安全加社区

公益译文项目

2020

网络安全框架制造篇

低影响性示例实施指南

第 1 卷 – 总体指导

NISTIR 8183A

美国国家标准与技术研究院（NIST）

美国商务部

2019 年 9 月

文档信息			
原文名称	Cybersecurity Framework Manufacturing Profile		
原文作者	Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Jeffrey Cichonski, Michael Pease, Neeraj Shah, Wesley Downard	原文发布日期	2019 年 9 月
原文发布单位	美国国家标准与技术研究院 美国商务部		
原文出处	https://doi.org/10.6028/NIST.IR.8183A-1		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区　　小蜜蜂公益翻译组

免责声明

• 本文原文来自于互联网的公共方式，由“安全加”社区出于学习交流的目的进行翻译，而无任何商业利益的考虑和利用，“安全加”社区已经尽可能地对作者和来源进行了通告，但不保证能够穷尽，如您主张相关权利，请及时与“安全加”社区联系。

•“安全加”社区不对翻译版本的准确性、可靠性作任何保证，也不为由翻译不准确所导致的直接或间接损失承担责任。在使用翻译版本中所包含的技术信息时，用户同意“安全加”社区对可能出现的翻译不完整、或不准确导致的全部或部分损失不承担任何责任。用户亦保证不用做商业用途，也不以任何方式修改本译文，基于上述问题产生侵权行为的，法律责任由用户自负。

使用说明

本指南介绍了用于保护制造环境的 PoC 方案，该方案仅在实验室环境中进行了测试。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。欢迎您对指南内容提出反馈意见，后续版本将根据各方建议、意见和成功案例进行优化。

请将反馈发至 CSF_Manufacturing_Profile_Implementation@nist.gov。

根据《网络安全框架》1.1 版更新进行修订

网络安全框架制造篇》（NISTIR 8183）起草并发布之时，《网络安全框架》为 1.0 版本。《实施指南》围绕《网络安全框架制造篇》初始版本中的内容，提供了实施指导和 PoC 方案示例。

《网络安全框架制造篇》（NISTIR 8183）拟根据《网络安全框架》1.1 版本中的更新内容进行修订并对外发布，代号为 NISTIR 8183（修订版 1）。

NISTIR 8183（修订版 1）发布后，《实施指南》会随即修订，合入《网络安全框架》1.1 版本中的内容，并对外发布，代号为 NISTIR 8183A（修订版 1）。

摘要

《实施指南》包含总体指导（第 1 卷）和概念验证（PoC）方案示例，展示在制造环境中如何按照《网络安全框架制造篇》中的低影响性要求来部署使用开源产品和商用现成（COTS）品。PoC 方案示例为流程型制造环境（第 2 卷）和离散型制造环境（第 3 卷）提供了可量化的网络、设备和业务性能影响指标。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用以管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用的网络安全标准和行业指南的补充而非替代。

关键词

计算机安全；网络安全框架（CSF）；分布式控制系统（DCS）；工业控制系统（ICS）；信息安全；制造业；网络安全；可编程逻辑控制器（PLC）；风险管理；安全控制；数据采集与监控系统（SCADA）

补充内容

本指南其余两卷为：

NISTIR 8183A 第 2 卷，网络安全框架制造篇低影响性示例实施指南：第 2 卷—流程型制造系统用例
https://doi.org/10.6028/NIST.IR.8183A-2

NISTIR 8183A 第 3 卷，网络安全框架制造篇低影响性示例实施指南：第 3 卷—离散型制造系统用例
https://doi.org/10.6028/NIST.IR.8183A-3

执行摘要

本文档提供了总体指导（第 1 卷）和概念验证（PoC）方案示例，展示在制造环境中如何按照《网络安全框架（CSF）制造篇》[8]中的低影响性要求来部署使用开源产品和商用现成（COTS）品。制造系统的完整性、可用性或机密性被破坏后，若预期对生产运营、制成品、资产、品牌形象、财务、人员、公众或环境仅会造成有限的负面影响，则该类系统的潜在影响级别为低。“有限的负面影响”指完整性、可用性或机密性被破坏后，可能会：

- 导致任务能力在一定时间内有一定程度的下降，系统仍可执行主要功能，但执行效果明显降低；
- 对运营资产造成较小损害；
- 造成轻微的财务损失；或
- 对个人造成轻微伤害。

PoC 方案示例分别针对流程型制造环境（第 2 卷）和离散型制造环境（第 3 卷），描述了实施方案对网络、设备和业务性能的影响。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。

《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用以管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用的网络安全标准和行业指南的补充而非替代。

《网络安全框架制造篇》重点阐述了期望的网络安全结果，可作为规划方案，指导读者如何识别机会，改善制造系统的网络安全状况。它根据特定的业务/任务目标，为安全活动划分了优先级，同时确定了哪些安全实践具有可操作性，可以为关键业务/任务目标提供支撑。

PoC 方案采用了商业产品，这并不代表着本指南为这些产品背书或保证其符合法规要求，各组织的信息安全专家应选用与本组织现有工具和制造系统基础架构最为契合的产品。组织可自愿采用这些方案或采用整体上遵循指导方针的方案，也可以基于本指南，对方案进行部分定制和实施。本指南不包含任何规范或强制性实践内容，也不具有法律效力。

1. 概述

根据 13636 号行政命令《提升关键基础设施的网络安全》[1]开发的自愿性《网络安全框架》提供了主次鲜明、基于性能的灵活的网络安全风险[1]管理方法，该方法可重复使用，具有成本效益，适用于关键基础设施服务交付中直接涉及的流程、信息和系统。

《网络安全框架》是基于风险的自愿性指导文件，包括行业标准和最佳实践，旨在帮助组织管理网络安全风险[2]。本框架是政府和私有部门的合作成果，采用通用语言阐述了如何基于业务需求高效地应对并管理网络安全风险，但并未提出合规要求。

针对制造业需求，政府与私营部门再次合作，制定了《网络安全框架制造篇》[8]，为制造系统及其环境中实施网络安全控制提供了可行方法。《制造篇》为保护制造系统及其组件、设施和环境定义了网络安全活动和期望结果。基于该文档，制造商可将网络安全活动与业务需求、风险承受能力和资源对齐。《制造篇》包含标准、指导方针和行业最佳实践，提供了适用于制造业的网络安全方法。

1.1 目的与范围

许多中小型制造商表示，实施基于标准的网络安全计划颇具挑战性。本文档提供了总体指导（第 1 卷）和概念验证（PoC）方案示例，展示在制造环境中如何按照《网络安全框架制造篇》[8]中的低影响性要求来部署使用开源产品和商用现成品（COTS）。制造系统的完整性、可用性或机密性被破坏后，若预期对生产运营、制成品、资产、品牌形象、财务、人员、公众或环境仅会造成有限的负面影响，则该类系统的潜在影响级别为低。“有限的负面影响”指完整性、可用性或机密性被破坏后，可能会：

- 导致任务能力在一定时间内有一定程度的下降，系统仍可执行主要功能，但执行效果明显降低；
- 对运营资产造成较小损害；
- 造成轻微的财务损失；或
- 对个人造成轻微伤害。

PoC 方案示例分别针对流程型制造环境（第 2 卷）和离散型制造环境（第 3 卷），描述了实施方案对网络、设备和业务性能的影响。各制造商应自行确定实施哪些方案内容。实施时应虑及的重要因素包括：公司规模、网络安全专业能力、风险承受能力及威胁态势。《网络安全框架制造篇》与制造业的目标和行业最佳实践保持一致，为制造商管理网络安全风险提供了思路。它所提出的基于风险的方法可自愿实施，用于管理与制造系统相关的网络安全活动及网络风险。该文档是对制造商当前所采用网络安全标准和行业指南的补充而非替代。

PoC 方案采用了商业产品，但这并不代表着本手册为这些产品背书或保证其符合法规要求。各组织的信息安全专家应选用与其现有工具和制造系统基础架构最为契合的产品。组织可自愿采用这些方案或采用整体上遵循指导方针的方案，也可以基于本手册，对方案进行部分定制和实施。本指南不包含任何规范或强制性实践内容，也不具有法律效力。

本项目有以下假设：

- 方案基于实验室环境开发；
- 实验室环境模拟了典型的小型制造商环境；
- 实验室环境无法反映生产环境的复杂性；且组织可获取实施制造业网络安全方案所需的技能和资源。

1.2 读者对象

本文档涉及制造系统相关细节信息。读者应熟知运营技术、计算机安全方面的一般概念以及通信协议（如网络中使用的协议）。目标受众包括如下各类：

- 设计或实施安全制造系统的控制工程师、集成人员和架构师；
- 管理、修复或保护制造系统的系统管理员、工程师等专业信息技术（IT）人员；
- 负责管理制造系统的人员；
- 高级管理人员，这部分人群为证明有必要实施制造系统网络安全计划以减轻对业务运行的影响而须了解前因后果；以及
- 欲了解制造系统独特安全需求的研究人员、学术机构和分析师。

1.3 文档结构

第 1 卷其余内容包括：

- 第 2 节简要介绍了制造系统。
- 第 3 节概述了《网络安全框架制造篇》内容。
- 第 4 节阐述了该项目的《网络安全框架制造篇》实施方法。
- 第 5 节概述了满足《网络安全框架制造篇》中“低影响性”要求所需的政策和程序文件。
- 第 6 节介绍了满足《网络安全框架制造篇》中“低影响性”要求所需的技术能力。
- 第 7 节讨论了满足《网络安全框架制造篇》中“低影响性”要求的可能方案。
- 第 8 节概述了实施方案的实验室环境。
- 附录 A 列举了本文档中使用的缩略词。
- 附录 B 提供了本文档使用的术语表。
- 附录 C 列举了本文档编写过程中所参考的文献。

本指南第 2 卷为流程型制造系统提供了按“低影响性”要求实施《网络安全框架制造篇》的 PoC 方案。

本指南第 3 卷为离散型制造系统提供了按“低影响性”要求实施《网络安全框架制造篇》的 PoC 方案。

2. 制造系统概述

制造业是一个庞杂的工业部门。制造业分为三类：流程型、离散型和兼具两者的混合型[3]。

流程型制造业通常使用两种主要流程：

- ***连续制造流程。***这类流程连续进行，通常分为不同阶段，经过不同程度的加工，最终形成产品。典型的连续制造流程包括电厂的燃油或蒸汽流、炼油厂的石油提炼和化工厂的蒸馏。
- ***批量制造流程。***这类流程具有清晰的处理步骤，可对一定数量的原料进行批量处理。批处理过程有明显的开始和结束动作，其间可能会有短暂的稳态操作。典型的批量制造流程包括食品、饮料和生物技术生产。

离散型制造业为生产某种产品通常会进行一系列操作，如电子和机械零件组装以及零件加工。流程型和离散型行业使用类似的控制系统、传感器和网络。此外，有些工厂同时使用离散型和流程型制造方法。

制造系统通常位于工厂内部或以工厂为中心的区域内。制造业一般使用可靠的高速现场总线和局域网（LAN）技术进行通信。无线网络技术在制造业中也开始流行。现场总线包括 DeviceNet、Modbus 和控制器局域网（CAN）总线。

关键基础设施领域的制造业包括公私营所有者和运营商等实体。关键基础设施组织利用工业控制系统（ICS）和信息技术（IT）来实现功能。由于依赖技术、通信以及 ICS/IT 互连性，潜在的漏洞发生了变化并越来越多，制造系统业务的潜在风险也随之增长。

3. 《网络安全框架制造篇》概述

《制造篇》[8]为在制造系统及其环境实施网络安全控制措施提供了可行方法。第 7 节中的子类描述源自 NIST 特刊（SP）800-53（修订版 4）[4]中的安全控制措施，并参考相关信息针对制造领域进行了修改。《网络安全框架》中提及的一般性参考文献 ISA/IEC 62443[5]也列在“参考资料”中。800-53 文件中若无相关信息，子类描述则以 COBIT 5 为参考。其他输入来源还包括 NIST SP 800-82（修订版 2）的 6.2 节（ICS 安全控制应用指南）和附录 G（工控系统安全控制包[3]）。对于参考一系列或全套控制措施的情况（例如，ID.GV-1 子类对所有“政策和程序”控制措施的参考），采用了包含全系列/套控制措施的整体方法。

《制造篇》针对制造系统环境对网络安全控制措施进行了修改，说明在应用《网络安全框架》中的大类和子类时，考虑到了特定领域的具体情况、业务驱动因素、风险评估和制造商优先级。《制造篇》用户还可以根据需要添加大类和子类，以应对特定或自身特有的风险。

4. 《网络安全框架制造篇》实施方法

在实现《制造篇》子类要求时，可根据特定的子类定义来制定、实施政策和程序并/或实施技术方案。

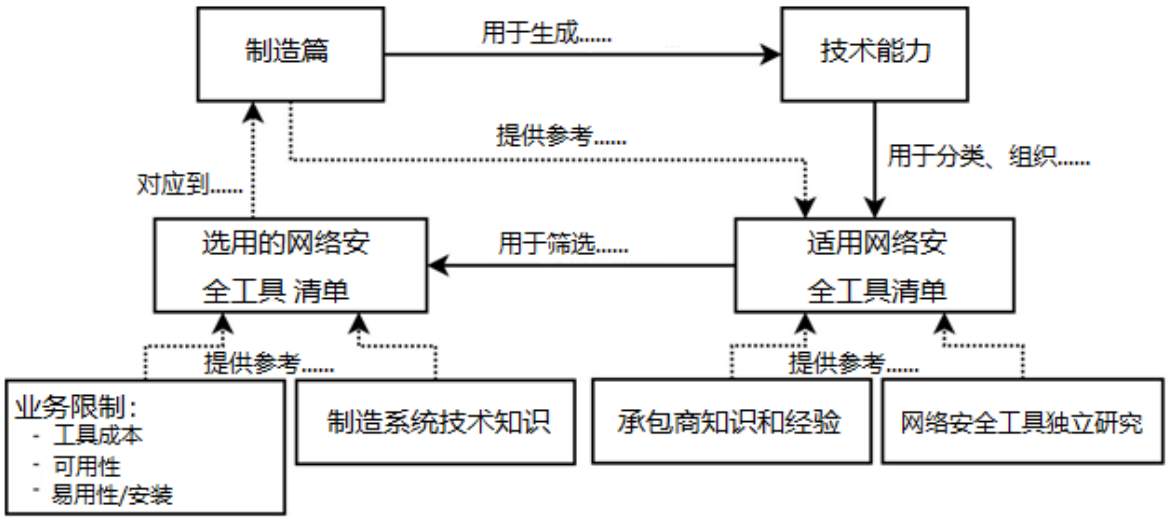

图 4-1 技术网络安全能力的识别、规划与实施方法

图 4-1 展示了技术网络安全能力的识别、规划与实施方法，同时定义了辅助性网络安全流程与程序。《网络安全框架制造篇》作为主要资源，描述了 NIST 的两种制造业测试场景下的期望网络安全结果。《制造篇》中所述结果基于工控系统所有者和运营商相关标准中的网络安全控制措施并与之互为参照。

