UITP ADVANCING PUBLIC TRANSPORT

报告

中小型公共交通运营商的网络安全

2024 年 | 2 月

目录

术语表

AD	活动目录
AI/ML	人工智能/机器学习
AV	反病毒
ANSSI	Agence Nationale de la Sécurité des Systèmes d’ Information 法国国家信息系统安全局
API	应用程序编程接口
BIA	业务影响分析
BCP	业务连续性计划
CAF	网络评估框架
CISO	首席信息安全官
CMDB	配置管理数据库
DCS	分布式控制系统
DiD	纵深防御
DMZ	隔离区
DoS	拒绝服务
DDoS	分布式拒绝服务
DR	灾难恢复
DRP	灾难恢复计划
EBIOS RM	EBIOS 风险管理
EDR	终端检测与响应
ENISA	欧盟网络安全局
FAIR	信息风险因素分析
FBOM	固件物料清单
FAT	出厂验收测试
FIVP	工厂集成与确认平台
HBOM	硬件物料清单
HMI	人机界面
HIDS	基于主机的入侵检测系统
IACS	工业自动化与控制系统
IAM	身份和访问管理
ICS	工业控制系统
IDS	入侵检测系统
IPS	入侵防御系统

IS	信息系统
ISMS	信息安全管理体系
IT	信息技术
LDAP	轻量目录访问协议
LPM	Loi de Programmation Militaire — 法国军事规划法
MFA	多因素鉴别
NIDS	网络 IDS
NIS	网络与信息系统
NIST	美国国家标准与技术研究院
NIST CSF	NIST 网络安全框架
OIDC	OpenID Connect
OS	操作系统
OT	运营技术
PAM	特权访问管理
PCN	过程控制网络
PIA	隐私影响评估
PII	个人身份信息
PLC	可编程逻辑控制器
PTO	公共交通运营商
RBAC	基于角色的访问控制
RDoS	勒索拒绝服务
SAT	现场验收测试
SBOM	软件物料清单
SIEM	安全事故与事件管理
SOAR	安全编排、自动化与响应
SSO	单点登录
VLAN	虚拟局域网
UBA	用户行为分析
UEBA	用户与实体行为分析
UITP	Union Internationale des Transports Publics（国际公共交通联会）
WSUS	Windows Server 更新服务

公共交通运营商的网络安全问题有哪些?

UITP 指出：**“网络安全对公共交通部门至关重要。运输系统通常涉及大量敏感数据，包括乘客和员工的个人信息。这会使运输系统成为网络攻击目标。运输系统也是至关重要的基础设施，而网络攻击造成的中断可能会对服务的安全性和可靠性产生严重后果。**

与此同时，在公共交通中越来越多地使用自动化系统和智能支付系统等技术，也增加了潜在的网络攻击漏洞。确保相应系统的安全对于公共交通部门的持续成功和发展至关重要。” [1]

根据欧盟网络安全局 (ENISA) 发布的《交通部门威胁报告》[2]，主要威胁包括：

- 勒索软件攻击；
- 数据相关威胁；
- 恶意软件；
- 拒绝服务 (DoS)、分布式拒绝服务 (DDoS) 和勒索拒绝服务 (RDoS) 攻击；
- 网络钓鱼/鱼叉式网络钓鱼；以及
- 供应链攻击。

由于可轻松获取基于 IT 的 OT 系统黑客工具，加之威胁行为体（包括网络犯罪分子和得到民族国家支持的组织）形势复杂，相应威胁正在增加。**无论规模大小，各 PTO 宜采取适当而适度的措施，保护其资产和服务免受网络攻击。**

报告目的

本文件为中小型公共交通运营商 (PTO) 提供了关于网络安全良好实践的易用性指导，可帮助其应对适用于其环境的威胁，并协助作为基本服务运营商的他们采取“适当且适度的技术和组织措施，以便管理对其网络和信息系统安全构成影响的风险”（《2018 年网络与信息系统 (NIS) 条例》）。

为满足这一要求，我们鼓励各 PTO 对其组织内的现行实践加以反思，并制定战略和路线图，以便提高其技术和组织安全专业知识水平，并随着时间的推移采取有效措施保护自己。

[1] https://www.uitp.org/topics/cybersecurity-in-public-transport/
[2] https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

报告受众

本文件面向试图对网络安全建立基本了解的 PTO 员工。无需先验知识即可阅读本文件。

报告结构

本文件介绍了在 PTO 内实施网络安全良好实践的情况，并指出了适用标准和法规。

它强调了信息技术 (IT) 与运营技术 (OT) 之间的差异，及其在普渡企业参考架构[3]（或普渡模型）下的划分情况，有助于读者理解两个关键点：

1. 铁路联锁或乘客信息系统等 OT 系统通常包含易受常见黑客工具攻击的 IT 要素，但仍需遵守 OT 系统管理要求；以及
2. 对于 IT 和 OT 系统而言，安全管理原则的实施可能大相径庭。

本文件符合欧洲议会和欧盟理事会 2016 年 7 月 6 日关于网络与信息系统高通用安全水平措施的《第 2016/1148 号 (EU) 指令》，并反映了《NCSC 网络评估框架 (CAF)》[4]中描述的安全目标、原则和良好实践指标。

本文件提出了四项网络安全目标：

A. 管理安全风险

B. 防范网络攻击

C. 检测网络安全事件

D. 将网络安全事故影响降至最低

会有单独章节对各项目标进行介绍，并辅以一套网络安全原则进行说明。为了说明如何在 IT 和 OT 背景下应用相应原则，我们采用了密码学领域的“Alice 和 Bob”[5]。在我们的案例中，Alice 是一名 OT 安全经理，而 Bob 则是一名 IT 安全经理，他们分别负责在普渡模型中分配到的级别，并在确保环境安全方面面临着巨大挑战。

[3] https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
[4] 《NCSC CAF 指南》 - NCSC.GOV.UK
[5] https://en.wikipedia.org/wiki/Alice_and_Bob

为了便于说明，用户故事描述的是 Alice 和 Bob 单独工作的情况。在现实中，双方宜共同合作，提供符合当地需求和具有成本效益的整体安全解决方案。

我们会借助附录中的一组 Alice 和 Bob 用户故事，对目标 B、C 和 D 加以说明。

报告内容还包括：

- 其他阅读材料和资源的链接，会以图形符号标出 
- 提示和具体建议，会以图形符号高亮显示 

网络安全导论

什么是网络安全?

可将网络安全定义为**“信息系统的理想状态。在该状态下，信息系统能够抵御来自网络空间的事件。相应事件可能会损害所存储、处理或传输数据以及相应系统所提供或可访问相关服务的可用性、完整性或保密性。网络安全要求采用信息系统安全技术，并以打击网络犯罪和建立网络防御为基础”**。[6]

信息技术 (IT) 和运营技术 (OT) 有何区别?

“**信息技术 (IT)** 是指侧重于数据存储、恢复、传输、操作和保护的硬件、软件和通信技术。

运营技术 (OT) 是指通过直接监控和控制物理设备、过程和事件来检测或引起变化的硬件和软件。”[7]

IT 系统的示例包括企业资源规划 (ERP) 系统，它是帮助整个企业运行的软件系统。OT 系统的示例包括 SCADA 或信号系统。

每组技术均要在特定背景下运行，在应用安全原则时宜以该背景为依据。适用于 IT 环境的安全措施可能不是 OT 背景下最有效或最合适的控制措施，因此可能需要使用其他（补偿性）控制措施。例如，IT 资产可能每周都会打补丁，但在关注资产可用性和经证实安全行为而非所存储数据保密性的 OT 背景下，这种停机可能难以实现。

什么是 ICS 安全的普渡模型?

