现场设备的类型包括远程终端测控单元 (RTU)、可编程逻辑控制器 (PLC)、执行器、传感器、人机界面 (HMI) 和相关通信。

协议：协议是指共享数据的两个组件用来理解共享数据的一套规则系统。协议不是“语言”，但可以更恰当地描述其为用于交流某语言的语法和句法。在工控系统的世界，这些协议中有许多是供应商独有的，是为功能和可靠性而非安全性而设计，并且通常以明文（未加密）传输。这强调了将 OT 环境与 IT 分开的必要。工业中常见的 ICS 协议的一些示例：Modbus RTU、Modbus TCP、Profibus、Profinet、DNP3 和 ControlNet。在 IT 端，基于 TCP/IP（如 FTP、DNS、HTTP、HTTPS）的协议很常见。

信息技术网络（IT）：通常指用于开展业务的网络，使用计算机来创建、操作、存储、检索和传输数据。

虚拟专用网络 (VPN)：公共网络（通常指因特网）与专用网络之间的安全连接。

验证：对某种断言进行证实的行为，例如计算机系统用户的身份。与识别（使某人或某物的身份显露）相比，身份验证是验证该身份的过程。一种典型的身份验证方式是用户提供的用于登录的密码。

硬化：一种安全措施，包括取消或禁用不必要的特性、功能、端口和服务，以及应用网路安全控制以防非授权使用。有两种类型的硬化：

1. 物理硬化：通过物理手段来禁用；取消不需要的通信端口，阻止对端口和驱动器的访问等。
2. 逻辑硬化：禁用未使用的网络和通信协议、未使用外围设备的驱动程序、Web 服务器等；然后再应用网路安全控制，例如对更新固件和加载程序启用密码保护、启用日志和告警、启用防病毒或设备附带的白名单等安全技术。

用户信息库：存储特定网域内用户/成员相关信息的系统，目的是确保集中地进行身份验证和授权。微软活动目录即 Microsoft Active Directory 是 IT 和 OT 网络中常见的用户信息库的常见示例。

远程访问：指用户（或信息系统）从外部与信息系统的安全外围进行通信的访问。（来源：NIST SP 800-53）自不同的地理位置来对安全区边界内的系统进行使用，且该使用权限与本人到场时的权限相同。远程访问中使用的设备示例：

1. 用于调制和解调数据的调制解调器。本质上是将来自网络外部的模拟电信号转换为数字 1 和 0，再由路由器处理，反之亦然。
2. 路由器位于调制解调器的下游。它们使用公共 IP 地址接入广域网或因特网。它们引导网络数据，同时对数据进行优先排序并为每次传输选择最佳路径。
3. 远程访问服务器提供管理来自 LAN 外部的远程连接的服务。通常称为跳转服务器/主机。

远程访问服务器：一种服务器，提供对来自 LAN 外部的远程连接进行管理的服务。通常称为跳转服务器。

远程终端测控单元（RTU）：设计用于支持分布式控制系统 (DCS) 和监控与数据采集 (SCADA) 远程站的设备。RTU 属于现场设备，用于监控参数及利用远程通信功能与监控控制器通信，它们包括调制解调器、蜂窝设备、无线电接口或任何大范围通信技术。有时 PLC 也作为 RTU 现场设备使用；在这种情况下，该 PLC 通常也被称为 RTU。它们通常安装在不易接电的地方，可使用太阳能供电。

允许名单：特定实体的列表，例如主机或应用程序，这些实体已知是良性的并被核准在组织和/或信息系统中使用。例如：仅允许在某主机上运行某些应用程序和服务，作为其硬化的一部分。

运营技术网络（OT）：OT 一词通常与工业控制系统 (ICS) 或过程控制网络 (PCN) 互换使用。该术语旨在区分企业的信息技术网络 (IT) 和控制运营资产的网络 (OT)。工业控制系统包括用于监视和控制物理过程的各种控制器和仪器，而 OT 包括管理工业运营的计算系统和基础设施（包括 ICS）。

战争拨号（拨号攻击）：战争拨号器是一种计算机程序，用于识别可成功地与计算机调制解调器建立连接的电话号码。该程序会自动拨打限定范围的电话号码并记录下来，并将成功接入调制解调器的号码输入数据库。一些程序还可识别计算机中运行的特定操作系统，并能自动进行渗透测试。在这种情况下，战争拨号器会按预先确定的常用用户名和密码表来尝试访问系统。

制造执行系统（MES）：指计算机化的系统和软件，用于生产和制造环境跟踪库存和其它生产信息，类似于企业资源计划软件，但更专注于制造过程（例如，跟踪和记录原材料到成品的转换）。

智能电子设备（IED）：任何包含一个或多个处理器、可从外部源接收数据/指令或向外部源发送数据/指令的设备（例如电子多功能仪表、数字继电器、控制器）。

资产：由组织拥有或受其监管的物理或逻辑对象，其对组织具有感知的或实际的价值。

纵深防御：使多个安全控制叠加以保护信息技术或运营技术环境的做法。

组态管理（CM）：用于控制对硬件、固件、软件和文档的修改的策略和程序，以确保信息系统在系统组建之前、期间和之后受到保护，防止被篡改。

附录 B 文件修订记录

本附录旨在记录每次发布时对文件所做的更改。应注意，章节编号特指所示日期发布的版本中的章节编号（各版本的章节编号并不总是相同）。

2024年1月，中期修订。作少许编辑修改。

2023 年 7 月。中期修订。本文有以下重大修改：

A. 改进并说明了有关消防的建议。

1. 改进了场所消防和设备消防的指南意见。

B. 更新了有关 ICS 安全的建议。

1. 提供了有关连接远程 SCADA 控制中心的指导。

C. 在附录 A 术语表中添加了术语。

2023 年 1 月。中期修订。进行了以下修改：

A. 阐明了消防建议。

B. 阐明了 ICS 管理建议。

C. 阐明并修改了 ICS 安全方面的建议，包括：

1. 修改了有关 ICS 和 OT 网络设备（包括安全系统）的组态配置和系统监控的建议。

2. 阐明了补丁管理建议。

3. 阐明了有关网络保护的建议。

D. 澄清并修改 ICS 运行/操作的建议，包括：

1. 阐明了报警管理建议。

2. 修改了的事故恢复计划——特别是可接受的备份文件的类型。

E. 在附录 A 术语表中添加了术语。

2022 年 7 月。中期修订。少许编辑修改。

2021 年 10 月。中期修订。更新了对电池测试的要求（2.7 节）。

2021 年 7 月。中期修订。更新并澄清了以下内容：

A. 工控系统的安全

i. 访问管理
ii. 组态管理
iii. 补丁管理
iv. 网络保障

B. 工控系统的运行

i. 紧急操作程序

C. 建筑和消防建议。

2020 年 7 月。中期修订。更新了有关应急计划和备件的指南。

2019 年 10 月这是本文件的第一版。