在该规划流程的第一步，重点研究实现特定结果或《制造篇》子类所需的网络安全相关工具、配置和最佳实践。通过《制造篇》子类和相应网络安全控制措施的描述，组织可深入了解测试环境中需要实现的各类技术能力。基于这些粗略的能力分类，NIST 研究人员确定了适用于这些分类的商业产品和开源工具并编制了列表，接下来，参考方案列表来落实规划并选取特定方案、工具和产品用于测试环境。选用技术时应考虑以下因素：测试技术知识、解决方案成本、可用性、成熟度、实施和管理所需的专业知识水平、实验室 IT 管理员的专业知识。

在大多数情况下，技术方案与《制造篇》子类并非一对一精确对应。在规划过程中会发现，实施某项技术能力多半只能部分满足子类要求，在某些情况下，需要实施多项技术能力才能实现《制造篇》某个子类所描述的结果。有些《制造篇》子类（如 RP.DS-3）要求在实施某项技术能力的同时，还要补充实施网络安全政策或程序。虽然该匹配过程增加了规划过程的复杂性，但有助于系统所有者了解可使用哪些技术方案实现最多的子类结果。可以根据组织的具体任务和业务目标划分优先级。

第 5 节概述了满足《网络安全框架制造篇》中“低影响性”要求所需的政策和程序文件。

第 6 节介绍了满足《网络安全框架制造篇》中“低影响性”要求所需的技术能力。

第 7 节讨论了满足《网络安全框架制造篇》中“低影响性”要求的可能方案。

5. 政策/程序能力概述

为实施这两个用例，为每个用例各开发了六份政策和程序文件：

5.1 网络安全计划文件

网络安全计划文件为组织启动、实施、维护和改进信息安全管理提供了指导方针和原则，包括安全政策、程序、指南和标准等一系列文件。网络安全计划旨在保护信息资源的机密性、完整性和可用性。

5.2 网络安全政策文件

网络安全政策文件规定了在本组织恰当、安全地使用信息技术服务的网络安全要求，目的是最大限度地保护组织及其用户免受可能危及其完整性、隐私、声誉和业务结果的网络安全威胁。

5.3 网络安全操作文件

网络安全操作文件制定了操作步骤，让管理人员及员工响应制造系统内发生的事件时有标准可循。实际操作中应时常提及本文件内容，确保制造系统内的所有员工和个人熟悉网络安全操作。

5.4 风险管理文件

风险管理策略文件阐述了如何识别、分析与管理组织所面临的风险。该文件概述了组织的风险管理策略，提供了标准术语、明确的角色和责任以及风险管理流程的详细信息¡£管理层可基于本文件了解风险、预估影响并确定问题响应措施。文件旨在为项目团队和利益相关者提供指导。

5.5 事件响应计划文件

事件响应计划文件阐述了组织内部响应信息安全事件的计划。它定义了参与者的角色和职责、事件特征、与其他政策和程序的关系以及报告要求。本计划的目的是检测和应对网络安全事件，确定其范围和风险，对事件做出恰当响应，将结果和风险告知所有的利益相关者，并降低事件再次发生的可能性。

5.6 系统恢复计划文件

系统恢复计划旨在确保发生网络安全事件时，重要的制造/业务流程不会中断，该计划利用与组织的 IT 和 OT 环境相关的基础设施存量和配置信息，为响应网络安全事件提供结构化方法，恢复运营能力。

- 系统恢复计划用以实现以下目标：
- 最大程度地缩短制造中断时间，控制损失；
- 评估损失，修复损坏，恢复制造系统；
- 有序、高效地管理恢复操作；及
- 安排人员在系统恢复场景下有效响应。

6. 技术能力概述

本节主要探讨需要哪些技术能力来满足《CSF 制造篇》的要求，这些能力由团队筛选确定。对于每项技术能力，均进行了概述，列出了实施该能力的安全效益，讨论了该能力可能对制造系统产生的潜在系统影响，并列出了实施该能力所满足的《CSF 制造篇》子类。

6.1 硬件存量管理

利用硬件存量管理工具，制造商可跟踪制造系统中的计算和网络设备，包括设备详细信息和位置信息。

6.1.1 安全效益

硬件存量管理工具用于跟踪制造系统中的物理计算和网络设备，检测新设备或未授权设备，监测设备删除情况，跟踪特定设备的详细信息。只有对环境中存在的计算和网络设备完整记录，才能全面部署网络安全防护措施。

6.1.2 潜在系统影响

硬件存量管理工具进行主动扫描时可能会对制造系统产生影响。在使用这些工具检测业务系统上的制造系统设备时务必谨慎。造成影响的原因可能是信息性质，也可能是网络流量。建议在计划停机期间用硬件存量管理工具进行主动扫描，收集详细的数据。要对制造系统进行持续监控，可使用被动硬件存量管理工具。

6.1.3《制造篇》子类

ID.AM-1, PR.DS-3, DE.CM-7

6.2 软件/固件存量管理

利用软件/固件存量管理工具，制造商可跟踪安装在制造系统计算和网络设备中的软件和固件，包括标识、版本号和位置信息。

6.2.1 安全效益

利用软件/固件存量管理工具，制造商可跟踪制造系统内系统上安装的软件和固件，检测新软件或未授权软件，跟踪软件版本，远程删除软件。有些软件存量管理工具还可将扫描扩展到系统本身（即扫描系统外围设备、已安装的 RAM 和处理器以及网络配置）。

6.2.2 潜在系统影响

软件/固件存量管理工具进行主动扫描时可能会对制造系统产生影响。在业务系统上使用这些工具务必谨慎。造成影响的原因可能是信息性质，也可能是网络流量。建议在计划停机期间用软件/固件存量管理工具进行主动扫描。

6.2.3 《制造篇》子类

ID.AM-2, PR.DS-3, DE.CM-7

6.3 系统开发生命周期管理

利用系统开发生命周期管理工具，制造商可跟踪制造系统软硬件组件的活动范围，包括各组件的启动、开发与获取、实现、运维以及其最终停用和处置。

6.3.1 安全效益

系统开发生命周期管理工具对软硬件进行从购买/安装到移除/停用的全流程跟踪。对固件、BIOS、驱动程序、软件和补丁等更新进行跟踪，可确保更有效地防范已知和未知漏洞，让制造商更好地了解其系统风险。

6.3.2 潜在系统影响

系统开发生命周期管理工具通常不在制造系统上安装或操作，应不会影响制造系统。

6.3.3 《制造篇》子类

PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-6, DE.CM-7

6.4 网络架构文档

利用网络架构文档工具，制造商可识别、记录和绘制联网制造系统设备、企业网络和其他外部网络连接之间的互连关系。

6.4.1 安全效益

有关制造环境的网络设备和互连关系的详细文档是《制造篇》的重要组成部分。只有全面了解环境内部的互连关系，才能部署好网络安全控制措施。这种信息对于有效监测同样重要。

6.4.2 潜在系统影响

网络架构文档工具使用自动拓扑发现技术时可能会影响制造系统。在业务系统上使用这些工具务必谨慎。造成影响的原因可能是信息性质，也可能是网络流量。建议在计划停机期间使用网络架构文档工具进行自动拓扑发现。在为网络架构编写文档时，特别是在网络规模不大或不复杂的情况下，也可以对网络连接进行物理检查或对网络日志进行分析。

6.4.3 《制造篇》子类

ID.AM-3, ID.AM-4

6.5 配置管理

利用配置管理工具，制造商可控制整个系统开发生命周期中的组件配置初始化、变更、监控和审核流程，构建和维护制造系统软硬件组件的完整性。

6.5.1 安全效益

借助配置管理，系统可安全部署并保持一致性，且在整个生命周期中始终保持这种状态。配置管理可提高系统的可见性，跟踪变更，降低由于配置问题和安全漏洞而导致的停机风险。此外，它还能检测和修正可能对性能或安全产生负面影响的错误配置，改善员工的体验。

6.5.2 潜在系统影响

配置管理工具可能会影响制造系统。这些工具在制造系统网络中传输各种类型的数据，数量可能会很庞大，还可能尝试更改配置或操控设备中的活动文件，影响制造系统运行。可在部署前和计划维护停机期间验证配置，最大限度地减少此类影

响。

6.5.3《制造篇》子类

ID.AM-3, ID.AM-4, PR.IP-1, PR.IP-4, PR.MA-1

6.6 建立基线

制造商可利用基线建立工具对制造系统基线配置进行管理。这些工具跟踪制造系统组件信息（例如软件许可证信息、软件版本号、人机界面（HMI）和其他 ICS 组件的应用程序、软件、操作系统；操作系统和应用程序的当前版本号和补丁信息；配置设置/参数）、网络拓扑，以及这些组件在系统架构中的逻辑位置。

6.6.1 安全效益

基线是一种自动化配置管理方法。具有安全基线且安全部署的系统对网络安全威胁具有更强的抵御能力。基线化提高了变更管理效率，在发生中断或网络安全事件时可加速恢复。

6.6.2 潜在系统影响

基线建立工具进行主动扫描时可能会对制造系统产生影响。在业务系统上使用这些工具务必谨慎。造成影响的原因可能是信息性质，也可能是网络流量。建议在计划停机期间使用基线建立工具进行主动扫描。

6.6.3 《制造篇》子类

ID.AM-3, PR.IP-1, DE.AE-1, DE-CM-7

6.7 更控制

利用变更控制工具，制造商可记录、跟踪和协调制造系统软硬件组件的变更。

6.7.1 安全效益

变更常伴有意想不到的副作用，导致停机或业务中断。合理的配置和更改控制计划可防止频繁停机。变更控制流程确保变更记录在案，由相关人员审批。

6.7.2 潜在系统影响

创建、修改和保存变更控制文档和程序不会影响制造系统。

6.7.3 《制造篇》子类

PR.IP-1, PR.IP-3, PR.MA-1, DE.CM-7

6.8 配置备份

利用配置备份工具，制造商可收集制造系统中的软硬件组件配置设置，并以组件的原始设备制造商（OEM）指定的数据格式进行存档。

6.8.1 安全效益

备份配置后，制造商可将设备的配置设置还原到特定时间点的已知正常状态。这样，在事故发生时，可快速恢复到之前的运行状态。

6.8.2 潜在系统影响

备份工具和方法在获取配置备份时可能会占用过多的处理能力或网络带宽，有时还需要对设备进行物理访问，因而给制造系统带来潜在影响。配置备份应根据计划停机时间进行规划。

6.8.3 《制造篇》子类

PR.IP-1, PR.IP-4

6.9 数据备份

利用数据备份工具，制造商可收集和保存制造系统中的文件和程序，以便在发生事故后进行恢复。

6.9.1 安全效益

备份数据后，可还原之前某一时间点的数据，帮助组织从事件中恢复。在发生勒索软件事件或硬件故障时，这些备份提供了额外保障，确保关键数据有备份并被离线保存。此外，从备份中恢复的数据还可用于取证调查。

6.9.2 潜在系统影响

备份工具和方法在获取数据备份时可能会占用过多的处理能力或网络带宽，有时还需要对设备进行物理访问，因而给制造系统带来潜在影响。远程备份通常需要在设备上安装软件代理。配置软件代理时，应尽可能使其占用最小处理能力，保证正常运行即可。配置基于网络的数据备份时，应尽可能使其占用最小网络带宽，保证正常运行即可。数据备份应根据计划停机时间（若有）进行规划。

6.9.3 《制造篇》子类

PR.IP-4

6.10 数据复制

制造商可使用数据复制工具将备份数据复制和传输到制造系统外部的物理位置。

6.10.1 安全效益

通过复制数据，组织可将数据存储在多个位置。物理分离和离线存储可进一步保证数据的完整性，这可以通过硬件级和软件级加密工具实现，保证组织的数据不会受到非法访问。

将数据复制到远程位置后，即便发生火灾、洪水或其他自然或人为灾害时，数据也会安然无恙。

6.10.2 潜在系统影响

数据复制和配置备份通常独立于制造系统，应不会影响制造系统。

6.10.3 《制造篇》子类

PR.IP-4

6.11 网络分段与隔离

利用网络分段与隔离方案，制造商可将制造系统网络与其他网络（如企业网、访客网络）分隔，将内部制造系统网络分割成更小的网络，控制特定主机和服务之间的通信。

6.11.1 安全效益

对网络进行合理分段可增强访问控制，方便 IT 管理员限制和监控用户对系统的访问。网络分段与隔离可最大程度地减少广播域流量，有助于限制事件的影响范围，提高网络性能。

6.11.2 潜在系统影响

网络分段与隔离可能会对制造系统产生潜在影响，在规划和部署网络分段与隔离时务必谨慎。根据网络设备的拓扑、硬件和配置，网络分段与隔离可能会造成不同程度的网络延迟。

6.11.3 《制造篇》子类

PR.AC-5

6.12 网络边界防护

制造商可利用网络边界防护方案限制进出制造系统网络的数据通信流量。网络边界防护功能包括但不限于使用防火墙、非军事区（DMZ）以及入侵检测和预防系统。

6.12.1 安全效益

组织可使用防火墙对其网络进行分段，仅允许授权连接访问网络。防火墙监控和记录访问或试图访问网络的流量，为响应和恢复活动提供了至关重要的取证数据。更高级的防火墙（通常称为“下一代防火墙”（NGFW））包括防病毒和恶意软件保护，数据集不断升级以检测最新威胁。这些 NGFW 还提供其他高级安全防护，如入侵检测、深度包检测、虚拟专用网（VPN）服务和拒绝服务防护。DMZ 的物理和逻辑隔离特性非常重要，因为它们只允许访问指定的服务器和隔离 DMZ 中存储的信息，而不会直接暴露敏感的制造网络。DMZ 网络可减少并控制从组织外部对内部系统的访问。入侵检测和防御系统可监控、检测、分析和阻止对网络或系统的非法访问。

6.12.2 潜在系统影响

网络边界防护方案对制造系统有潜在影响，在规划和部署这些方案时务必谨慎。串联部署边界防护设备（如防火墙）可能会加大网络延迟，特别是当设备和网络的能力不匹配时（例如，1G 网络上部署 100M 以太网设备）。

6.12.3《制造篇》子类

PR.AC-5, PR.PT-4, DE.CM-1

6.13 远程安全接入

利用远程安全接入方案，制造商可建立安全信道，通过不可信网络（包括互联网等公共网络）传输信息。

6.13.1 安全效益

通过建立安全信道或加密隧道，制造商可向外部实体授予对制造系统中敏感组件的访问权限，以便获取厂商升级包、技术支持或允许员工远程访问等。制造系统中的数据经过加密，可通过 VPN 这样的安全信道访问，防止被潜在的恶意用户获取。