“普渡企业参考架构 (PERA) 是**工业控制系统 (ICS) 安全的结构模型，涉及物理过程、传感器、监督控制、操作和物流的分割。**长期以来，ICS 网络分割一直被视为保护运营技术 (OT) 免受恶意软件和其他攻击的关键框架。如图 1 所示，该框架仍可使用。然而，这种方法并没有真正考虑到安全系统（如传信系统），因此也可以考虑基于以下宏观分割的方法：

---

6 https://www.ssi.gouv.fr/entreprise/glossaire/c/#:~:text=La%20cybers%C3%A9curit%C3%A9%20fait%20appel%20%C3%A0,en%20place%20d'une%20cyberd%C3%A9fense

7 https://blog.isa.org/what-is-the-difference-between-it-and-ot-security

- 传信控制网络 (SCN)，对安全性至关重要（OT 环境）
- 运行控制网络 (OCN)，对可靠性至关重要（OT 环境）
- 行政控制网络 (ACN)，面向业务（IT 环境）
- DMZ 和互联网接入，即从 PTO 到互联网应用程序的连接

此外，根据这种方法，任何第三方网络均应被视为“敌手”。

普渡模型展示了 ICS 架构典型元素的互连方式，并将其划分为包含 IT 和 OT 系统的独立区域。如果实施得当，该模型有助于在 ICS/OT 和 IT 系统之间建立“气隙”，将相应系统隔离开来，以便组织能够在不妨碍业务开展的情况下实施有效的访问控制。”[8]

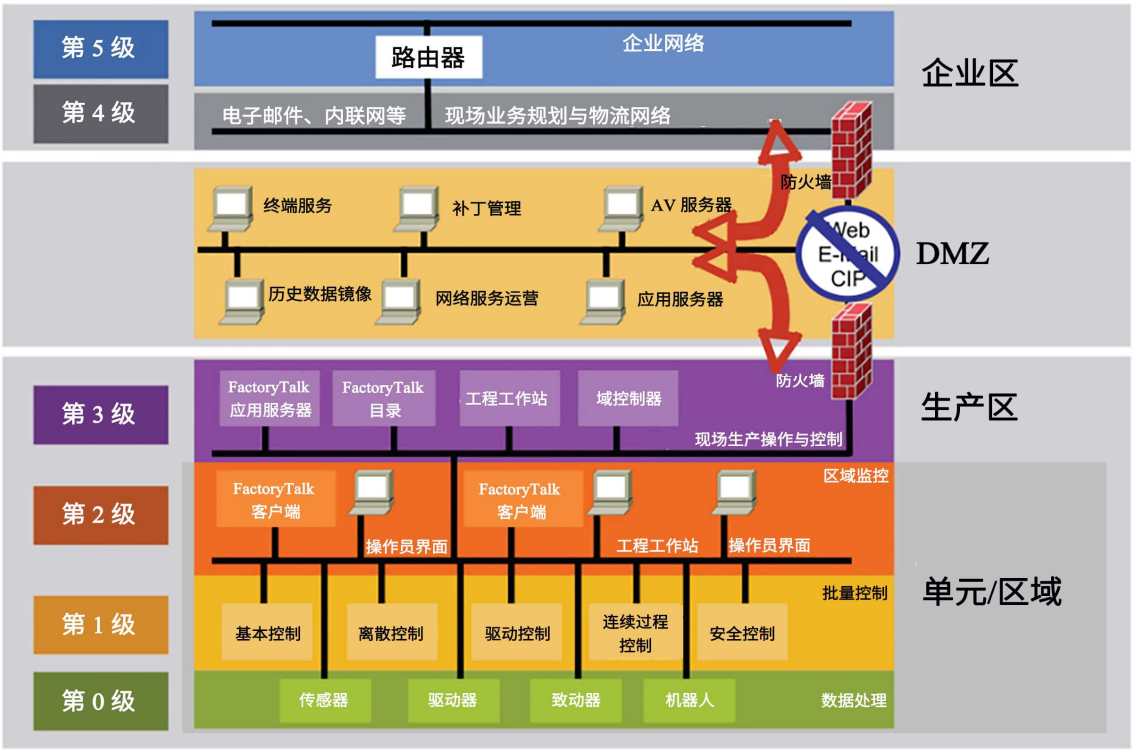

图 1:普渡企业参考架构（来自罗克韦尔自动化）

企业区

企业区（第 4 和 5 级）是指工业设施中的 IT 网络。对于位于该网络层的所有资产，宜遵循 IT 安全和运行补丁策略，包括定期更新和升级。与工业生产活动相比，这一层专门用于办公操作。它可以与上述 ACN 区相对应。

[8] https://www.zscaler.fr/resources/security-terms-glossary/what-is-purdue-model-ics-security

过程控制网络的 DMZ

DMZ（位于第 3 层和第 4 层之间）由安全保护措施划定，如果设计得当，可在企业区和工业区之间产生“气隙”。此类保护措施宜由 IT 部门管理，并遵循严格策略，即哪些流量可以流出或流入过程控制网络 (PCN)。DMZ 也可位于企业网络外围，以便有效隔离第三方网络或互联网。

应该注意的是，许多公司仍希望将数据从过程控制网络共享到其他业务领域（ACN、第三方网络、互联网）。因此，在使用防火墙等可能被黑客攻击的双向软件保护措施时，不可能存在完美 DMZ 气隙。在这种情况下，对于许多行业（包括铁路行业），建议使用由数据二极管强制执行的单向数据流，确保 IT 流量无法流入 OT 网络。

过程控制网络

过程控制网络（包括第 0 至 3 层）由生产区和单元/区域区组成。它包含工业厂房中的 PLC、DCS 和 HMI 等 OT 资产，并受 OT 管理实践约束。如前所述，在 PTO 环境中，可以找到其他类型的设备，例如基于计算机的联锁装置、ATC 系统、站台屏蔽门、PIS、门禁控制等，相应设备不一定由 PLC 驱动。在较大型 PTO 环境（如地铁）中，术语“过程控制”不太合适，使用术语“SCN”和“OCN”可能更合适。

位于 PCN 层中的系统可能与安全相关，通常需要保证较高可用性，几乎不允许中断。必须预测任何影响流程可用性或安全状态的安全管理活动。预测工作通常要提前很久进行，且需要采取能反映受影响资产特殊需求的方法。此外，任何版本更新宜谨慎进行，最好在现有测试台上进行预先测试。

相关的网络安全规范和法规有哪些?