在实现该功能时，更高级的情况是使用基于安全套接字层（SSL）的 VPN，对远程访问设备执行安全运行状况检查，确保受感染机器不会访问关键的系统组件。

6.13.2 潜在系统影响

远程安全接入方案可能会影响制造系统，制造系统运行时进行远程接入务必谨慎。通过远程访问连接进行操作时可能会产生过多网络流量，应严格控制通过远程访问进行运维，须基于计划停机时间规划此类活动。

6.13.3《制造篇》子类

PR.AC-5, PR.MA-2

6.14 管理网络接口

利用管理网络接口方案，制造商可控制通过网络设备的物理端口收发的连接和信息。

6.14.1 安全效益

管理网络接口控制对特定网络的连接，加大了未授权设备进入网络的难度。当未授权设备插入网络接口时，只有在配置端口后，管理接口才会发送流量。这样，管理接口就确保了只有已识别的设备才能通过网络发送流量。

6.14.2 潜在系统影响

管理网络接口方案可能会影响制造系统，增加运维活动（例如升级网络组件、将维护计算机连接到本地网络等）的难度。

6.14.3 《制造篇》子类

PR.AC-5

6.15 绘制数据流

制造商可利用数据流图了解制造系统联网组件之间的数据流动情况。

6.15.1 安全效益

通过记录数据流，组织能够了解预期网络行为。知悉设备的通信情况对故障排除以及随后的响应和恢复活动均有意义。可在取证活动中使用这些信息，也可以通过分析这些信息来识别异常情况。

6.15.2 潜在系统影响

数据流绘制工具在使用主动扫描或要求使用网络监控工具（例如串联部署的网络探针）时可能会影响制造系统。使用这些工具检测业务系统上的数据流时务必谨慎。信息性质、网络流量或制造系统组件与网络的瞬间断开都可能会造成影响。建议在计划停机期间利用数据流绘制工具进行检测。

6.15.3《制造篇》子类

ID.AM-3, ID.AM-4, PR.AC-5, DE.AE-1

6.16 时间同步

制造商可使用时间同步方案同步制造系统所有组件的时间，生成准确的时间戳。

6.16.1 安全效益

时间同步可防止重放攻击，对于 Kerberos 等身份验证协议至关重要。在进行调查时，时间同步对于关联事件或日志也颇有意义。

6.16.2 潜在系统影响

时间同步应不会影响制造系统，但未同步的时间或错误配置可能会影响需要时间同步的服务。

6.16.3 《制造篇》子类

PR.PT-1

6.17 凭证管理

利用凭证管理工具，制造商可管理用户认证和授权凭证的生命周期。

6.17.1 安全效益

使用凭证管理工具，制造商可安全地存储凭证，对凭证执行生命周期管理活动，例如要求更改密码、为各用户定义权限级别以及撤消凭证。有些凭证管理方案取消了静态和长期权限，最大程度地减少了攻击面。

6.17.2 潜在系统影响

凭证管理工具通常不在制造系统上安装或操作，应不会影响制造系统。制造系统运行时，不应更新凭证。方案若可自动轮换凭证，应配置为仅在计划维护停机期间更改凭证。

6.17.3 《制造篇》子类

PR.AC-1, PR.MA-1, PR.MA-2

6.18 认证授权

制造商可使用认证授权工具验证用户身份，实施最小权限原则。利用支持认证授权的工具和技术，制造商能够设置用户权限，确定用户是否具有访问系统资源的权限。在可行情况下，将集中认证授权机制集成至系统架构。

6.18.1 安全效益

有了集中认证系统，用户仅通过一套登录凭证便可访问系统。此外，单一平台上的集中认证授权功能为授权管理员提供了统一的用户访问管理方法。最小权限确保用户和程序只获得执行其任务所需的权限。

6.18.2 潜在系统影响

认证授权工具可能会影响制造系统。这些工具通常需要在设备上安装软件代理，或者需要使用网络进程，导致时延或中断制造过程。建议备份认证授权服务器，防止操作人员“消失”（Loss of View）和“失控”（Loss of Control)事件。制造商应出于性能、安全或可靠性原因，划定认证授权的不适用范围。

6.18.3 《制造篇》子类

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

6.19 防病毒/恶意软件

利用防病毒/恶意软件工具，制造商可监控计算设备，检测主流恶意软件，防止或遏制恶意软件事件。

6.19.1 安全效益

对许多制造商来说，恶意软件是最常见的威胁。反病毒/恶意软件工具可保护设备，防止设备受到恶意软件（如勒索软件、病毒、蠕虫、木马和恶意移动代码）感染。

6.19.2 潜在系统影响

防病毒/恶意软件工具可能需要在设备上安装软件代理，或者在认证后执行网络扫描，对制造系统造成潜在影响。配置这些工具时，应尽可能使其占用最小处理能力，保证正常运行即可。防病毒/恶意软件工具在经过认证进行网络扫描时，可能会产生过多的网络流量。配置这些工具时，应尽可能使其占用最小网络带宽，保证正常运行即可。建议根据计划停机时间规划扫描。

6.19.3 《制造篇》子类

DE.CM-4

6.20 风险评估

制造商可使用风险评估工具评估制造系统的风险。

6.20.1 安全效益

风险评估会从内外部威胁来评估组织的安全态势，识别当前安全漏洞、控制差距和不合规情况。实施风险评估时，可通过调查、讨论和/或问卷进行。风险评估是整个风险管理流程中的一部分，为高管提供必要信息，以确定应对已知风险的合理行动方案。这些评估结果可用于培养员工的安全意识，也可作为培训工具。定期进行风险评估可减少工作场所中的网络安全事故。

6.20.2 潜在系统影响

风险评估工具的访问、运行一般独立于制造系统，应不会对制造系统产生影响。

6.20.3 《制造篇》子类

ID.RA-1

6.21 漏洞扫描

利用漏洞扫描工具，制造商可扫描、检测和识别软件缺陷或错误配置，防止制造系统出现漏洞。

6.21.1 安全效益

识别制造网络中存在哪些已知安全漏洞，补丁管理才能有的放矢。

6.21.2 潜在系统影响

漏洞扫描工具会影响业务系统。漏洞扫描工具可能需要在设备上安装软件代理，或者在认证后通过网络进行扫描。漏洞扫描工具可能会产生过多网络流量，在极端情况下，甚至会由于扫描时使用了侵入性方法而导致设备故障。配置这些工具时，应尽可能使其占用最小网络带宽，保证正常运行即可。建议基于计划停机时间规划扫描，避免在制造系统运行时进行扫描。

6.21.3 《制造篇》子类

ID.RA-1, DE.CM-8

6.22 漏洞管理

利用漏洞管理工具，制造商可记录、管理、缓解制造系统中的漏洞。

6.22.1 安全效益

制造商可使用漏洞管理工具对系统进行安全更新，并找出需要采取补充控制措施的地方以保护无法更新的设备。

6.22.2 潜在系统影响

漏洞管理工具可能会影响制造系统。补丁程序可消除漏洞，但也会从生产或安全角度引入风险。

修补漏洞可能还会改变操作系统或应用程序的运行方式。建议咨询产品厂商，确认是否具有已批准补丁列表和漏洞管理流程。建议基于计划停机时间规划漏洞管理，并将其融入系统开发生命周期、配置管理和更改管理流程。

6.22.3 《制造篇》子类

ID.RA-1, DE.CM-4, RS.MI-3

6.23 安全事件管理

利用安全事件管理工具，制造商可记录、跟踪和协调制造系统设备或网络中的恶性事件缓解活动。

6.23.1 安全效益

安全事件管理工具让制造商能够最大程度地减少安全事件引起的停机时间，提高制造系统的效率和生产力。制造商可参考安全事件处理过程中获得的信息，做好准备，应对未来可能出现的其他安全事件。组织可制定事件响应计划，在事件发生前主动或事件发生后立即采取行动，降低事件的影响。

6.23.2 潜在系统影响

安全事件管理工具的访问、运行一般独立于制造系统，应不会对制造系统产生影响。

6.23.3 《制造篇》子类

RS.MI-2, RS.MI-3

6.24 网络监控

利用网络监控工具，制造商可捕获、保存和检查来自制造系统网络的网络流量，并持续监控，发现潜在网络安全事件迹象。

6.24.1 安全效益

制造商可利用网络监控工具识别可疑流量和其他威胁向量，对事件做出快速响应。这些工具有助于减少人为错误、配置问题和其他环境因素引起的安全事件。有效的网络监控能够促进网络性能问题的检测、诊断和解决，通过主动识别威胁和瓶颈减少安全事件。

6.24.2 潜在系统影响

网络监控工具的访问、运行一般独立于制造系统，应不会对制造系统产生影响。然而，某些网络流量抓包方法（例如串联部署的网络探针、镜像端口）会加大网络设备负载，加大网络延迟。

6.24.3 《制造篇》子类

PR.DS-5, PR.MA-2, PR.PT-4, DE.CM-1, DE.CM-6, DE.CM-7

6.25 系统操作监控

通过系统操作监控方案，制造商能够监控、保存、检查和限制制造系统用户的活动。

6.25.1 安全效益

监控制造系统内的系统和用户可确保其行为符合预期。此功能还能识别出问题发生时对系统进行操作的用户，为故障排除提供有用信息。监控还有助于发现制造系统中的错误配置或其他潜在错误。

6.25.2 潜在系统影响

系统操作监控工具可能会影响制造系统。这些工具通常需要在设备上安装软件代理，因此会占用处理能力和网络带宽。配置软件代理时，应尽可能使其占用最小处理能力，保证正常运行即可。

6.25.3 《制造篇》子类

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

6.25 维护跟踪

利用维护跟踪方案，制造商能够对制造系统计算设备的维护和维修活动进行规划、跟踪、授权、监控和检查。

6.26.1 安全效益

对制造系统内设备的变更进行跟踪可确保所有的维护或变更操作均妥善记录在案。跟踪这些事件可形成审计线索，为故障排除、响应和恢复提供有用信息。通过维护跟踪，制造商可了解组件应何时维修，并就何时停产做出明智决策。这种类型的跟踪还可以实现提前协调，以免在制造系统内造成中断。

6.26.2 潜在系统影响

维护跟踪工具的访问、运行一般独立于制造系统，应该不会对制造系统产生影响。

6.26.3 《制造篇》子类

PR.MA-1, PR.MA-2

6.27 物理访问控制

制造商可利用物理访问控制方案拒绝或限制个人非法访问制造系统。

6.27.1 安全效益

限制物理访问权限可以防止未经授权的恶意用户访问关键组件，进而保护制造系统。此外，这也有助于防止意外损坏或无心之失。

6.27.2 潜在系统影响

物理访问控制工具不会影响制造系统。

6.27.3 《制造篇》子类

PR.AC-2, PR.DS-5, PR.MA-1

6.28 物理访问监控

利用物理访问监控方案，制造商可记录、监控、存档和检查所有个人对制造系统的物理访问。

6.28.1 安全效益

通过记录、监控、存档和检查个人对制造设施和位置的物理访问，制造商能够了解制造系统内的物理访问情况。关联这类日志后，还能识别恶意威胁源起方及其他恶意活动。

6.28.2 潜在系统影响

物理访问监控工具不会影响制造系统。

6.28.3 《制造篇》子类

PR.AC-2, PR.PT-1, DE.CM-2, DE.CM-3

6.29 端口和服务锁定

利用端口和服务锁定方案，制造商能够发现并禁用非必要的物理和逻辑网络端口及服务。

6.29.1 安全效益

发现并禁用制造系统中的无用物理端口可阻止恶意设备连接到网络，避免为恶意威胁源起方大开方便之门。搞清楚网络中正在使用哪些逻辑端口以及需要哪些服务，这属于纵深防御，恰似添加了一道额外屏障。

6.29.2 潜在系统影响

端口和服务锁定可能会影响制造系统。在禁用所有端口和服务之前，都必须弄清它们的作用，确认它们非制造系统所需。

6.29.3 《制造篇》子类

PR.IP-1, PR.PT-3

6.30 媒体防护

制造商可利用媒体防护方案限制在制造系统中使用移动媒体。

6.30.1 安全效益

有了媒体防护方案，未知和潜在恶意设备很难连接到制造系统设备，相关威胁相应降低。

6.30.2 潜在系统影响

媒体防护方案对制造系统有潜在影响，针对特权用户的媒体防护限制了特权用户对制造系统事件或事故的响应能力，因而可能会对制造系统有一定影响。务必确认特权用户具有执行其角色功能所需的访问权限。

6.30.3 《制造篇》子类

PR.PT-2

6.31 加密

制造商可利用加密方案保护敏感的制造系统数据，将其访问权限局限于授权用户。

6.31.1 安全效益

加密是将明文转换为密文的过程，只有输入正确密钥才能查看，这就确保了数据在使用/传输时和静止状态的机密性。在数据被窃取或泄露时，加密可将敏感信息的泄露风险降至最低。

6.31.2 潜在系统影响

使用加密工具可能会影响制造系统，因为加解密数据时的运算需要处理能力和内存。若在嵌入式设备上执行加密，影响则更为严重。加解密方法的选用也可能会对具有时效性的数据通信造成影响。此外，用于加密设备之间通信的物理网络硬件可能会加大网络延迟。加密可有效保护数据机密性和完整性，但必须认真规划实施过程，以尽量减少对制造过程的潜在干扰。

6.31.3 《制造篇》子类

PR.DS-5

6.32 数据泄露防护

制造商可利用数据泄露防护方案检测并防止非法访问和传输敏感的制造系统数据。

6.32.1 安全效益

检测并防止泄露网络设备中的敏感信息。

6.32.2 潜在系统影响

基于网络的数据泄露防护工具在监控、检测数据泄露时通常不会影响制造系统。基于端点的数据泄露防护工具会占用处理能力和/或网络带宽，进而影响制造系统。配置这些工具时，应尽可能使其占用最小处理能力，保证正常运行即可。

6.32.3 《制造篇》子类

PR.DS-5

6.33 媒体过滤

媒体过滤方案确保媒体中的数据无法恢复。

6.33.1 安全效益

媒体过滤方案可确保机密信息从包含存储介质（如 USB 闪存驱动、内外置硬盘、存储卡）的设备中删除或销毁。设备淘汰后，若其中信息未经妥善处理可能会带来安全问题。

6.33.2 潜在系统影响

媒体过滤工具一般独立于制造系统运行，应不会对制造系统产生影响。相关流程应与配置和变更管理流程集成，保证组件有源可查，有责可究。

6.33.3 《制造篇》子类

PR.DS-3, PR-IP-6

6.34 事件日志

利用事件日志方案，制造商可捕获、保存、存档和检查制造系统及其网络中发生的事件。

6.34.1 安全效益

事件日志提供系统操作方面的重要信息。这些信息可用于优化报告、日志收集、分析，有助于防止安全入侵事件。日志功能若足够强大，不仅能减少安全事件的影响，还能助力组织的合规建设。