适用法律法规应由法律部门列出并定期审查。此外，法律部门宜在网络安全团队的协助下，评估相应法律法规对 IT 和 OT 安全的影响。

与网络安全相关的规范和法规包括：

ISO 27001	《信息安全管理体系 (ISMS) 标准》
ISO 27005	《信息安全风险管理指南》
IEC 62443	确定了实施和维护电子安全工业自动化与控制系统 (IACS) 的要求和流程的系列标准
(EU) 2016/1148	《网络与信息系统指令》，旨在协调和加强欧洲市场网络安全。现在被 NIS2（第 2022/2555 号 (EU) 指令）取代。该指令旨在“加强安全要求、解决供应链安全问题、简化报告义务，并引入更严格的监管措施和执法要求，包括在整个欧盟范围内统一制裁”。
CLC/TS 50701	技术规范，介绍了解决铁路部门网络安全问题的要求和建议。TS 50701 已提交至 IEC，经批准成为国际标准，目前正作为编制 IEC 63452 的参考资料。
EN 50129:2018	《铁路应用（与安全相关的传信电子系统）安全标准》，要求对可合理预见 IT 安全威胁（无法通过简单论据排除）的影响进行处理，并在安全案例中进行引用。

目标 A：管理安全风险

管理安全风险主要涉及识别和缓解风险，以此避免与网络事故相关的安全、监管、财务和声誉损害，同时保持运营连续性。

治理是风险管理的基石。它要求我们指定高级责任人；确定安全政策、角色和职责；定期进行风险分析；实施安全措施，防止威胁行为体利用可能影响系统安全的漏洞。

作为 PTO，您需要详细了解您所拥有的资产（“您无法保护您不知道的资产”），包括对配套基础设施（如电力）和外部供应商（第三方供应链）的任何依赖关系。

治理

“网络安全治理是一项全面网络安全战略，与组织运营相结合，可防止活动因网络威胁或攻击而中断。网络安全治理的特点包括：

- 问责制框架
- 决策层级
- 与业务目标相关的已界定风险
- 缓解计划和策略
- 监督流程和程序”。[9]

为了实现成功治理，宜在董事会层级建立问责制；制定一套明确的保护政策，以便解决技术、行政和物理方面的网络安全问题；并根据上报流程，确定并分配角色和职责。

此类政策的示例如下：

技术政策：围绕网络分割、反病毒和密码管理的规则。

行政政策：可接受的使用政策，包括个人对系统（包括互联网）的使用；对“超级用户”帐户的控制；以及入职、调动和离职流程，以便确保用户在离开某个岗位或公司后无法保留访问权限。

[9] https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance#:~:text=Cybersecurity%20governance%20is%20a%20comprehensive,Decision%2Dmaking%20hierarchies

物理政策：对钥匙的控制；安保人员；禁止“尾随”通过安全屏障。

路标：小型企业的安全控制措施类型 - SecurityMadeSimple.org

路标：CIS 关键安全控制措施

建议建立 ISO 27001 标准中确定的信息安全管理体系（ISMS），该体系宜在“计划-执行-检查-处理 (PDCA)”循环内不断改进。

风险管理

安全风险评估是识别和确定组织所面临安全风险规模的关键，有助于适当安排风险管理活动的优先次序。

在投标或项目阶段，可对 IT 和 OT 基础设施进行不同粒度（从产品到系统）的风险评估。

通常情况下，您会想解与考虑中系统 (SuC) 相关的安全威胁，以及目前存在的或保护系统需要解决的任何安全障碍。随着时间的推移，相应威胁和障碍可能会发生变化。良好实践表明，宜定期更新风险评估，使其保持相关性。如欲了解有关威胁的信息，请访问与您所在行业相关的威胁情报源。

相应威胁可能试图利用人员、流程和技术中的漏洞（可能由您或第三方供应商的员工引入），这就是为什么必须系统解决网络安全问题，而非仅仅关注技术要素。

宜通过风险评估流程得出一套明确安全要求，并根据适用 IT 或 OT 网络安全政策加以实施。

在即将发布的《风险评估报告》（计划于 2024 年初发布）中，UITP 建议采用两种不同的方法进行风险评估和管理，其主要依据是网络攻击得逞会给组织造成损失的估计值：

对于估计影响金额少于 150 万美元的组织（小型 A 类组织），UITP 建议使用简化跟踪内容[10]，其中包括简单快捷的流程，即对防御目标进行映射，并针对为该类组织裁剪得出的少量问题给出答复。

[10] 基于以色列国家网络局网络防御条令：《组织网络防御全面应用指南》，2021 年 6 月

对于价值超过 150 万美元阈值的组织（大中型 B 类组织），跟踪内容包括网络安全风险评估流程、差距分析，以及缓解风险的工作计划。

下文概述了针对各类跟踪内容可采取的方法；有关全面详细的说明，请参阅预计于 2024 年初发布的单独报告。

A 类组织

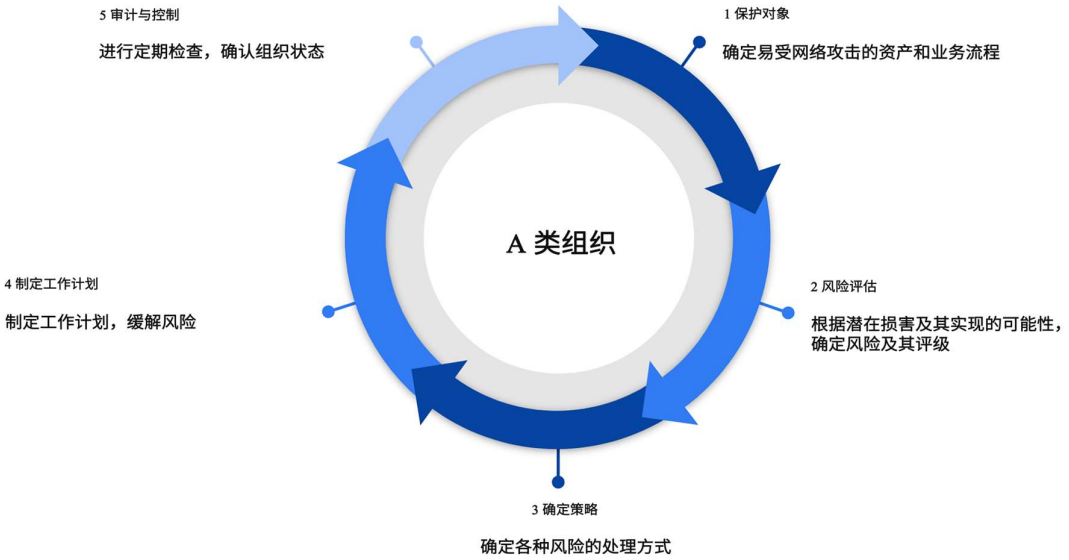

图 *2* - A 类风险评估流程

B 类组织

对于 B 类组织，确定了三种不同用例，并制定了风险评估流程，有助于进行用例确定：

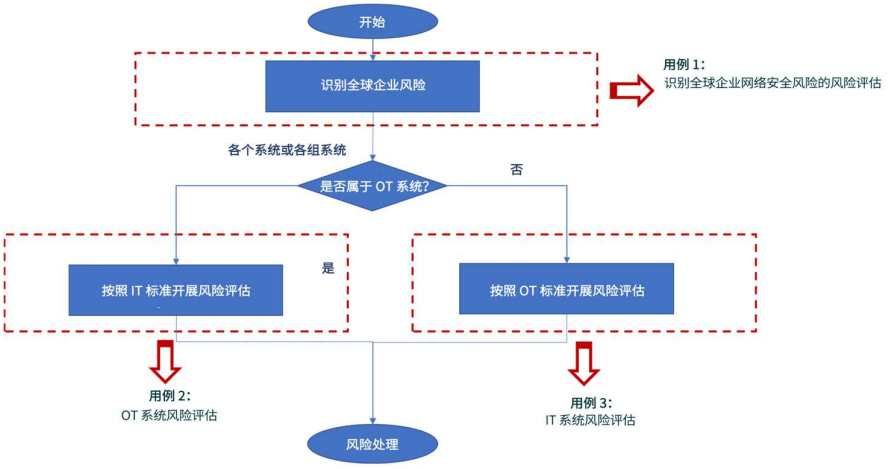

图 *3* - B 类用例确定

资产管理

将网络安全纳入资产管理，您需要：

1. 了解交付和维护贵组织设备和固件所需的一切；以及
2. 从网络安全的角度对其进行管理，直至其安全停用和退役。

资产登记册的详细程度需要足以支持网络安全管理活动，并可能受当地法规指示。例如，如果希望通过搜索资产登记册来确定整个组织内的过时或脆弱资产，那就需要跟踪详细版本信息。相应信息可以与在公共漏洞和暴露 (CVE) 系统 [11] 中发布的忠告性漏洞通知等相匹配。

需要对清单进行维护，以便保持其准确性。根据良好实践，建议为各项资产确定负责人和位置。

在确定要列入登记册的资产时，宜考虑服务器、工作站、平板电脑、交换机、防火墙、PLC、路由器等，并考虑为各项资产保存以下信息：

- 全局信息：设备名称、描述和业务功能、品牌、型号、MAC 地址、支持性合同参考，以及设备拥有者和位置
- 网络信息：主机名、IP 地址、VLAN

11 公共漏洞和暴露 - 维基百科

- 系统信息：操作系统/固件版本
- 应用程序信息：已安装应用程序及其版本列表

宜根据变更情况维护清单。自动化资产检测工具可在这方面提供帮助。在 IT 背景下，配置管理数据库 (CMDB) 可用于强制执行计算环境重要组件的允许配置。

资产通常包含数据、配置信息或安全凭证（如密码）。相应信息可帮助攻击者或导致未经授权的信息披露。

当相应设备被重新分配、送往第三方维修或在寿命结束时退出生产时，必须安全删除相应信息。在某些情况下，如存储 PII 的硬盘或备份磁带，您可以选择物理销毁而非删除。

供应链

贵组织会依赖于外部供应商和合作伙伴，他们及他们的分包商和供应链很可能会带来安全风险。供应链攻击越来越常见，攻击者利用建立在信任基础上的关系、软件更新和已连接网络作为攻击载体。此外，与合作伙伴共享的特权信息可能会在该合作伙伴本身就是攻击（如勒索软件）受害者的情况下暴露。

根据良好实践，建议使用风险评估来确定合同中应包含的相应安全义务，并仔细考虑 SuC 的任何数据共享范围。宜通过采购流程获得 SuC 的硬件 (HBOM)、软件 (SBOM) 和固件 (FBOM) 清单。上述清单将支持您的资产管理和漏洞管理需求，并在出现问题时派上用场。

对于关键供应链合作伙伴，您可以考虑创建共享事故管理流程，明确需要相互提供支持的职责。

与资产管理类似，确定第三方清单也很有价值。该清单详细说明了合作伙伴关系的范围和程度，包括共享的信息、网络和应用程序访问权、合作伙伴的关键性和网络安全成熟度。第三方的网络安全成熟度各不相同，不妨考虑索要其持有的任何网络认证（如 62443-2-2）副本、检查认证范围，并要求其填写网络安全问卷，或提供其维护的任何安全记分卡的详细信息。还要考虑通过审计流程证实其安全声明的真实性。

路标：网络安全实用指南：招标要求 (UITP)

目标 B：防范网络攻击

防范网络攻击，需要我们在以下领域实施安全控制措施，以此降低风险敞口水平：

- 物理安全
- 系统安全
- 网络安全架构
- 数据安全
- 身份与访问控制
- 员工宣传与培训

物理安全

根据“**纵深防御**”方法，宜在考虑物理安全因素的情况下考虑网络安全，为系统增加额外的保护层 — 在这种方法中，失去单层保护确实会使资产失去保护。常规物理安全控制措施有时被称为“枪支、大门和警卫”，通常要求：

- 用户进入现场后，会受徽章和安全区域保护，且现场会根据区域或位置的敏感性实施安全控制措施，例如在某些区域不得携带电子产品。
- 存放敏感 IT 设备的场所/房间均配有徽章保护措施（仅授权人员可进入），记录并定期审查进入情况。
- 全天候对敏感位置进行视频监控。
- 安装探测和保护系统（火灾/烟雾和水探测/保护、入侵探测等），并定期检查。
- 来访者均有明确身份标识，并有专人陪同。
- 定期审计物理安全控制措施。
- 对移动车载资产使用安全钥匙，以便保护驾驶室和其他敏感区域，如 Kaba 锁/钥匙。

要成功实施、运行和维护物理安全要求，可能需要设施管理团队的支持。

路标：英国国家安全保护局：NPSA

系统安全

系统安全性取决于许多因素，尽管有机会影响其中某些领域，但并非所有因素都在我们的掌控之下。

理性情况下，所有系统均遵循“**安全设计**”原则。实际上，许多 IT 和 OT 系统组件并不如此。作为 PTO，不妨通过适当的安全风险管理方法（如针对 OT 的 IEC-62443-3-2 及其安全区域和管道概念），探索在遗留实施方案或新采购设备中部署额外安全控制措施的机会，以此确保根据风险评估确定的关键性，为资产分配适当安全控制措施，并确保没有任何一个漏洞会导致系统漏洞或其他令人担忧的结果。此类模型还有助于建立监控点，用于支持检测控制措施（目标 C）。

加固（或**安全配置**）是一系列实践，旨在缩小系统攻击面，使攻击者更难破坏系统。通常情况下，该过程始于已定义的基线构建，删除了不必要的用户、应用软件和服务，如游戏和自动运行功能。然后，访问控制可确保仅有授权用户才能安装软件或更改与安全相关的配置。在适当的情况下，主机基线宜包括终端检测与响应 (EDR[12]) 软件（定期更新），以便识别和消除病毒和勒索软件。

然后，相应配置必须由授权用户仔细进行变更管理，并定期检查，以便确保保护性防御措施仍然有效，且不会因应用补丁（尤其是功能包或系列包）而被移除或降级。宜妥善保管与配置相关的文件，并根据配置予以维护。

可从互联网安全中心获取有关安全配置的详细指南，该中心为许多软件产品提供了配置指南。然后，某些网络安全评估工具可根据相应行业基准提供合规报告。

路标：CIS 基准：CIS 互联网安全中心

路标：NIST SP 800-128《信息系统安全配置管理指南》

攻击者可以利用未加管理的**漏洞**来破坏系统安全。随着时间的推移，往往能在 IT 和 OT 固件、软件和硬件中发现新漏洞，因此从安全角度来看，最好使用供应商仍然支持的技术。

鉴于许多商业操作系统的生命周期较短，而其所支持的 OT 系统的生命周期较长，因此在 OT 环境中越来越多地使用 COTS 技术时，需要特别注意使用报废策略。

[12] 终端检测与响应 - 维基百科

路标：UITP 报告：《运行环境和网络安全方面的报废问题》

宜定期识别和评估组织内的漏洞，以便能优先考虑并缓解相应漏洞带来的风险，如通过打补丁等方式。根据具体情况，有多种方法来识别漏洞。可以考虑采用被动或主动自动扫描、入侵检测系统、持续监控系统、内部或外部安全评估团队，或将供应商提供的漏洞警报订阅与 SIEM[13] 中的详细资产登记册相结合。

在某些情况下，您可能会发现打安全补丁并不可行：这可能是因为定制系统或遗留系统尚无补丁可用，或永远不会有补丁。在其他情况下，宜通过补丁管理流程确保从授权来源（如供应商网站）获取补丁、评估补丁对运行的影响、根据关键性确定优先级（根据通用漏洞评分系统[14]，各个漏洞均有一个关键性分数），并及时应用。在部署前，宜在目标环境的数字孪生环境中测试补丁，宜采取措施使补丁能够“回退”和/或将系统回滚到已知良好状态。