6.34.2 潜在系统影响

事件日志方案对制造系统有潜在影响。事件记录器要正常工作，制造系统中的

设备必须生成消息，发送给记录器。发送这些消息会消耗网络带宽，流量大小取决于主机数量和配置的日志级别（如严重错误、警告、调试等）。在占用网络带宽和目标日志级别之间须有所取舍，基于风险做出决策。在向事件记录器发送大量消息时，设备负载可能会加重。

6.34.3 《制造篇》子类

PR.PT-1, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

6.35 取证

制造商可利用取证方案对制造系统中的数据进行识别、收集、检查和分析，查明事件原因。

6.35.1 安全效益

通过收集网络环境中的取证数据，组织可对网络数据进行检查，为识别恶意活动和查明潜在攻击者提供更多的数据支撑。基于设备和网络日志，组织可追究威胁源起方责任。若需外部事件响应公司协助调查事件，取证数据也非常有用。

6.35.2 潜在系统影响

取证工具一般独立于制造系统运行，因此应不会对制造系统产生影响。

6.35.3 《制造篇》子类

DE.AE-2，RS.AN-3

表 6-1 CSF《制造篇》子类与技术能力对应关系表

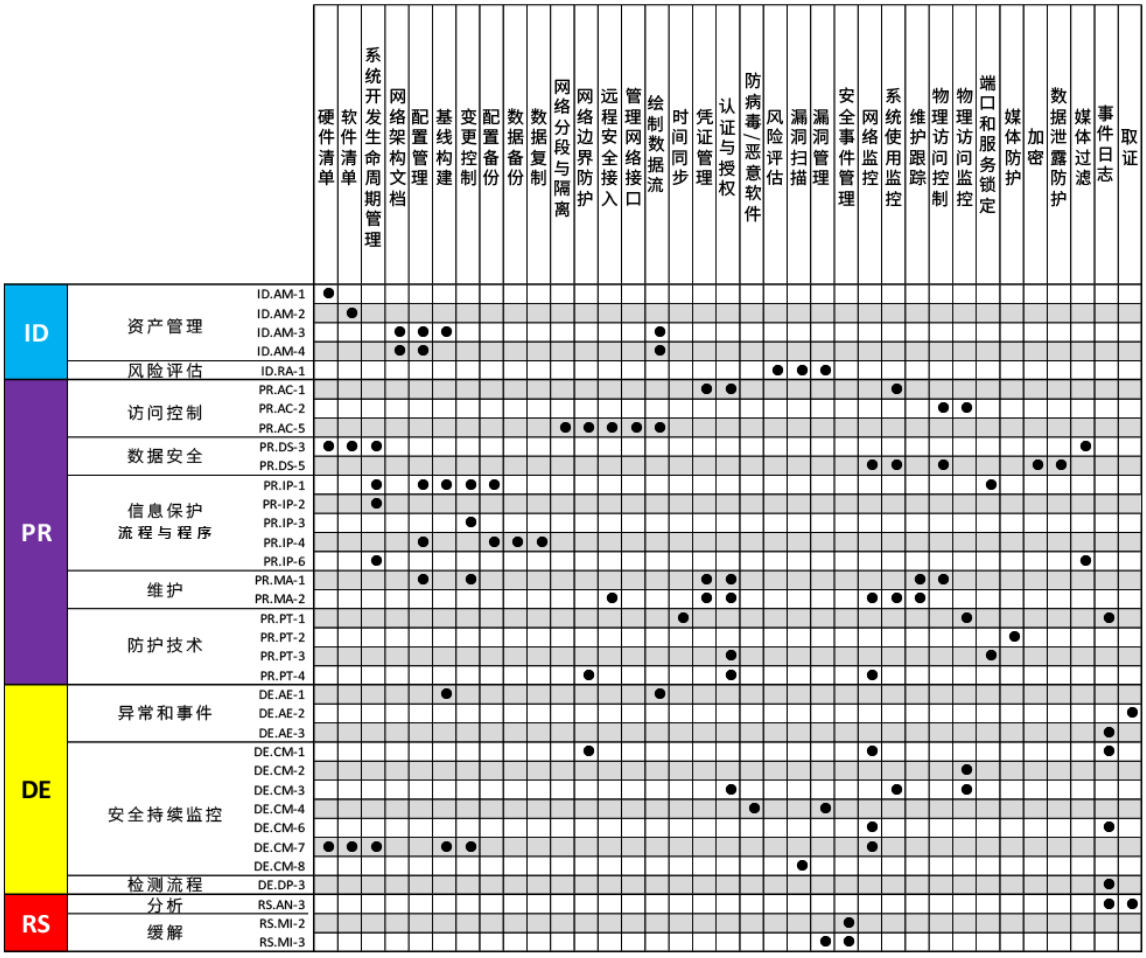

表 6-1 总结了本节的主要内容，给出了网络安全计划中所实施的技术能力与《CSF 制造篇》子类的对应关系。

7. 能力与制造篇的对应关系

本节分析了实现各子类需求要采取的政策和程序（见第五节）和/或技术方案（见第六节），并列举了小型制造商实现这些需求可能要采取的方案。判断这些方案是否可行主要取决于成本、易用性以及要投入的工作量。表中所列举的可能方案仅为示例，并非全部。关于每个用例的实验室环境中实施的特定方案，我们将在卷 2 和卷 3 中介绍。

功能	大类	子类	制造篇	实施概要
识别	资产管理（ID.AM）	ID.AM-1	**低** • 制作制造系统组件清单。 • 制造系统组件包括可编程逻辑控制器（PLC）、传感器、执行器、机器人、机床、固件、网络交换机、路由器、电源以及其他联网组件或设备。应按组织规定对系统组件清单进行评审和更新。 • 为了对制造系统组件实施问责制，需提供硬件清单明细表、组件负责人、联网组件或设备、机器名称和网络地址。清单明细表需列出制造商、设备类型、型号、序列号和物理位置等信息。	针对这类需求，可采用具有**硬件清单**技术能力的方案。 • 这些方案包括：Open-AudIT、Nmap、LANSweeper、Spiceworks、OCSinventory-ng 和 Excel（人工输入）。 • 用例中实施的方案：Open-AudIT
		ID.AM-2	**低** • 列出当前制造系统的软件组件。 • 制造系统软件组件包括软件证书信息、软件版本号、人机界面（HMI）及其他工控系统（ICS）组件应用、软件和操作系统。应按组织规定对系统软件清单进行评审和更新。	针对这些子类，可采取具有**软件清单**技术能力的方案。 • 这些方案包括：Open-AudIT、Nmap、LANSweeper、Spiceworks、OCSinventory-ng 和 Excel（人工输入）。 • 用例中实施的方案：Open-AudIT
		ID.AM-3	**低** • 明确制造系统内部的所有连接以及制造系统和其他系统之间的连接。对各个连接进行记录、授权和检查。 • 连接信息包括接口特征、数据特征、端口、协议、地址、数据描述、安全要求以及连接性质。	针对这类需求，可采用具有以下技术能力的方案：**网络架构文档、配置管理、基线构建**和**绘制数据流。** • 这些方案包括：GRASSMARLIN、Microsoft Visio、Wireshark、Nmap、Open-AudIT、Tenable Nessus 和 Ntopng • 用例中实现的方案：GRASSMARLIN、Microsoft Visio Wireshark、Open-AudIT
		ID.AM-4	**低** • 识别并列明制造系统的所有外部连接。 • 外部系统包括工程设计服务、单独授权的服务、个人设备和其他托	针对这类需求，可采用具有以下技术能力的方案：**网络架构文档、配置管理、**和**绘制数据流**。 • 这些方案包括：GRASSMARLIN、Microsoft Visio、Wireshark、Nmap、Open-AudIT、Tenable Nessus 和 Ntopng

功能	大类	子类	制造篇	实施概要
			管的服务。	• 用例中实现的方案：GRASSMARLIN、Microsoft Visio Wireshark、Open-AudIT
		ID.AM-5	**低** • 按类别、重要性和业务价值列出制造系统组件和功能，确定优先级。 • 明确需对所拥有、保管或控制的哪种信息（如敏感信息或受保护信息）采取安全保障措施。	针对这类需求，可在**《风险管理》**文档中的**“资产重要性矩阵”**一节中加入政策和程序描述。
		ID.AM-6	**低** • 确定和维护制造系统的员工网络安全角色和责任，包括第三方提供商的网络安全角色和责任。 • 对制造系统组件有物理或逻辑访问权限的人员发生变更（如转岗或合同终止）后，第三方提供商应及时通知组织。 • 第三方提供商包括服务提供商、承包商以及提供制造系统开发、技术服务、外包应用或网络和安全管理服务的其他组织。	针对这类需求，可在网络安全政策文档的**“基于角色的安全职责”**制定政策和程序。
	业务环境（ID.BE）	ID.BE-1	**低** • 明确并传达组织在供应链中的角色。明确组织的外部上下游供应渠道。确定制造系统支撑的总体业务。	针对这类需求，可在**《网络安全计划》**的**“组织概述”**一节中制定政策和程序。
		ID.BE-2	**低** • 明确并传达制造商在关键基础设施及其行业部门内的地位。 • 明确并传达制造系统相关的关键基础设施和关键资源。制定关键基础设施和关键资源保护计划，形成文件，并进行维护。	针对这类需求，可在**《网络安全计划》**的**“组织概述”**一节中制定政策和程序。
		ID.BE-3	**低** • 明确并传达生产运营的优先级别、目标和活动，纳入安全考虑，以及对生产运营、组件和个人带来的风险。 • 通过重要性分析，确定制造系统中的关键组件和功能。	针对这类需求，可在**《网络安全计划》**的**“组织概述”**一节中制定政策和程序。
		ID.BE-4	**低** • 明确关键制造系统流程和组件所需的支撑	针对这类需求，可在**《网络安全计划》**的**“组织概述”**和**“应急能力”**章节制定政策和

功能	大类	子类	制造篇	实施概要
			服务，理清这些服务的优先顺序。 • 为已确定的关键制造系统组件提供不间断电源，便于制造系统在主电源故障时切换到长期的备用电源。	程序。
		ID.BE-5	低 • 明确制造系统为支持关键服务的交付需满足的恢复要求。	针对这类需求，可在**《系统恢复》**中制定政策和程序。
	治理（ID.GV）	ID.GV-1	低 • 制定并宣传全面介绍制造系统安全要求的安全政策。该政策包括角色定义和分配、责任、管理承诺、各组织实体之间的协调以及合规，要反映出负责各安全方面（如技术、物理、人员、网络/物理、访问控制、媒体保护、漏洞管理、维护和监控）的组织实体之间进行的协调，并且覆盖制造系统的整个生命周期。根据需要，对安全政策进行评审和更新。 • 确保安全政策得到对生产运营承担责任和义务的高级管理人员的批准。	针对这类需求，可在**《网络安全政策》**中制定政策和程序。
		ID.GV-2	低 • 制定和宣传制造系统的安全计划。该计划包括人员的安全角色、职责划分、管理承诺、组织实体之间的协调和合规。该计划还涵盖第三方提供商的安全要求、角色和责任。应按组织规定对安全计划进行评审和更新。	针对这类需求，可在**《网络安全计划》**中制定政策和程序。
		ID.GV-3	低 • 确保充分了解和管理对生产运营产生影响的网络安全法律和法规。	针对这类需求，可在**《网络安全计划》**的**“适用法律和法规”**一节中制定政策和程序。
		ID.GV-4	低 • 制定全面的生产运营风险管理战略，将网络安全纳入该战略。应按规定对风险管理战略进行评审和更新。 • 明确并分配保护制造系统所需的资源。	针对这类需求，可在**《风险管理》**中制定政策和程序。
	风险评估（ID.RA）	ID.RA-1	低 • 制定计划，对制造系统	针对这类需求，可采用具有风险评估和

功能	大类	子类	制造篇	实施概要
			中存在的漏洞进行识别、记录和上报，包括在安全可行的情况下对制造系统、系统组件或典型系统进行漏洞扫描。	漏洞扫描和**漏洞管理**技术能力的方案。 这些方案包括：DHS 网络安全评估工具（CSET）、NamicSoft、OpenVAS、Tenable Nessus、AlienVault OSSIM 和 Microsoft Excel（手动）。 用例中实施的方案：CSET NamicSoft Tenable Nessus 针对其中一些子类的需求，可在**《网络安全运营》**的**“漏洞管理”**一节中加入政策和程序描述。
		ID.RA-2	**低** • 建立并保持与安全组织和协会的持续联系，获得安全告警和通告。安全组织和协会包括特殊利益群体、论坛、专业协会、新闻组和/或相似组织内安全从业人员组成的同行小组。制定威胁感知计划，包括组织之间的信息分享能力。组织应考虑构建对保密信息和非保密信息的共享能力。 • 针对潜在漏洞和事件，及时开展协作并共享信息。国土安全部的国家网络安全和通信集成中心（NCCIC）[6]对依赖于网络安全和通信的业务元素进行集中协调和整合。工控系统网络应急响应小组（ICS-CERT）[7]与国际和私营部门的计算机应急响应小组（CERT）合作，对控制系统相关的安全事件和缓解措施进行分享。	针对这类需求，可在以下章节中加入政策和程序描述：**《网络安全计划》**的**“信息共享计划”**和**“安全感知培训”**章节、**《风险管理》**的**“风险识别”**一节以及**《事件响应计划》**中的**“信息分享政策”**一节。
		ID.RA-3	**低** • 定期评估制造系统面临的风险并输出文档，包括生产运营和资产所面临的威胁和威胁的潜在影响。这里的威胁指内外部威胁。	针对这类需求，可通过在**《风险管理》**的**“风险、监控和控制”**一节中加入政策和程序描述。
		ID.RA-4	**低** • 对制造系统进行重要性分析，评估生产运营、资产和人员遭遇入侵或重创时会带来的不利影响。	针对这类需求，可在**《风险管理》**的**“定期审查”**一节中加入政策和程序说明。
		ID.RA-5	**低** • 对制造系统进行风险评估，包括生产运营、资产和人员所面临的	针对这类需求，可在**《风险管理》**的**“风险监控和控制”**和**“风险上报”**一节中加入政策和程序说明。