宜将任何补丁的应用情况反映在资产登记册或 CMDB 中。

某些环境的自动补丁管理工具也会报告部署状态和失败补丁，如 Windows 的 WSUS。Linux 环境中也有相应工具。

路标：NIST 国家漏洞数据库 NVD

网络安全架构

保护网络包括对交换机、路由器等网络设备应用安全配置（如上文所述），也包括使用其他安全控制措施来分割和隔离相应网络。“分割”和“隔离”这两个术语经常被混淆。

网络**分割**：将大型网络划分为较小网络。

网络**隔离**：控制网络设备和服务之间的通信。

传统上，网络分割和隔离通常通过面向互联网的边界防火墙来实现，或者通过一对防火墙和一个隔离区（如普渡模型所示）来实现可信区和非可信区之间的隔离。该模型有两个主要弱点：将整个网络划分为可信区域后，攻击者便能在该区域内自由行动，在机器之间穿梭。这种“扁

13 安全信息与事件管理 - 维基百科
14 公共漏洞评分系统 - 维基百科

平化”网络拓扑结构无法应对当今网络威胁，如鱼叉式网络钓鱼。此外，在大型网络中，通过防火墙过滤规则隔离通信很快就会变得复杂，造成潜在实施错误，从而被攻击者利用。

良好实践要求我们在不影响组织效率的情况下，限制对敏感资产的访问（遵循**最小特权**和**应需可知**原则）。在这一专业领域，需要对资产有充分了解，认真规划并实施现有安全控制措施，如：

- 使用带访问控制列表的路由器或第 3 层交换机和数据二极管对网络进行分割，以便强制执行单向数据流，并确保免受来自较不安全区域的攻击；
- 使用网络访问控制、网络防火墙和基于主机的安全解决方案（如 EDR）过滤网络流量；
- 使用虚拟化技术，将局域网分割为 VLAN，并将具有不同“信任”级别的应用程序隔离到不同的虚拟机中；
- 部署多因素鉴别，强化标准用户名/密码对；
- 确保访客访问使用专用 Wi-Fi 网络，并与企业 IT 和 OT 网络分离；以及
- 制定远程访问策略，列出所有远程访问用例和相关解决方案，以及经批准的第三方连接登记册。

目标 C 将检查监控和检测控制措施的使用情况，为网络安全提供支持，并在网络隔离等其他措施缺失或实施不力时发挥补偿性控制作用。

数据安全

数据以纸质和数字形式存在，每种形式均会受到一系列不同的威胁。某些数据可能对贵组织至关重要，因此必须了解相应数据的位置、去向，以及数据保密性、完整性或可用性受损后可能会对组织运营产生何种影响。同时要记住，某些数据代表了现实世界资产的配置或表示形式，如果修改不当，可能会对安全造成影响。其他数据可能看起来不那么重要，但如果被恶意方访问，可能会为攻击提供便利。

良好实践表明，宜对关键数据进行标识和编目（就像资产登记册中的软件或硬件资产一样），以便跟踪其位置、授权用户和用途，并确保其得到适当处理：

- 无论是静态数据还是传输中数据，均要防止未经授权的访问。加密技术可以在这方面提供帮助；
- 备份，以防其被破坏或不可用。备份可离线保留（或隔离），通过加密备份本身来防止勒索软件和丢失；以及

- 不再需要时，可将其存档或安全删除。

数据移动并不总是通过网络（可能会受到使用监控），也会使用介质和移动设备进行，包括 USB 驱动器。宜考虑对所有此类设备进行编目，并（就 USB 设备而言）使用加密类设备，对所保存数据进行加密，仅在正确输入密码后方可解密。除支持本地加密外，如果设备丢失或需要在停用前进行远程净化，您可以使用其他类型的移动设备远程擦除数据。

身份与访问控制

身份与访问控制关注的是“谁”（哪些用户）和“什么”（系统和设备）可以访问组织系统和数据，并要求相应用户、系统和设备通过可信机制证明其身份。

简单来说，就是用户用用户名标识自己，然后用密码鉴别该身份。一旦通过鉴别，该用户便能访问其身份已被授予访问权限（授权）的系统和资源。为了使授予资源访问权限的过程更容易于管理（和审计），使用**基于角色的访问控制** (RBAC) 有助于将系统特权授予角色，然后再将角色授予用户。当用户在组织中的岗位出现变动时，将用户的系统角色与其组织角色进行重新调整，以便根据需要授予和撤销系统权限，就会变得更加简单。良好实践建议：

- 授予访问权限应遵循最小特权原则（上文已讨论过），即每个实体仅被授予履行其职能所需的最低限度系统资源和授权；
- 宜避免使用通用帐户和共享密码；以及
- 强制执行强密码策略。

路标：NCSC 密码指南

通常情况下，有些用户对系统会有较高访问权限（特权提升）。这些“超级用户”（或**特权帐户**）经常可以做出可能影响业务的更改，如创建虚拟用户并将其添加到工资单中，或删除整个系统。建议通过额外鉴别机制（如多因素鉴别 (MFA) 或硬件支持证书）以及严格的监控和审计来保护相应帐户（和远程访问帐户）。此外，不妨考虑对此类帐户使用有时限的访问权限，或为特权活动使用专用机器和独立帐户，以此避免因访问电子邮件或浏览互联网而造成恶意软件大面积感染或鱼叉式网络钓鱼的风险。

考虑一下，如果某用户以域管理员身份登录，并拥有对所有网络资产的访问权限，那么就会引发恶意软件感染或勒索软件攻击！

在考虑身份问题时，很容易将重点放在用户身上。但我们应该记住，网络设备也有身份，攻击者在网络上放置未经授权的（流氓）设备，再借助此类设备从远程位置访问网络的情况并不罕见。因此，根据良好实践，建议定期扫描网络中的未知设备。

员工宣传与培训

诚然，人为错误往往是造成网络事故的原因之一，但将用户描述为安全链中的薄弱环节并不公平，这会使他们觉得自己成为了疯狂推销安全宣传活动的目标。然而，如果能向他们提供与其角色相关且有吸引力的网络安全宣传材料和培训渠道，他们就能成为您实现网络安全的强大合作伙伴。

建议在员工入职培训中纳入网络安全宣传内容，为员工提供与其职责相关的网络安全培训，并定期更新此类信息，将网络安全思维融入整个组织。进行内部测试是有价值的，如为财务和客户管理团队模拟首席执行官欺诈或物理入侵。但必须考虑如果实施不力可能对员工福祉造成的影响。例如，内部网络钓鱼活动向员工发送声称是奖励信的电子邮件附件。此类错误会破坏我们所需要的网络安全文化。组织及其领导层最好树立正面网络安全行为和期望榜样；感谢用户提出安全问题（就像我们对安全问题所做的那样）；并及时采取适当行动。

从商业白标网络安全宣传课程到培养网络安全意识和团队精神的非商业乐高游戏，有许多资源可供使用。

路标：决策与中断 decisions-disruptions.org

目标 C：检测网络安全事件

正如我们所看到的，监控和检测是保证主机、系统和网络设备活动安全的关键控制领域。如果没有这种能力，您将难以及时发现恶意软件、恶意电子邮件或违反策略的用户行为，更不用说遏制和减轻其影响。

要可靠而及时地检测到异常活动，就必须了解“好是什么样子”，包括适当的用户行为。在网络安全宣传培训的支持下，并辅以技术细节（如从威胁情报来源获得的恶意软件特征码、攻击方法和入侵指标 (IOC)），这种理解是实现及时且可靠潜在安全事故检测的关键。

您的 IT 和 OT 监控系统需要从设备和网络传感器中获取事件详细信息，以便准确了解活动情况。相应信息宜包括主机、网络交换机、传感器、服务器和网关的系统日志和警报，以及资产之间的通信流。可能需要对相应系统和设备的日志记录功能进行一些配置，但宜为各个系统和设备创建详细日志，记录带有时间戳的安全相关事件。宜确保日志（以及提供日志的系统）具有共同的时间源（或至少在时间上保持一致），以便有效关联并分析日志中的详细信息，从而识别恶意活动并对其进行排序。

由于日志对监控和检测非常重要，因此必须加以保护。如果不采取安全措施，攻击者可能会试图从日志中删除其活动的痕迹，包括来自任何网络 IDS 的日志。此外，日志的详细程度可能会泄露信息，（如被滥用，）可能会导致泄密或侵犯隐私。根据良好实践，建议保护日志免受修改，仅允许授权个人根据日志访问策略进行访问，并对主日志数据副本执行操作 — 确保原始数据的完整性。

通过维护和反馈（包括及时应用新的恶意软件特征码和 IOC），检测能力就能发出警报。为了使相应警报随时待命，不妨用其他数据来丰富日志记录数据，以便能够快速确定受影响资产，并在同时收到多个警报的情况下适当安排响应优先级。

通常情况下，安全警报会被发送到安全运营中心 (SOC)，监控人员会根据攻击者的战术、技术和程序 (TTP)，以及他们监控的系统和正常流量行为进行调查。建立一个训练有素、功能强大的 SOC（可能需要全天候待命）可能是一项昂贵的提议。不妨考虑将这项任务外包给 OEM、系统集成商或其他熟悉所观察系统的合格第三方。

路标：MITRE ATT&CK 敌手战术与技术框架 MITRE ATT&CK®

可根据特定威胁知识来配置监控和检测工具，为检测提供帮助。可访问美国网络安全与基础设施安全局 (CISA) 网站，免费获取此类信息和其他良好指南：

路标： 首页 | CISA

目标 D：将网络安全事故影响降至最低

网络安全事故可能相对较小，也可能迅速发展到可能造成严重影响的地步，以至于必须上报并作为危机处理。宜考虑制定事故管理流程，并辅以基于场景的事故响应计划，同时制定明确上报流程，可将事故单独上报给危机管理流程。该流程应有高级管理层参与。

计划宜确保在发生网络安全事故或危机时能继续运行（可能会降低运行水平），并宜侧重于遏制和缓解风险场景和影响（最好通过先前的网络安全风险演练确定）。计划不仅要考虑内部关系和影响，还要考虑外部关系和影响，如客户、行业合作伙伴、供应链和监管机构。根据事故性质，可能需要在规定期限内和频率内向相应机构报告。

响应计划需要涵盖整个事故或危机生命周期，并宜确定事故/危机响应小组的角色和职责，以及所需资源和状态报告协议。

许多此类计划被束之高阁，未经测试、沟通不畅且过时已久 — 包含遗留员工和系统详细信息。

计划会过时，最初可能无法很好地发挥作用 — 特性是技术性响应计划更是如此。与辅助设备不兼容的情况很常见，关键响应小组成员无法到岗的情况也并非罕见（这本身就值得测试）。计划肯定会有需要改进之处。根据良好实践，建议（针对不同场景）定期测试计划，并对其进行维护，将任何变化和经验教训纳入其中。

根据场景性质，不妨考虑网络安全事故响应专业人员或其他第三方专业支持。

如果遇到网络安全事故或危机并启动了计划，那么事后宜积极考虑开展公开而广泛的事故审查流程。该流程不会归咎于任何人，而是寻求流程改进，尽力确保从每起事故中吸取教训（无论问题发生在何处），确保了解根本原因，并采取补救措施。高级管理层宜对该流程予以支持，并需要获取所有相关数据。

附录：ALICE 和 BOB 的故事

目标 B：ALICE 和 BOB 防范网络攻击的故事

Alice

Alice 的系统不在专门建造的资料室中，而是在经过改造的资料室中。供电和制冷都是专用的，但房间没有高架地板和漏水检测装置。除此之外，房间坚固，配有坚固的物理锁，且秩序良好，配有适当类型的灭火器。只要进水风险较低，设备冷却也没有问题，Alice 就可以选择让地板保持原样。然而，由于附近没有 CCTV，门上也没有电子安全系统，这就意味着没有进入资料室的审计线索。Alice 可以考虑实施逻辑访问控制系统。该系统可对未经授权的访问采取保护和检测措施。

Alice 的资料室包含许多系统，其用户与其组织的企业 IT Windows Active Directory (AD) 实施隔离。

微软 AD 是组织用户和资源集中目录，可提供用户和设备的识别与鉴别机制，同时确保数据访问安全。Alice 的系统并未与目录集成，而是拥有自己的本地用户目录，其中一些用户设有通用用户名和密码，相应用户名和密码会在用户群中共享；有时，用户会将相应凭证粘贴在系统显示器上，便于查询。

Alice 有几种选择：她可以选择减少密码共享，增加密码复杂性和更改频率，甚至可以考虑将系统中的 Windows 要素（数据历史记录和/或工程工作站）与本地 Windows 目录集成在一起。

关键在于，Alice 将其目录（和林/域）与 Bob 管理的目录（和林/域）分离，这样她就无需在两个环境之间开辟攻击者可以利用的通道。这种分离的代价是 Alice 需要根据组织入职、调职和离职流程的变更，手动同步其目录。

Alice 的某些系统是多年前由以前的团队实施的遗留系统，使用的协议并不安全，很难单独升级。Alice 可以考虑与系统供应商联系，了解改进系统安全性的方案。例如，她可以有选择性地用更现代、更安全的替代品替换个别组件，或者计划迁移到更新的系统基线。该基线包含更安全组件、最新安全补丁，并且可以更容易地与其他安全控制措施集成。与此同时，Alice 希望找到另一种管理风险的方法（可能是通过提高网络安全性），但与应用补丁一样，任何此类实施都需要经过一段时间的详尽测试和安全分析。

根据良好实践，建议为漏洞打安全补丁。但由于 OT 系统的可用性需求、停机维护机会有限，且缺乏漏洞管理安全补丁，因此很难为此类系统打修补。

打安全补丁可能是当务之急，但 OT 系统的任何演进通常都要提前数月进行规划，并安排在停机维护时进行。根据变更内容，还可能需要开展详细安全分析，并辅以独立评估。

Alice 可能会发现替代缓解策略（也称为**补偿性控制措施**）的益处。其中一种选择是网络 IDS (NIDS)，它本质上是被动的，在 OT 网络上很安全 — 它不会主动扫描网络，而只是监听。与 IT 网络相比，OT 环境的变化频率较低，一旦调整为 OT 环境的标准行为，便能迅速标记任何异常流量，并通知 Alice。Alice 可以与运营团队合作，采取适当的预先计划缓解措施。Alice 不妨考虑专门为 OT 网络设计的 IDS，而非为 IT 协议设计的 IDS。