功能	大类	子类	制造篇	实施概要
			威胁、漏洞、威胁发生的可能性及影响。将风险评估结果发送给利益相关方。	
		ID.RA-6	**低** • 制定并实施全方位战略，对制造系统面临的风险进行管理，包括明确风险响应并对其进行优先级排序。	针对这类需求，可在**《风险管理》**中加入政策和程序说明。
	风险管理战略(ID.RM)	ID.RM-1	**低** • 建立制造系统的风险管理流程，有效识别和辅助解决风险相关问题和信息，并将其传达给内外部关键利益相关方。	针对这类需求，可在**《风险管理》**的**“风险通知流程”**一节中加入制定政策和程序说明。
		ID.RM-2	**低** • 明确制造系统的风险承受能力。	针对这类需求，可在**《风险管理》**的**“风险容忍度”**一节中加入政策和程序说明。
		ID.RM-3	**低** • 基于组织在关键基础设施和相关行业风险分析中的角色，确定制造系统的风险承受能力。	针对这类需求，可在**《风险管理》**的**“风险容忍度”**一节中加入政策和程序说明。
防护	**访问控制（PR.AC）**	PR.AC-1	**低** • 构建和管理用户和制造系统的识别机制和凭证。	针对这类需求，可采用具有以下技术能力的方案：**凭证管理、认证和授权、和系统使用监控。** 这些方案包括：Microsoft Active Directory、FreeIPA、OpenLDAP、或本机操作系统/设备能力。 用例中实施的方案：Microsoft Active Directory、本机操作系统/设备能力
		PR.AC-2	**低** • 对制造设施的物理访问进行防护。明确紧急情况下的访问要求。 • 维护并审查访客对制造系统所在设施访问的记录。 • 物理访问控制措施包括获得授权的人员名单、身份凭证、陪同要求、保安、围栏、十字转门、门锁、对设施访问的监控。	针对这类需求，可采用具有以下技术能力的方案：**物理访问控制**和**物理访问监控。** 这些方案包括： 获得授权的人员名单、登录/登出记录表、身份凭证、陪同要求、保安、围栏、十字转门、门锁、电子访问控制系统、摄像头和设施访问监控。 用例中实施的方案：锁、围栏、电子访问控制系统 、登录/登出记录表
		PR.AC-3	**低** • 明确制造系统的使用限制、连接要求、实施指南以及远程访问授权。 • 标明接触设备的用户存在的活动远程连接。 • 远程访问方法包括无线、拨号、宽带、VPN 连接、移动设备连接以	针对这类需求，可在网络安全政策文档中的**远程访问**一节中加入政策和程序描述。

功能	大类	子类	制造篇	实施概要
			及通过外部网络的通信。	
		PR.AC-4	**低** • 对制造系统的用户访问权限进行定义和管理。明确并记录用户对制造系统的哪些操作无需身份证明或认证（如紧急情况下）。	针对这类需求，可在**《网络安全运营》**中的**“人员行为”**一节加入政策和程序描述。
		PR.AC-5	**低** • 保护制造系统的网络完整性，在适当情况下进行网络分段和隔离。识别和控制系统组件之间的连接。对制造系统的外部边界和关键内部边界的连接和通信进行监控和控制。部署边界保护设备。 • 边界防护机制包括路由器、网关、单向网关、数据二极管以及防火墙（将系统组件划分为多个逻辑独立网络或子网）。	针对这类需求，可采取具有以下技术能力的方案解决：**网络分段和隔离、网络边界防护、远程安全接入、管理网络接口和绘制数据流。** 这些方案包括：路由器、网关、单向网关、数据二极管、防火墙、DMZ、交换机、Snort、BRO、VPN、远程桌面、本机操作系统/设备能力、GRASSMARLIN、Microsoft Visio、Wireshark 和 Ntopng。 用例中实施的方案：路由器、防火墙、DMZ、交换机 、VPNs、TeamViewer、本机操作系统/设备能力 、GRASSMARLIN、Microsoft Visio、Wireshark
	意识与培训（PR.AT）	**PR.AT-1**	**低** • 对制造系统用户和管理人员进行安全意识培训。 • 培训内容包括用以保障系统安全的防护措施及用户行为的基本知识、对疑似网络安全事件的响应以及运营安全意识等。	针对这类需求，可在**《网络安全计划》**的**“安全意识培训”**一节加入政策和程序描述。
		PR.AT-2	**低** • 确保对制造系统拥有特权访问权限的用户了解其业务的需求和责任。 • 制定标准，对特权用户访问权限进行评估、配置和验证。	针对这类需求，可在**《网络安全计划》**的**“安全意识培训”**一节中加入政策和程序描述。
		PR.AT-3	**低** • 明确和实施针对第三方提供商和用户的安全需求。确保第三方提供商了解其在制造系统安全方面的责任和业务职责。对制造系统组件具备物理或逻辑权限的任何人员发生变动时，要求发送通知。 • 确保外部系统服务的提供商符合规定的安全需求。对外部服务提供商进行监控和评估，确保其满足安全合规要求。	针对这类需求，可在**《网络安全计划》**的**“安全意识培训和第三方责任和要求”**一节中加入政策和程序描述。
		PR.AT-4	**低**	

功能	大类	子类	制造篇	实施概要
			• 确保高管了解制造系统的安全和保护要求及其要承担的安全防护职责。	针对这类需求，可在**《网络安全计划》**的**“管理层承诺”**一节中加入政策和程序描述。
		PR.AT-5	**低** • 对负责制造系统的物理保护和安全的人员进行培训，确保其了解自身职责。 • 制定标准，对物理安全人员的访问权限进行评估、配置和验证。	针对这类需求，可在网络安全政策文档中的**“员工要求”**一节中加入政策和程序描述。
	数据安全（PR.DS）	**PR.DS-1**	**低** 无	无
		PR.DS-2	**低** 无	无
		PR.DS-3	**低** • 在制造系统的整个生命周期内实施系统组件责任制，例如组件拆卸、调换和处置。 • 在对移动媒体进行处置、释放或重用时应进行数据销毁。系统组件出入厂区时，均需授权、监控和控制，并维护组件记录。	针对其中一些这类需求，可采取提供以下能力的方案：**硬件清单、软件清单、系统开发生命周期管理**和**媒体过滤。** 这些方案包括：Open- AudIT、LANSweeper、Spiceworks、OCSinventory-ng、AlienVault OSSIM、MS Excel (Manual)和媒体过滤工具。 用例中实施的方案：Open-AudIT DBAN 针对其中一些这类需求，可在**《网络安全政策》**的**“设备生命周期责任制”**一节和**《网络安全运营》**的**“媒体过滤”**一节中加入政策和程序描述。
		PR.DS-4	**低** • 确保维持足够的资源进行制造系统信息处理、联网、通信和数据存储。 • 从制造系统中下载要处理的审计记录，存储至备用系统。	针对这类需求，可在**《网络安全运营》**的**“制造系统监控”**和**“维持资源”**章节中加入政策和程序描述。
		PR.DS-5	**低** • 防止制造系统发生数据泄露。 • 监控制造系统的外部边界和内部关键点，对非授权访问和使用进行检测。 • 制定面向制造系统所有用户的书面访问协议。	针对其中一些这类需求，可采取具有以下能力的方案：**网络监控、系统使用监控、物理访问控制、加密**和**数据泄露防护。** 这些方案包括：安全洋葱（Security Onion）、Snort、Suricata、Zeek 网络安全监控器、本机操作系统/设备能力、获得授权的人员名单、登录/登出记录表、身份凭证、陪同要求、保安、围栏、十字转门、门锁、电子访问控制系统、摄像头、设施访问监控、Microsoft EFS、Microsoft BitLocker、AxCrypt、VeraCrypt、GTB Inspector 和 Comodo DOME。 用例中实施的方案：安全洋葱（Security Onion）、Microsoft EFS、门锁、围栏、Electronic Access Control System、登录/登出记录表、GTB Inspector、VeraCrypt 针对其中一些这类需求，可在《网络安全政策》中的“用户访问协议”一节中加入政

功能	大类	子类	制造篇	实施概要
				策和程序描述。
		PR.DS-6	**低**	无
			无	
		PR.DS-7	**低**	无
			无	
	信息保护流程与程序（PR.IP）	**PR.IP-1**	**低** • 明确制造系统的基线配置，形成文档，并对该配置进行维护。 • 基线配置包括制造系统组件信息（例如软件许可证信息、软件版本号、人机界面（HMI）和其他ICS组件的应用程序、软件和操作系统、操作系统和应用程序的当前版本号和补丁信息；配置设置/参数）、网络拓扑，以及这些组件在系统架构中的逻辑位置。 • 配置制造系统，仅保证提供基本能力。检查基线配置，禁用不必要的能力。	针对这类需求，可采取具有以下技术能力的方案：**系统开发生命周期管理、配置管理、建立基线、变更控制、和配置备份、端口**和**服务锁定。** 这些方案包括：Open- AudIT、LANSweeper、Spiceworks、OCSinventory-ng、Microsoft Excel（手动）、I-doit、Salt、Puppet、Ansible、GRASSMARLIN、Wireshark、Nmap 和 Native 操作系统/设备能力 用例中实施的方案：Open-AudIT、Microsoft Excel、GRASSMARLIN、Wireshark、本地操作系统/设备能力
		PR.IP-2	**低** • 采取纳入安全考虑的系统开发生命周期对制造系统进行管理。 • 将安全要求纳入制造系统及其组件的采购流程。	针对这类需求，可采取提供**系统开发生命周期管理**技术能力的方案。 这些方案包括：Open- AudIT，LANSweeper、Spiceworks、OCSinventory-ng 和 Microsoft Excel（手动） 用例中实施的方案：Open-AudIT
		PR.IP-3	**低** • 对制造系统及其组件实施配置变更控制。 • 分析变更控制评审带来的安全影响。	针对其中一些这类需求，可采取提供**变更控制**技术能力的方案。 这些方案包括：Open- AudIT、GRASSMARLIN、Wireshark、I-doit、Salt、Puppet 和 Ansible。 用例中实施的方案：Open-AudIT、GRASSMARLIN、Wireshark 针对其中一些这类的需求，可在《**网络安全运营**》的**“变更控制”**一节中加入政策和程序描述。
		PR.IP-4	**低** • 对制造系统数据进行备份并维护备份数据。 • 制造系统数据包括软件、配置和设置、文档和系统配置数据（如计算机配置备份、应用配置备份以及所有ICS可编程设备的操作控制界限、控制范围和事前操作设定点）。	针对这类需求，可采用具有以下技术能力的方案：**配置管理、变更控制、配置备份、数据备份**和**数据复制。** 这些方案包括：Open- AudIT、I-doit、Salt、Puppet、Ansible、Veeam Backup and Replication、Bacula Systems、Clonezilla、Commvault Backup & Recovery、Redo backup 和本机操作系统/设备能力。
		PR.IP-5	**低**	

功能	大类	子类	制造篇	实施概要
			• 为制造系统制定、落实、实施有关消防系统和环境控制措施的政策和规定。 • 消防机制应将制造环境考虑在内（如喷水系统可能会为特定环境带来损害）。	针对这类需求，可在**《网络安全计划》**的**"消防条例"**一节中加入政策和程序描述。
		PR.IP-6	**低** • 确保按照政策销毁制造系统数据。	这针对这类需求，可采取具有**系统开发生命周期管理**和**媒体过滤**技术能力的方案。 这些方案包括：Open- AudIT、LANSweeper、Spiceworks、OCSinventory-ng、AlienVault OSSIM、Microsoft Excel（手动）和媒体过滤工具。 用例中实施的方案：Open-AudIT、DBAN
		PR.IP-7	**低** • 修改保护流程时应纳入通过监控、统计、评估以及总结的经验教训得到的改进。	针对这类需求，可在**《网络安全计划》**的**"定期计划复审"**一节中加入政策和程序描述。
		PR.IP-8	**低** • 对于制造系统的安全事件和缓解措施的相关信息，与特定的合作伙伴进行信息协同和分享。 • 在可行的情况下，采取自动化机制，促进信息协同。	针对这类需求，可在**《事件响应计划》**的**"信息分享政策"**一节中加入政策和程序描述。
		PR.IP-9	**低** • 制定并维护响应和修复计划，明确基本功能和相关应急需求，并提供事件响应路线图。这些计划包括恢复目标、还原优先级、指标、应急角色、人员分配和联系信息。即使在制造系统中断时也要确保维持其基本功能，并最终完成系统还原。 • 定义事件类型并明确维持和完善事件响应和应急能力所需的资源和管理支持。	针对这类需求，可在**《事件响应计划》**和**《系统恢复计划》**中加入政策和程序描述。
		PR.IP-10	**低** • 审核响应和恢复计划，评估这些计划是否有效以及计划执行的准备度。	针对这类需求，可在**《网络安全计划》**的**"事件管理"**一节中加入政策和程序描述。
		PR.IP-11	**低**	

功能	大类	子类	制造篇	实施概要
			• 制定和维护关于制造系统的人员安全计划，该计划应包括政策、岗位风险描述、人员筛选、转岗和离职、访问协议、第三方角色和责任以及人员制裁。	针对这类需求，可在**《网络安全计划》**中加入政策和程序描述。
		PR.IP-12	**低** • 制定和维护流程，确保对漏洞进行持续审核，并制定漏洞缓解策略。	针对这类需求，可在**《网络安全运营》**的**"漏洞管理"**一节中加入政策和程序描述。
	维护（PR.MA）	**PR.MA-1**	**低** • 制定制造系统组件的维护和维修计划，按计划执行任务，并做好记录和记录评审。 • 建立维护人员授权流程，非授权维护人员须在陪同下执行任务。 • 确认维护或维修会影响哪些安全控制措施。	针对其中一些这类的需求，可采取具有以下技术能力的方案：**配置管理、变更控制、凭证管理、认证和授权、维护跟踪**和**物理访问控制。** 这些方案包括：Open- AudIT、I-doit、Salt、Puppet、Ansible、GRASSMARLIN、Wireshark、Microsoft Active Directory、FreeIPA、OCSinventory-ng、Fiix、Freshservice 和 Microsoft Excel。 用例中实施的方案：Open-AudIT、Microsoft Excel GRASSMARLIN、Wireshark、Microsoft Active Directory 针对其中一些这类的需求，可在**《网络安全政策》**的**"物理安全"**和**"系统维护"**章节中加入政策和程序描述。
		PR.MA-2	**低** • 确保对远程维护活动进行审批，对此类活动进行监控和控制。 • 对于远程维护，加强认证，做好记录，并妥善终止会话。	针对其中一些这类的需求，可采取具有以下能力的方案：**远程安全访问、凭证管理、认证和授权、网络监控、系统使用监控**和**维护跟踪。** 这些方案包括：VPN、远程桌面、Microsoft Active Directory、FreeIPA、OCSinventory-ng、Fiix、Freshservice、Microsoft Excel 和本地操作系统/设备能力。 用例中实施的方案： Cisco AnyConnect VPN、TeamViewer、Microsoft Active Directory Microsoft Excel、本机操作系统/设备能力 针对其中一些这类的需求，可在**《网络安全政策》**的**"远程维护"**和**"系统维护"**章节中加入政策和程序描述。
	防护技术（PR.PT）	**PR.PT-1**	**低** • 对审计进行记录，明确事件类型、发生时间和地点、事件源、事件结果、事件相关人员或制造组件的ID。 • 根据以国际协调时间（UTC）或格林尼治（GMT）标准时间为准的内部系统时钟生成时间戳。	针对这类需求，可采用具有以下技术能力的方案：**时间同步、物理访问监控**和**事件日志。** 这些方案包括：本机操作系统/设备能力、电子访问控制系统、登录/登出记录单、摄像头、Graylog、Alienvault – OSSIM 和 SIEMonster。 用例中实施的方案：本机操作系统/设备能力、电子访问控制系统、登录/登出记录表