根据其网络内的安全情况，其他选择可能包括禁用服务或通过修改防火墙规则库或交换机上的访问控制列表来增加额外访问控制。Alice 可能会发现，保护其网络的边界防火墙属于交钥匙工程的实施内容，工程交付后就没再更新过，密码也很简单，甚至包括安装日期。防火墙可能属于较早且不太先进的类型，并包含关键漏洞。如果是这样的话，她不仅可以考虑更改密码，还可以考虑升级到更现代的防火墙（下一代防火墙 — NGFW）。这种防火墙可以理解穿过它的 TCP/IP 流，并有可能阻止和报告恶意软件。

Alice 负责处理边界内不同类型的资产，包括工作站、Windows 服务器和 PLC。由于 Alice 面临的边界环境多种多样，而且她不太可能拥有一套备用系统，因此她可以与系统供应商探讨各种选择。相应供应商可以利用工厂集成与确认平台 (FIVP) 合成或模拟她当前的大部分环境。

对于 OT 资产，Alice 宜考虑：

- （使用 VLAN）将相应资产定位在专用网段上，与其他流量分离开；
- 要求使用 USB 介质净化站或其他专用设施，先对任何穿越网络边界的 USB 设备进行“扫描和净化”处理；
- 确保相应资产与互联网、第三方访问和其他可信度较低的网络隔离。或许可以与供应商合作，实施数据二极管，将必要的 OT 协议单向传递给可信度较低的网络或第三方；
- 使用专用工具（如果有的话）对已安装软件进行健全性检查，并与已知良好软件进行比较；以及
- 制定报废管理计划，确定老化资产的风险管理战略。

对于安全系统，强烈建议：

- 对安全系统和过程控制系统之间的接口进行控制。宜将专用安全仪表系统 (SIS) 安装在本地网络上，与其他 OT 网络分割开；
- 宜采取措施防止对安全系统进行远程编程；
- 宜使用密码保护安全系统；
- 宜要求通过物理方式访问安全配置变更；
- 如果安全 PLC 与过程控制 PLC 位于同一设备机架中，则宜采取保护措施，限制非安全功能与安全功能之间的访问；
- 宜将用于过程控制的无线网络专用于此目的，并确保鉴别机制和安全协议使用等方面的安全实施；以及
- 不将 OT 设备连接到非 OT 网络，包括企业 Wi-Fi。

Bob

Bob 很幸运，他所在的位置部署了物理安全保护措施。他为 IT 设备专门建造了一个资料室。室内有专用架空电源、烟雾探测装置、带水探测装置的高架地板、与资料室一起管理的冗余电源和冷却装置，以及物理和电子安全锁。电子门禁系统可提供定期审查的报告。

他的组织使用 Windows Active Directory (Windows AD) 进行身份管理，他将单点登录 (SSO) 技术与多因素鉴别相结合，这样用户就能被唯一识别，无需记住大量复杂的密码，并能从远程位置安全登录。

近年来，Bob 获得了投资。他将外部防火墙更新为具有额外安全功能的下一代防火墙，并将其应用扩展到内部网络，以便将某些部门的信息置于带有专用系统和存储的独立 VLAN 上。加上对安全协议使用的增多，他的某些系统得以迁移到云中，使他能够灵活应对不断变化的需求，并降低了组织面临的建筑物损坏及其所含设备丢失的风险。Bob 能够使用虚拟化和混合云模型来推进其业务连续性计划，并快速配置测试系统，以便为其补丁管理策略提供支持。

Bob 的设备相对较新，能够记录大量与网络安全相关的事件和其他信息。相应信息会自动与 SIEM 共享，帮助其识别系统中存在的漏洞以及突然出现的新资产。他还使用其他软件对关键系统进行定期漏洞扫描，这可以帮助他有针对性地开展安全补丁活动。

由于他所在的组织更注重数据保密性，而非系统可用性，因此 Bob 能够与组织商定每周的补丁窗口期，并根据主动维护计划，每月重启一次关键系统。他使用大规模补丁部署工具来避免访问单个机器，并能在必要时强制将补丁应用到终端用户机器上。

他的大多数服务器和主机均包含软件代理。相应代理会定期扫描设备，以便保持 CMDB 中资产登记册的准确性。该数据库会高亮显示与商定软件基线的任何偏差。对设备控制软件的投资可确保所有 USB 设备要在经过加密和恶意软件扫描之后，才能用于他所管理的资产。

Bob 每周的补丁活动和漏洞扫描均会突出某些安全漏洞，他会以适当的形式与高级管理层分享，好让董事会了解风险。Bob 的安全控制措施每年均要接受外部独立渗透测试 (PenTest) 小组的测试。他的目标是在下一个财政年度为其 ISMS 系统申请到 ISO27001 证书。

目标 C：ALICE 和 BOB 检测网络安全事件的故事

Alice

虽然 Alice 可能觉得她的网络比 Bob 的网络更“封闭”（术语解释见 EN50159:2010），但她可能会发现，可供她选择的基于主机或网络的监控和检测系统更加有限。例如，通过网络 IDS (NIDS) 了解其 OT 系统的解决方案可能会更少，这样一来，通过此类解决方案了解攻击者或恶意软件对系统状态和运行背景的影响时，Alice 能获得的益处会有所减少。

来自 IT 领域的通用 IDS 解决方案容易将 OT 系统行为错误地标记为异常。相应“误报”可能很多。每次误报都需要由熟悉 Alice 系统、其协议和行为的称职分析师开展调查。

此外，基于规则的 IDS 系统，或需要定期更新特征码来识别新威胁的系统，可能会在难以应用变更的受控环境中带来其他挑战。

Alice 可能会发现，使用典型网络流量基线模型（从其环境中学习）的基于 AI/ML 的 NIDS 解决方案会是更好的选择，因为以后任何偏离已知良好状态的情况均会被标记为异常。当然，此类模型需要长期维护，才能说明环境中的授权变化，并减少作为调查警报提出的误报数量，但 Alice 环境的益处可能是它比 Bob 的环境更容易控制，变化也更少。

其中一些持续监控系统具有 OT 协议感知能力，能够理解传信和 SCADA 协议，以及与 Alice 的 OT 网络相连接的其他类型设备，如 CCTV 和 PIS。此类系统能够为任何事故提供有用的背景资料。

视供应商情况而定，深度包检测 (DPI) 可用于了解封装在相应协议中并在应用层执行的消息内容，还可能支持分区和安全级别等 IEC-62443 概念。通过这种能力，便能将安全模型叠加到现有系统上，以便识别任何违反该模型的行为，例如不同区域的设备之间或相同区域内任何未经授权的连接。

如果 Alice 选择将基于主机和网络的 IDS 集成到现有 IT SOC 中，那么就需要对分析人员进行专门培训，使他们能够像使用 IT 一样有效地使用 OT 协议。然而，Alice 很可能会得出结论，认为专门的 OT SOC（与遏制和补救其环境中威胁所需的物理干预和控制行动相结合）更适合她所在的组织。专门针对 OT 的 IDS 宜与主要 SIEM 解决方案实现本地集成，全天候监控任何潜在 OT 事故。

NIDS 的性能取决于它所接收和理解的信息。相应信息通常从日志文件和网络流量中获取。在整个系统中查找足够详细的日志，以便为安全分析提供佐证时，Alice 可能会遇到困难。此外，她可能会发现网络交换机无法（弹性）支持镜像 [15] 或 SPAN 端口，无法复制网络流量并将其转发给网络 IDS。在这种情况下，Alice 可以考虑使用硬件网络 TAP[16]。此外，Alice 的环境可能包含多个时间源，日志文件会反映这一点。理想情况下，系统会使用通用而准确的时间源，但在无法做到这一点的情况下，确保各种时间源在时间上保持一致会很有帮助，这样就能更容易识别和理解任何攻击。

Bob

Bob 可能会发现，他有很多监控和检测系统可供选择（既有开源产品，也有商业产品），其中一些解决方案（如 EDR）还可能提供自动响应能力，可以在其环境中自如使用。Bob 不太可能在更新和维护其工具方面遇到困难，他应该能够在其系统中识别和配置足够详细的日志文件，从而对其周边的网络、系统和用户行为产生广泛了解。

不过，Bob 可能会发现，与其环境相关的大量出入口都需要监控。Bob 需要警惕电子邮件对其用户和系统的威胁，并警惕用户的不良上网行为（如浏览有害网站）。相应行为可能导致恶意软件被下载到其网络上，从而导致勒索软件爆发或远程入侵。

Bob 最担心的问题之一就是他所保护数据的保密性遭到破坏。除典型防火墙和网络监控外，Bob 不妨监控其网络上的典型数据访问模式（用户行为（和实体）分析 [17]），以便识别异常情况。例如，某部门用户突然访问另一部门的敏感数据（如人力资源或财务记录），或数据被存储在云中，或被攻击者渗出。

[15] 端口镜像 - 维基百科
[16] 网络分流器 - 维基百科
[17] 用户行为分析 - 维基百科

目标 D：ALICE 和 BOB 将网络安全事故影响降至最低的故事

Alice

Alice 需要与运营和安全团队合作，确定其 OT 响应和恢复流程，以便了解事故对其环境的影响，以及实现安全、成功和及时恢复所需的资源。任何包含安全关键要素的灾难恢复计划都需要进行安全分析，确保不会对运输网络及其乘客造成危害。Alice 的响应和恢复计划很可能需要供应商的大力支持，特别是在需要开发新软件补丁时更是如此。

例如，Alice 需要考虑勒索软件在其环境中（或在相关 IT 环境中，如果她尚未在 OT 和 IT 环境之间实施安全的单向流）的影响，以及对控制系统工作站或此类系统运行所需的数据和配置文件的加密。

与 Bob 一样，Alice 的事故管理流程应包括以下步骤：

- 准备；
- 检测；
- 遏制；
- 根除；
- 恢复；以及
- 吸取经验教训。

然而，在 OT 背景下，收集证据（和遏制事故）的能力可能会受设备位置的影响。相应设备可能位于偏远或不安全的位置，并且需要多种经认证的技能组合，如地铁传信系统或轨道旁电源。此外，及时解决服务问题很可能被视为优先事项。在这种情况下，如果没有专门针对 OT 的持续监控系统，进行网络取证和确定根本原因的能力很可能会受到限制。

如果网络“扁平”，未被分割开，就算想遏制也会更加困难。通过网络分割，Allice 可以隔离出现问题的网络部分，保护已感染区域以外的系统，从而遏制问题发生。这样，遏制和根除活动的影响就会局限于感染区域，使其他服务得以继续提供。无论如何，Alice 都希望尽早遏制并删除在其环境中发现的任何恶意软件。

根据设备的性质，当设备从存储中重新加载其配置时，简单重启可能会清除恶意软件，但在其他情况下，可能需要有针对性地清除恶意软件。如果 Alice 的设备受安全案例保护，那么她可能会发现，在清除恶意软件后，她无法为设备打补丁以防恶意软件卷土重来，因为这样做会改变设备的配置，与安全案例中记录并经 OEM 认证的运行配置有所不同。

Alice 可以选择重建受影响的设备。重建可能很简单，仅需创建一个干净的存储卡或 USB 设备即可。但在其他情况下，使用原始介质进行恢复（或由 OEM 参与并可能返厂恢复），可能更适合需要重新获得安全保证的设备。

可以认为某些系统具有特殊风险，或其损失对业务影响最大。Alice 应尽可能对相应系统的恢复进行测试。此类测试被称为灾难恢复测试，通常会在尝试后续测试之前确定需要解决的问题。Alice 可能会发现，她缺乏用于测试的适当备用设备，原因可能是相应设备无法使用或丢失（或从未采购），且（由于设备老化而引起的）报废问题，迫使她不得不进行未来的业务连续性规划。

Bob

Bob 的响应和恢复流程宜以业务影响分析演练为指导，考虑其关键系统恢复的可预见影响和时间表。该分析通常包括讨论在没有各系统的情况下，企业可以管理多长时间（恢复时间目标，“RTO”）、在事件中可以容忍的数据丢失程度（恢复点目标，“RPO”），以及恢复所需的资源。

对于各种潜在事故类型，Bob 的 SOC 宜确定要如何使用操作手册（或运行手册）做出响应，以便在任何此类事故发生之前对其流程进行质量检查、测试和优化。例如，如果 Bob 的组织要识别在其网络中传播的勒索软件，则其标准流程可能包括隔离受感染的网段，以便遏制传播、将未感染系统和存储设备下线，以及删除已感染系统。在此类攻击中，时间至关重要，Bob 的 SOC 可能会考虑使用 SOAR[18] 解决方案来自动执行计划响应。归根结底，每项技术响应措施仅是公司事故响应计划中的一个要素。该计划还需要考虑通报、上报和危机管理活动。

在许多情况下，Bob 系统的物理位置对其运行并不重要，他在准备 DR 测试和事故响应时可以有很多选择。Bob 可能会得到供应商的大力支持，并能够利用虚拟化、云备份和托管技术访问替代基础设施，以便简化系统和数据恢复。

[18] 安全编排 - 维基百科

致谢

UITP 社区由衷感谢网络安全委员会第 3 工作组的贡献 — 在帮助当前出行系统防范网络威胁做足准备方面，他们为本文件的起草做出了重大贡献。

本报告完成时，工作组包括以下成员：

工作组组长 Simon Tonks（阿尔斯通）

网络安全委员会主席 Paul Gwynn (INIT)

Baldwin Gislason Bern（安讯士）

Carlo Cafasso (ATM SPA)

Majdeline Elatrache (STIB-MIVB)

Jules Gascoigne（伦敦交通局）

Geraud Lanquetin (SNCF)

Eddy Thésée（阿尔斯通）

Serge Van Themsche (Waterfall Cybersecurity)

UITP 团队

Miryam Hernandez (UITP)

安全与安保顾问 Denis Luyten (UITP)

Benjamin Steens (UITP)

文件变更历史

文件版本	工作组批准日期	网络安全委员会批准日期	发布日期	更新概述
第 1 版	2023 年 9 月	2023 年 11 月	2023 年 12 月	--
第一版修订	--	--	--	--

这是国际公共交通联会 (UITP) 的官方报告。UITP 代表了公共交通部门主要参与者的利益。其成员包括交通主管部门、所有集体客运方式的私营和公共运营商以及业界。UITP 负责客运的经济、技术、组织和管理方面，以及制定全球出行和公共交通政策。

本报告由 UITP 网络安全委员会编制

Rue Sainte-Marie 6, B-1080 Brussels, Belgium | 电话:+32 (0)2 673 61 00 | 传真:+32 (0)2 660 10 72 | info@uitp.org | www.uitp.org
版权所有 — 责任出版人 Mohamed Mezghani, Rue Marie 6, B-1080 Brussels, Belgium | 法定送存：D/2024/0105/16

DIGITAL VERSION AVAILABLE ON MYLIBRARY