功能	大类	子类	制造篇	实施概要
		PR.PT-2	低 • 采取防护措施限制便携式存储设备的使用。	针对这类需求，可采取具有**媒体保护**技术能力的方案。 这些方案包括：USB 端口锁，本机操作系统/设备能力 用例中实施的方案：USB 端口锁
		PR.PT-3	低 • 配置制造系统，仅保证提供基本能力。	针对这类需求，可采用具有以下技术能力的方案：**认证和授权**和**端口和服务锁定**。 这些方案包括：Microsoft Active Directory、FreeIPA、Nmap、本机操作系统/设备能力。 用例中实施的方案：Microsoft Active Directory、本机操作系统/设备能力
		PR.PT-4	低 • 对制造系统的外部边界和关键内部边界的通信进行监控和控制。	针对这类需求，可采用具有以下技术能力的方案：**网络边界保护、认证和授权**和**网络监控。** 针对这类需求，可采用具有以下技术能力的方案：防火墙、安全洋葱（Security Onion）、Snort、Suricata、Zeek 网络安全监控器、Microsoft Active Directory 和 FreeIPA 用例中实施的方案：Microsoft Active Directory、安全洋葱（Security Onion）、防火墙
检测	**异常与事件（DE.AE）**	DE.AE-1	低 • 针对制造系统的网络操作及期望数据流，设定基线，做好基线记录和维护，方便事件检测。	针对这类需求，可采用具有**建立基线和绘制数据流**技术能力的方案。 这些方案包括：Open- AudIT、GRASSMARLIN、Wireshark、I-doit、Salt、Puppet、Ansible、Microsoft Visio 和 Ntopng 用例中实施的方案：Open-AudIT、GRASSMARLIN、Wireshark Microsoft Visio
		DE.AE-2	低 • 查看和分析在制造系统内发现的事件，了解攻击目标和攻击方法。	针对这类需求，可采用具有**取证**技术能力的方案。 这些方案包括：Graylog、Wireshark、安全洋葱（Security Onion）、Zeek 网络安全监控器和计算机辅助调查环境（CAINE）。 用例中实施的方案：Graylog、Wireshark、安全洋葱（Security Onion）
		DE.AE-3	低 • 输出整个制造系统的事件数据，可参考事件报告、审计监控、网络监控、物理访问监控和用户/管理员报告等。	针对这类需求，可采用具有**事件日志**技术能力的方案。 这些方案包括：Graylog，Alienvault – OSSIM，SIEMonster 用例中实施的方案：Graylog
		DE.AE-4	低 • 明确检测到的事件对生产运营、资产和人员带来的不利影响，然后与风险评估结果相关联。	针对这类需求，可在**《网络安全运营》的"制造系统监控"**一节中加入政策和程序描述。

功能	大类	子类	制造篇	实施概要
		DE.AE-5	**低** • 确定制造系统的事件告警阈值。	针对其中一些这类的需求，可在**《事件响应计划》**中加入政策和程序描述。
	持续性安全监控（DE.CM）	DE.CM-1	**低** • 对制造系统网络的当前安全状态进行监控，检测已知网络安全事件以及潜在网络安全事件迹象。 • 检测未授权的本地连接、网络连接和远程，识别对制造系统的非法使用行为。 • 对定义的网络安全事件生成审计记录。 • 监控制造系统的外部边界和内部关键边界的网络通信。	针对这类需求，可采取具备以下技术能力的方案：**网络边界保护、网络监控**和**事件日志。** 这些方案包括：防火墙、安全洋葱（Security Onion）、Snort、Suricata、Zeek 网络安全监控器 Graylog、Alienvault – OSSIM 和 SIEMonster。 用例中实施的方案：防火墙、安全洋葱（Security Onion）、Graylog 针对其中一些这类需求，可在**《网络安全政策》**中的**"持续监控"**一节中加入政策和程序描述。
		DE.CM-2	**低** • 持续监控制造系统设施的安全状态，检测物理安全事件。	针对这类需求，可采取具有**物理访问监控**技术能力的方案。 这些方案包括：电子访问控制系统、摄像头和登录/登出记录表 用例中实施的方案：电子访问控制系统、登录/登出记录表
		DE.CM-3	**低** • 对员工在制造系统上的活动进行安全状态监控。 • 实施软件安装及利用限制。	针对这类需求，可采取具备以下技术能力的方案：**认证和授权、系统使用监控和物理访问监控。** 这些方案包括：Microsoft Active Directory、FreeIPA、赛门铁克端点防护、国产操作系统/设备能力、电子访问控制系统、摄像头和登录/登出记录表 用例中实施的方案：Active Directory、赛门铁克端点防护、本机操作系统/设备能力 、电子访问控制系统、登录/登出记录表
		DE.CM-4	**低** • 在安全可行的情况下，在整个制造系统中部署恶意代码保护机制，检测并删除恶意代码。 • 在新版本发布时，根据制造系统的配置管理政策和程序，更新恶意代码保护机制。	针对这类需求，可采取具有**防病毒/恶意软件和漏洞管理**技术能力的方案。 这些方案包括：Symantec Endpoint Protection，ClamAV，NamicSoft，OpenVAS，Tenable Nessus 用例中实施的方案：赛门铁克端点防护、NamicSoft
		DE.CM-5	**低** 无	无
		DE.CM-6	**低**	

功能	大类	子类	制造篇	实施概要
			• 对外部服务提供商在制造系统上的活动持续进行安全状态监控。 • 对于外部服务提供商，检测已知网络安全事件以及潜在网络安全事件的迹象。 • 对外部提供商的合规情况进行监控，使其符合人员安全政策和程序以及合同安全要求。	针对这类需求，可采取具有**网络监控和事件日志**技术能力的方案。 这些方案包括：安全洋葱（Security Onion）、Snort、Zeek 网络安全监控器、Graylog、Alienvault – OSSIM 和 SIEMonster。 用例中实施的方案：安全洋葱（Security Onion）、Graylog
		DE.CM-7	**低** • 对制造系统的未授权人员、连接、设备、访问点和软件持续进行安全状态监控。 • 对系统清单与实际情况的出入进行监控。	针对这类需求，可采取具有以下技术能力的方案：**硬件清单、软件清单、系统开发生命周期管理、建立基线、变更控制和网络监控。** 这些方案包括：Open- AudIT、LANSweeper、Spiceworks、OCSinventory-ng、AlienVault OSSIM、Microsoft Excel（手动）、I-doit，Salt、Puppet、Ansible、GRASSMARLIN、Wireshark、安全洋葱（Security Onion）、SNORT、Suricata 和 Zeek 网络安全监控器 用例中实施的方案：Open-AudIT、GRASSMARLIN、Wireshark 、Microsoft Excel、安全洋葱（Security Onion）
		DE.CM-8	**低** • 在安全可行的情况下，对制造系统进行漏洞扫描。在漏洞扫描过程中，进行漏洞分析、修复和信息共享。 • 在安全可行的情况下，采取控制系统专用的漏洞扫描工具和技术。 • 由于主动漏洞扫描会产生网络流量，因此需确保漏洞扫描过程不会对系统功能带来不利影响。	针对其中一这类需求，可采取具备**漏洞扫描**能力的方案。 这些方案包括：Tenable Nessus、OpenVAS 和 AlienVault OSSIM 用例中实施的方案：Tenable Nessus 针对其中一这类需求，可在**《网络安全运营》**的**“漏洞管理”**一节加入政策和程序描述。
	检测流程（DE.DP）	**DE.DP-1**	**低** • 定义在制造系统上进行检测活动的角色和职责，确保可问责到人。	针对这类需求，可在《网络安全政策》的**《基于角色的安全职责》**一节中加入政策和程序描述。
		DE.DP-2	**低** • 确保检测活动符合适用的联邦和州法律、行业法规和标准、政策以及其他适用的要求。	针对这类需求，可在**《网络安全政策》**中的**“持续监控”**一节中加入政策和程序描述。
		DE.DP-3	**低、中等和高** • 确保事件检测流程按预期正常运转。	针对这类需求，可采取提供**事件日志**技术能力的方案 这些方案包括：Graylog，Alienvault – OSSIM 和 SIEMonster 用例中实施的方案：Graylog
		DE.DP-4	**低**	

功能	大类	子类	制造篇	实施概要
			• 向指定人员传达事件检测信息。 • 事件检测信息包括常规账户使用告警、未授权的远程访问、无线连接、移动设备连接、配置修改、与系统组件清单进行对比、维护工具使用以及非本地维护、物理访问、温度与湿度、设备交付和移除、信息系统边界的通信、移动代码使用、VoIP的使用以及恶意软件披露。	针对这类需求，可在**《网络安全政策》**的**“持续监控”**一节中加入政策和程序描述。
		DE.DP-5	**低** • 检测流程修改要涵盖监控、评测、评估方面的改进以及经验教训。 • 确保制造系统安全计划纳入安全检测流程的评审、测试和持续改进。	针对这类需求，可在**《网络安全计划》**的**“事件管理”**和**“定期计划重审”**章节中加入政策和程序描述。
响应	**响应计划（RS.RP）**	**RS.RP-1**	**低** • 在制造系统发生网络安全事件时或之后，执行响应计划。	针对这类需求，可在**《事件响应计划》**的**“目的和范围”**一节中加入政策和程序描述。
	沟通（RS.CO）	**RS.CO-1**	**低** • 确保员工了解事件响应的目标、恢复优先级、任务执行顺序以及责任分工。	针对这类需求，可在**《事件响应计划》**的**“策略”**一节中加入政策和程序描述。
		RS.CO-2	**低** • 对涉及的利益相关方及时汇报制造系统的网络安全事件。 • 确保按照响应计划汇报制造系统的网络安全事件。	针对这类需求，可在**《事件响应计划》**的**“内外部沟通”**一节中加入政策和程序描述。
		RS.CO-3	**低** • 与每个响应计划涉及的利益相关方分享网络安全事件信息。	针对这类需求，可在**《事件响应计划》**的**“内外部沟通政策”**一节中加入政策和程序。
		RS.CO-4	**低** • 关于网络安全事件响应行动，与所有利益相关方协调一致。 • 事件响应利益相关方包括任务/业务负责人、制造系统负责人、集成商、厂商、人力资源办公室、物理和人员安全办公室、法务部门、运营人员和采购办公室。	针对这类需求，可在**《事件响应计划》**的**“内外部沟通”**一节中加入政策和程序描述。
		RS.CO-5	**低**	

功能	大类	子类	制造篇	实施概要
			• 适当时主动与行业安全组织分享网络安全事件信息，实现更广泛的网络安全态势感知。 • 国土安全部的国家网络安全和通信集成中心（NCCIC）[6]对依赖于网络安全和通信的业务元素进行集中协调和整合。工控系统网络应急响应小组（ICS-CERT）[7]与计算机应急响应小组（CERT）合作，对控制系统相关的安全事件和缓解措施进行分享。	针对这类需求，可在**《网络安全政策》**的**“持续监控”**一节中加入政策和程序描述。
	分析（RS.AN）	**RS.AN-1**	**低** • 查看检测系统生成的网络安全相关通知。	针对这类需求，可在**《网络安全运营》**的**“制造系统监控”**一节中加入政策和程序描述。
		RS.AN-2	**低** • 通过深入的调查取证和分析，全面了解网络安全事件。 • 将检测到的事件信息和事件响应与风险评估结果相关联，了解事件对整个组织的影响。	针对这类需求，可在**《事件响应计划》**的**“政策”**一节中制定政策和程序描述。
		RS.AN-3	**低** • 对收集的网络安全事件信息进行取证分析，查明事件的根本原因。	针对这类需求，可采取具备**事件日志和取证**技术能力的方案。 这些方案包括：Graylog、Wireshark、Zeek 网络安全监控器、计算机辅助调查环境（CAINE）、Alienvault – OSSIM、SIEMonster 和安全洋葱（Security Onion）。 用例中实施的方案：Graylog、Wireshark、和安全洋葱（Security Onion）。
		RS.AN-4	**低** • 根据响应计划中规定的严重性和影响对网络安全事件进行分类。	针对这类需求，可在**《事件响应计划》**中的**“事件严重性划分”**一节中添加政策和程序描述。
	缓解（RS.MI）	**RS.MI-1**	**低** • 对网络安全事件进行控制，尽可能减少对制造系统的影响。	针对这类需求，可在**《事件响应计划》**的**“事件响应流程”**一节中添加政策和程序描述。
		RS.MI-2	**低** • 对制造系统中发生的网络安全事件进行缓解。	针对这类需求，可采取具备**事件管理**技术能力的方案。 这些方案包括：Sandia Cyber Omni Tracker (SCOT)、Hive 项目和事件响应请求跟踪器(RTIR)。 用例中实现的方案：Hive 项目。
		RS.MI-3	**低** • 在网络安全事件响应过程中，对发现的漏洞进行缓解或标识为可	针对这类需求，可采用具有**漏洞管理与事件管理**技术能力的方。 这些方案包括：NamicSoft、

功能	大类	子类	制造篇	实施概要
			接受风险。	OpenVAS、Tenable Nessus、AlienVault OSSIMSandia、Sandia Cyber Omni Tracker (SCOT)、Hive 项目和事件响应请求跟踪器(RTIR)。 用例中实现的方案：NamicSoft 和 Hive 项目。
	改进（RS.IM）	**RS.IM-1**	**低** • 将从当前的事件处理活动中总结的经验教训纳入事件响应流程、培训和测试中，并进行改进。	针对这类需求，可在**《事件响应计划》**中的**“政策”**一节中加入政策和程序描述。
		RS.IM-2	**低** • 更新响应计划，应对计划实施、执行或测试过程中引起的组织、制造系统、攻击向量、运行环境方面的变化以及导致的问题。 • 更新可包括对中断或故障作出响应并预先制定程序。 • 建立响应计划演进流程，纳入新威胁、改进的技术以及总结的教训和经验。	针对这类需求，可在**《事件响应计划》**的**“政策”**一节中加入政策和程序描述。
恢复	**恢复计划（RC.RP）**	**RC.RP-1**	**低** • 在制造系统发生网络安全事件时或之后，执行恢复计划。 • 在规定时间内，根据配置，利用受到完整性保护的信息，将制造系统恢复到事件前组件的已知正常运行状态。	针对这类需求，可在**《事件恢复计划》**的**“目标”**一节中加入政策和程序描述。
	改进（RC.IM）	**RC.IM-1**	**低** • 将从当前的事件处理活动中总结的经验教训纳入事件响应流程、培训和测试中，并进行改进。	针对这类需求，可在**《系统恢复计划》**的**“计划测试”**和**“计划维护”**章节中加入政策和程序描述。
		RC.IM-2	**低** • 更新恢复计划，应对计划实施、执行或测试过程中引起的组织、制造系统和运行环境方面的变化以及导致的问题。 • 确保这些更新纳入恢复计划。	针对这类需求，可在**《系统恢复计划》**的**“计划测试”**和**“计划维护”**章节中加入政策和程序描述。
		RC.CO-1	**低**	

功能	大类	子类	制造篇	实施概要
	沟通 (RC.CO)		• 对信息发布进行集中管理和协调，对组织公开发布的言论进行管控。 • 公共关系管理包括管理媒体互动、对所有访谈邀请进行协调和记录、对电话和邮件请求进行处理并分类、将媒体邀请知会对应的内部专家，使其准备接受采访，对提供给媒体的所有信息进行审查，并确保员工熟知公共关系和隐私政策。	针对这类需求，可在**《系统恢复计划》**中的**"内外部沟通"**一节中加入政策和程序描述。
		RC.CO-2	**低** • 采取危机响应策略，应对不利影响，挽救组织声誉。 • 危机响应策略涵盖采取的各种措施，如分析危机原因、改变人们对处于危机中的组织的看法以及降低危机带来的不利影响。	针对这类需求，可在**《系统恢复计划》**中的**"内外部沟通"**一节中加入政策和程序描述。
		RC.CO-3	**低** • 将恢复活动传达给涉及的所有利益相关方以及中高层管理团队。	针对这类需求，可在**《系统恢复计划》**中的**"内外部沟通"**一节中加入政策和程序描述。

8. 实验室环境概述

本节详细介绍位于马里兰州的盖瑟斯堡的国家标准和技术研究所（NIST）总部实验室环境（即实验室）。该实验室具有联网服务器组成的共享基础设施、评测工具、工业机器人、硬件在环仿真器等技术，为在两个制造系统（过程控制系统（PCS）[12]和协同机器人系统（CRS）[11]）上实现《制造篇》提供支持。PCS 和 CRS 利用工业硬件（如可编程逻辑控制器、机械手臂和传感器）、联网设备和工业协议模拟流程型制造系统和离散型制造系统。有关这两个系统详情，请参见 8.1 和 8.2 节。

图 8-1 所示的网络基础架构用于以下研究用途： 测试、部署和托管网络安全工具和网络流量评测系统、生成和操控用于触发异常网络活动的网络流量，以及存储实验数据文档。该架构使用了虚拟化环境，为构建该架构所需的大量网络安全技术和工具提供支持。

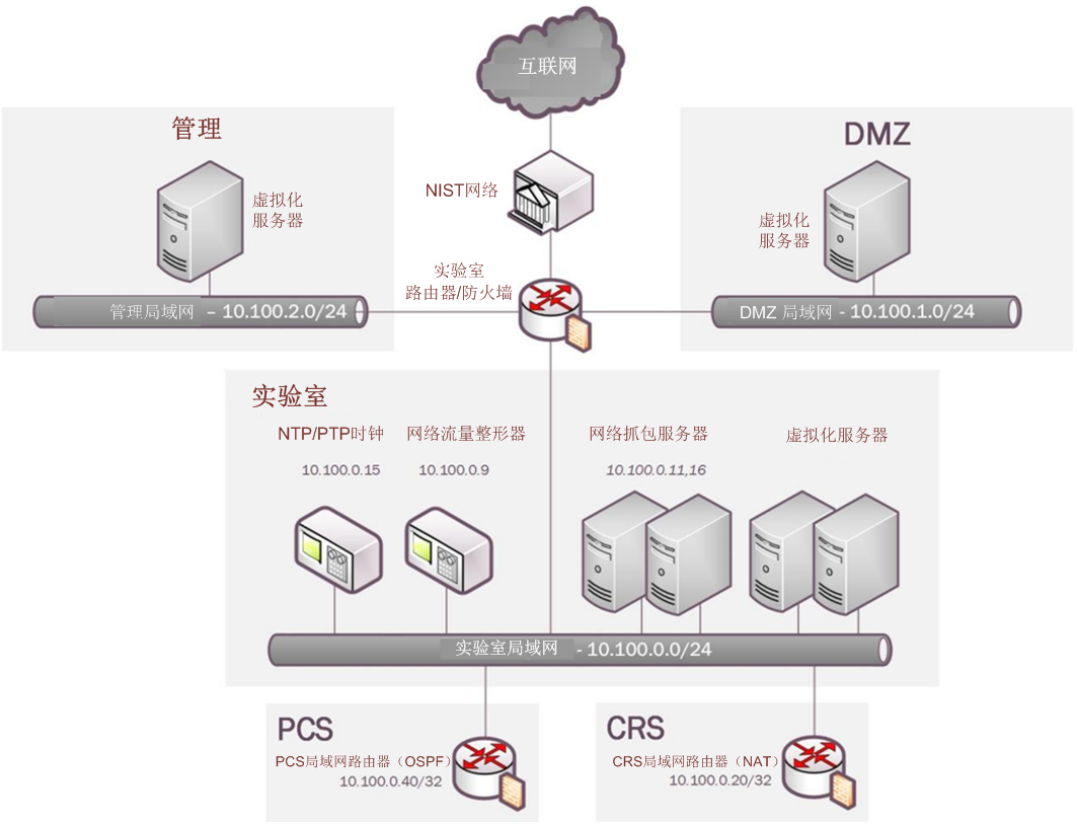

图 8-1 实验室网络基础架构

实验室网络基础架构可划分为三个独立的网络区域： 管理区、DMZ（非军事化）区和实验室区。管理区中的主机用于管理实验室设备（如网络硬件和虚拟化服务器）。DMZ 区的主机用于在实验室网络和顶层网络（NIST 网络）之间进行数据分享。实验室区包含可共享的评测服务器和工具以及用于托管网络安全工具的虚拟化架构。

实验室区连接本地 PCS 和 CRS 网络，这两种网络独立运行。PCS 网络通过开放式最短路径优先（OSPF）路由协议连接实验室局域网，而 CRS 网络通过动态网络地址转换技术（动态 NAT）连接实验室局域网。

PCS 和 CRS 网络中都具备专用网络抓包服务器。该服务器通过两种方式抓包：报文镜像和利用基于“线路插件”（bump-in-the-wire）技术的网络探针。要进行报文镜像，需配置网络设备（如路由器和交换机）对报文进行复制然后转发至另一端口。网络探针提供类似功能，但须通过线缆接入网络。在实验中，镜像的报文通过报文代理汇总为两种流（一种包含 PCS 流量，另一种包含 CRS 流量）。来自聚合器和

网络探针的网络流量最终到达网络抓包服务器，该服务器对这些报文进行缓存、存储并随即进行处理从而计算衡量指标和关键性能指标用于实验分析。

8.1 流程型制造系统

过程控制系统模拟工业连续制造系统，实现材料连续生产和加工制造过程。在该过程中，材料持续运动，发生化学反应或进行机械处理或热处理。从一般意义上说，连续制造指全天候（24/7）运行，基本不会因检修而停产，这与批量制造形成鲜明对比。例如，连续型制造系统可用于化工生产、炼油、天然气加工和废水处理。

过程控制系统（PCS）采取田纳西-伊斯曼挑战问题[9]（真实存在的化工生产过程）作为化学反应仿真模型。该系统集成了 Ricker[10]开发的控制算法用于控制模拟的化学反应。该系统采用可编程逻辑控制器（PLC）和工业网络交换机等广泛部署的工业硬件设备实现控制回路，对完整的连续型化工制造系统进行模拟。通过配置硬件在环（hardware-in-the-loop）技术，试验台可利用工业硬件设备评估制造系统的性能，并通过软件实现化工生产过程仿真。

图 8-2 PCS 系统

8.1.1 控制系统运行

过程控制系统（PCS）中内置一款软件模拟器，用于模拟田纳西-伊斯曼化学反应过程。模拟器采用 C 代码编写，在基于 Windows 7 的计算机上执行。此外，该系统还包括可编程逻辑控制器（PLC）、通过 MATLA 实现的软件控制器、人机界面（HMI）、OPC（过程控制的对象链接与嵌入技术）数据访问（DA）服务器、历史数据库、工程工作站和数台虚拟局域网（VLAN）交换机和网络路由器。PCS 部署在 19 英寸的机架系统中，如 8-2 图所示。

田纳西-伊斯曼工厂模拟器需要控制器实现控制回路，从而确保持续运营。Simulink 中实现的分散式控制器（由 Ricker [10]开发）可用作过程控制器。Ricker 实现精确匹配工厂模拟器，控制器作为独立软件过程，运行在单独的计算机上，而工厂模拟器运行在另一台计算机上。

要实现工厂模拟器和控制器之间的通信，需部署提供工业网络协议能力的硬件 PLC 设备。采取工业协议实现工厂模拟器和 PLC 之间的通信。工厂模拟器将传感器信息发给控制器，控制器的算法基于传感器输入计算执行器所需的值，然后将这些值发回工厂控制器。

在工厂模拟器计算机上安装多节点 DeviceNet 卡。DeviceNet 是自动化行业的一种通用工业协议，用于实现控制设备之间的数据交换。单个硬件设备可利用多节点卡模拟多个虚拟的 DeviceNet 节点。在我们的示例中，每个传感器和执行器均为专用节点。因此，该系统中配置了 53 个虚拟节点（包括传感器的 41 个虚拟节点和执行器的 12 个虚拟节点）。并且，开发了软件接口用于通过 DeviceNet 在工厂模拟器和 PLC 之间发送和接收传感器和执行器的值。

OPC DA 服务器在 Windows 7 计算机上运行，充当 PLC 的主要数据网关。PLC 与 OPC DA 服务器进行通信，对所有传感器和执行器的信息进行更新和检索。在 PLC 专业术语中，传感器和执行器的信息称为“标签”。该控制器提供 MATLAB Simulink 接口与 OPC DA 服务器直接通信。

该系统提供人机界面（HMI）和历史数据库。HMI 为图形化用户界面，面向操作员或用户显示过程状态信息。历史数据库是记录所有过程传感器和执行器的信息的主数据库。HMI 和历史数据库均通过内置接口与 OPC DA 建立连接，访问所有过程信息。

在该系统中，工程工作站用于提供工程支持，如 PLC 开发和控制、HMI 开发和部署以及对历史数据库进行数据检索。

8.1.2 网络架构

PCS 网络通过边界路由器与实验室主局域网隔离。路由器利用动态路由协议，即开放式最短路径优先（OSPF），与顶层的主路由器进行通信。网络架构如图 8-3 所示。

所有的网络流量均需通过边界路由器访问实验室的主局域网。

系统中存在两个虚拟网段，每个网络均由以太网交换机管理。HMI 和控制器位于虚拟网络 VLAN-1 中，而工厂模拟器、历史数据库、OPC DA 服务器和 PLC 位于虚拟网络 VLAN-2 中。

VLAN-1 对中央控制室环境进行模拟。在该环境中，HMI 和控制器以虚拟化的形式部署在同一网段。VLAN-2 模拟由生产厂区、PLC、OPC 服务器和历史数据库组成的过程运行环境。

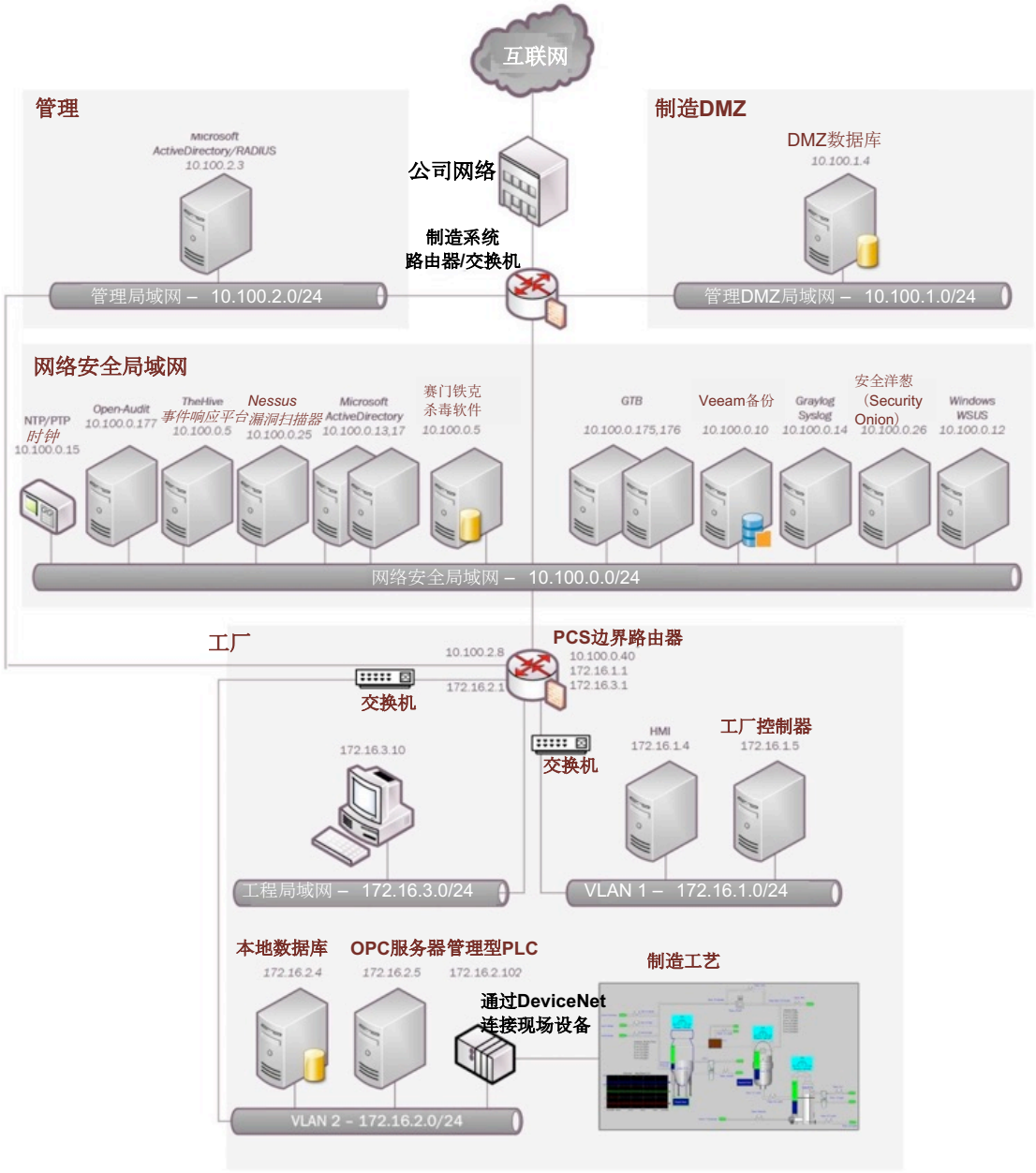

图 8-3 PCS 网络架构

8.2 离散型制造系统

CRS 工作单元包括两个机械手臂，用于执行称为机器送料[11]的材料处理流程，如图 8-4 所示。这一机械化的机器送料流程利用机器人与机器进行交互，替代人类进行的手动操作（如装载和卸载机器的部件、打开和关闭机门、激活操作员控制面板的按钮等）。

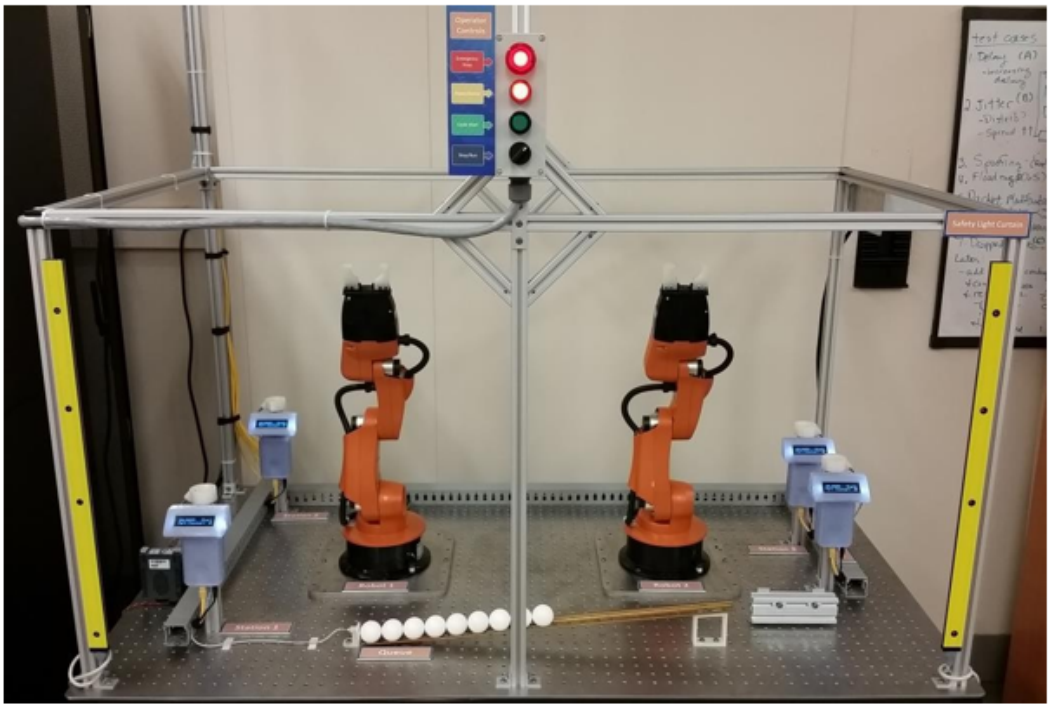

图 8-4 CRS 工作单元准备就绪，等待操作员启动制造流程。
操作员控制模板位于图的上部。

人类操作员通过人机界面（HMI）以及工作区外部的控制面板与工作单元进行交互。

工作单元需具备可重构性，支持多类作业方法、网络拓扑以及工业组网协议。这两个机器人互相配合，负责整个制造流程的部件输送。之所以部署两个机器人是因为该工作单元共有四个站，单个机器人无法同时接触这四个站。同时，部署两个机器人也提升了工作单元的效率。

8.2.1 控制系统运行

机械手臂通过四个模拟的机器操作（称为“站”）传输部件。每个站由以下装置组成： 固定装置（用于固定部件）、红外接近传感器（检测部件）、单板计算机（模拟典型加工中心的操作和通信）以及液晶显示屏（LCD，显示站的运行状态）。这些站通过工作单元的局域网与管理型 PLC 进行通信。管理型 PLC 对制造过程的方方面面进行监测和控制。

PLC 根据这四个加工站的制造数据确定机械装置需进行哪些必要操作（作业）才能确保部件在整个制造过程中持续正常运动。同时，PLC 与 HMI 进行通信，便于操作员及时了解操作状态并进行管控。工作单元由联网服务器组成的共享基础架构、评测工具和其他技术提供支持。该基础架构用于多项研究职能，如网络安全工具的测试、部署和托管、网络流量的评测和抓包系统、对触发异常网络活动的网络流量进行生成和处理以及实验数据文件存储。在实现中，同时部署了虚拟服务器基础架构为所需的多项网络安全技术和工具提供支持。

8.2.2 网络架构

如图 8-5 所示，CRS 网络采取层级架构，将提供管理功能的设备与控制制造过程的设备进行隔离。工作单元的顶层路由器为西门子提供的 RUGGEDCOM RX1510 路由器，该路由器提供防火墙能力，实现基于规则的网络流量放行和限制。该路由器通过网络地址转换（NAT）连接实验室的局域网（即图 8-5 中的试验台局

域网）。管理型局域网的二层网络流量由 Netgear GS724T 托管以太网交换机处理，而控制型局域网的网络流量由西门子 i800 托管以太网交换机处理。

路由器和网络交换机用于将收到的网络流量镜像至位于测量机架上的抓包服务器上。串联（即 bump-in-the-wire）在网络中的网络探针部署在 PLC、HMI 和站 1，专门用于将进出网络流量转发至抓包服务器。

所有的基于制造过程的网络通信均采取 Modbus TCP 工业网络协议，机器人控制器和机器人驱动程序之间的网络流量采取机器人操作系统（ROS）本身的 TCPROS 和 UDPROS 协议。

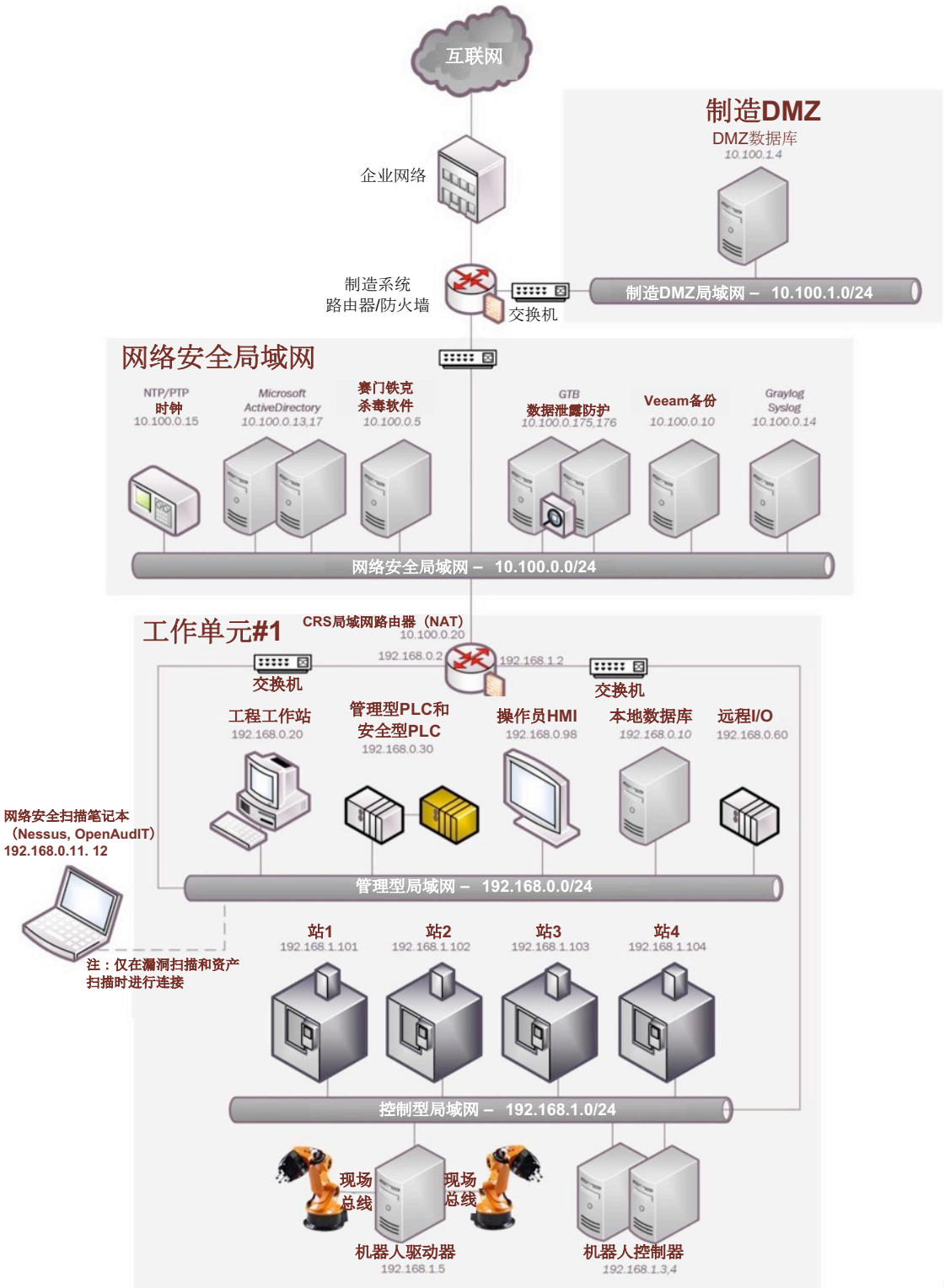

图 8-5 机器人装配 CRS 网络

附录 A 缩略语和缩写词

CAN	Controller Area Network	控制器区域网
CERT	Computer Emergency Response Team	计算机应急响应小组
COTS	Commercial Off-The-Shelf	商用现货
CRS	Collaborative Robotics System	协作机器人系统
CSF	Cybersecurity Framework	网络安全框架
DA	Data Access	数据访问
DCS	Distributed Control System	分布式控制系统
DHS	Department of Homeland Security	美国国土安全部
DMZ	Demilitarized Zone	隔离区（非军事化区）
FIPS	Federal Information Processing Standards	联邦信息处理标准
GBPS	Gigabits Per Second	千兆/秒
GMT	Greenwich Mean Time	格林尼治标准时间
HMI	Human Machine Interface	人机界面
ICS	Industrial Control System	工控系统
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	工控系统网络应急响应小组
ICSJWG	Security Industrial Control System Joint Working Group	工业控制系统联合工作小组
IEC	International Electrotechnical Commission	国际电工委员会
IP	Internet Protocol	互联网协议
ISA	The International Society of Automation	国际自动化协会
IT	Information Technology	信息技术
KPI	Key Performance Indicator	关键性能指标
LAN	Local Area Network	局域网
LCD	Liquid Crystal Display	液晶显示屏
LVL	Level	级别
MBPS	Megabits Per Second	兆/秒
MFG	Manufacturing	制造业
NAT	Network Address Translation	网络地址转换
NCCIC	National Cybersecurity & Communications Integration Center	国家网络安全和通信集成中心
NGFW	Next Generation Firewall	下一代防火墙
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NIST SP	NIST Special Publication	NIST特别刊物
NISTIR	NIST Internal Report	NIST内部报告
OEM	Original Equipment Manufacturer	原始设备制造商
OPC	Open Process Control	开放式过程控制
OSPF	Open Shortest Path First	开放式最短路径优先
OT	Operational Technology	运营技术
PCS	Process Control System	过程控制系统

PLC	可编程逻辑控制器
RAM	随机存取存储器
ROS	机器人操作系统
SCADA	数据采集与监视控制系统
SEC	安全
SSL	安全套接层
TCP	传输控制协议
TCPROS	基于TCP的机器人操作系统协议
UDP	用户数据报协议
UDPROS	基于UDP的机器人操作系统协议
USB	通用串行总线
US-CERT	美国计算机紧急响应小组
UTC	世界标准时间
VLAN	虚拟局域网
VoIP	基于IP的语音传输
VPN	虚拟专用网络

附录 B 参考资料

[1] 第 13636 号行政命令，提升关键基础设施网络安全，DCPD-201300091，2013 年 2 月 12 日. https://www.govinfo.gov/app/details/FR-2013-02- 19/2013-03915

[2] 国家标准与技术研究院（2014），提升关键基础设施网络安全框架，1.0 版.（国家标准与技术研究院，马里兰州盖瑟斯堡），2014 年 2 月 12 日 https://doi.org/10.6028/NIST.CSWP.02122014

[3] Stouffer KA，Lightman S，Pillitteri VY，Abrams M，Hahn A（2015），工业控制系统（ICS）安全指南.（国家标准与技术研究院，马里兰州盖瑟斯），NIST 特刊（SP）800-82，第二版. https://doi.org/10.6028/NIST.SP.800-82r2

[4] 联合特遣队转型方案（2013），联邦信息系统与组织的安全和隐私控制. （国家标准与技术研究院，马里兰州盖瑟斯），NIST 特刊（SP）800-53，第四版，包含截至 2015 年 1 月 22 日的更新. https://doi.org/10.6028/NIST.SP.800-53r4

[5] 国际自动化协会（2019）ISA99，工业自动化及控制系统安全. https://www.isa.org/isa99/.

[6] 国家网络安全和通信集成中心（NCCIC） https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

[7] 美国国土安全部，国家网络安全和通信集成中心（NCCIC）（2019）网络安全和基础设施安全局—工业控制系统. https://ics-cert.us-cert.gov/.

[8] Stouffer K，Zimmerman T，Tang CY，Lubell J，Cichonski J，McCarthy J（2019）网络安全框架制造篇.（国家标准与技术研究院，马里兰州盖瑟斯），NIST 内部报告（NISTIR）8183，包含截至 2019 年 5 月 20 日的更新. https://doi.org/10.6028/NIST.IR.8183

[9] J. J. Downs 和 E. F. Vogel，全厂范围内的工业过程控制问题，计算机与化学工程，第 17 卷，第 3 期，245-255 页，1993.

[10] L. Ricker，田纳西-伊斯曼挑战过程分散控制，过程控制杂志，第 6 卷，第 4 期，205-221 页，1996.

[11] Zimmerman T（2017）机器人网络安全性能分析度量和关键性能指标.（国家标准与技术研究院，马里兰州盖瑟斯），NIST 内部报告（NISTIR）8177，包含截至 2019 年 5 月 21 日的更新. https://doi.org/10.6028/NIST.IR.8177

[12] Tang CY（2017）过程控制系统网络安全性能分析关键性能指标.（国家标准与技术研究院，马里兰州盖瑟斯），NIST 内部报告（NISTIR）8188，2017. https://doi.org/10.6028/NIST.IR.8188

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。