National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-82

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

《工业控制系统安全指南》
NIST SP800-82

目 录

摘要

此文件提供建立安全的工业控制系统（ICS）的指导。这些 ICS 包括监控和数据采集（SCADA）系统，分布式控制系统（DCS），和其他控制系统，如在工业部门和关键基础设施中经常可以看到的撬装式的可编程逻辑控制器（PLC）。ICS 通常用于诸如电力、水和污水处理、石油和天然气、化工、交通运输、制药、纸浆和造纸、食品和饮料以及离散制造（如汽车、航空航天和耐用品）等行业。这些控制系统是美国关键基础设施运作的关键，通常是高度相互关联和相互依存的系统。要注意的是大约有 90％的国家关键基础设施是私人拥有和经营的。联邦机构也经营了上面提到的许多工业流程；其他例子包括空中交通管制和材料处理（例如，邮政邮件处理）。本文提供了对这些 ICS 及典型系统技术的概述，识别对这些系统的典型威胁和脆弱性，并提供安全对策建议，以减轻相关风险。

最初，ICS 与传统的信息技术（IT）系统几乎没有一点相似，因为 ICS 是孤立的系统，使用专门的硬件和软件来运行专有的控制协议。而现在广泛使用的、低成本的互联网协议（IP）设备正在取代专有的解决方案，从而增加了网络安全漏洞和事故的可能性。由于 ICS 采用 IT 解决方案以提升企业业务系统的连接和远程访问能力，并被设计为可使用工业标准的计算机、操作系统（OS）和网络协议，它们已经开始类似于 IT 系统了。这种集成支持新的 IT 能力，但它为 ICS 提供的与外界的隔离明显比原先的系统少多了，这就产生了更多的安全保护需求。虽然在典型的 IT 系统中已经设计了安全解决方案来处理这些安全问题，但是在将这些相同的解决方案引入 ICS 环境时，必须采取特殊的预防措施。在某些情况下，需要为 ICS 环境量身定制的新的安全解决方案。

虽然有些特征是相似的，ICS 还有与传统的信息处理系统不同的特点。这些差异来自于在 ICS 中的逻辑执行会直接影响物理世界这一事实。这些特征包括对人类的健康和生命安全的重大风险，对环境的严重破坏，以及严重的财务问题如生产损失，对一个国家的经济产生负面影响，妥协的所有权信息。 ICS 具有独特的性能和可靠性要求，并经常使用的操作系统和应用程序可能对典型的 IT 人员而言被认为是标新立异的。此外，有时安全和效率的目标会与在控制系统的设计和操作中的安全性相冲突。

最初 ICS 主要面对的是本地威胁，因为它们的许多组件都连接在被物理保护的区域中，并没有连接到 IT 网络或系统。然而，将 ICS 系统集成到 IT 网络中的趋势显著减少了 ICS 与外界的隔离，从而产生了更多的保护这些系统对抗远程、外部威胁的需求。此外，越来越多的无线网络应用使 ICS 实现要面临更多的来自某些敌人的风险，这类人与设备在物理上比较接近，但又没有直接的物理连接。控制系统面临的威胁可以来自多个方面，包括敌对政府，恐怖组织，心怀不满的员工，恶意入侵者，复杂性，事故，自然灾害以及由内部的恶意或意外行为。 ICS 安全目标通常按照可用性、完整性和保密性的优先顺序排列。

一个 ICS 可能面临的事故包括：

阻止或延迟通过 ICS 网络的信息流，这可能会破坏 ICS 的运作

对命令、指示或报警阈值非授权的更改，可能损坏、禁用或关闭设备，产生对环境的影响，和/或危及人类生命

不准确的信息被发送到系统操作员，或者是掩饰非授权的更改，或导致操作者发起不适当的行动，均可能产生不同的负面影响

ICS 软件或配置参数被修改，或 ICS 软件感染恶意软件，都会产生不同的负面影响

干扰安全系统的运行，可能危及人类生命。

ICS 实施的重要安全目标应包括以下内容：

限制对 ICS 网络的逻辑访问和网络活动。这包括使用防火墙的一个非军事区（DMZ）的网络架构，以防止网络流量在企业网络和 ICS 网络之间直接传递，并对企业网络用户和 ICS 网络用户分别提供独立的身份验证机制和凭证。ICS 还应使用多层的网络拓扑结构，使最关键的通信发生在最安全和最可靠的层面。

限制对 ICS 网络和设备的物理访问。对组件的非授权的物理访问可能会导致对 ICS 功能的严重扰乱。应采用组合的物理访问控制机制，如锁、智能卡阅读器和/或警卫。

保护单个的 ICS 组件免受暴露。这包括尽可能迅速地部署安全补丁，一旦在它们在现场条件下通过测试后；禁用所有未使用的端口和服务；限制 ICS 的用户权限，只开放每个人的角色所需要的权限；跟踪和监测审计踪迹；在技术上可行的地方使用如防病毒软件和文件完整性检查软件等安全控制措施来预防、阻止、

检测和减少恶意软件。

在不利条件下保持功能。这涉及到设计 ICS 以使每个关键组件都有冗余。此外，如果一个组件失败，它应该不会在 ICS 或其他网络上产生不必要的流量，或不会在其他地方引起另一个问题，如级联事件。

事件发生后，恢复系统。事故是不可避免的，事件响应计划是必不可少的。一个良好的安全计划的主要特点是一个事件发生后，可以以最快的速度恢复系统。

为在 ICS 中妥善地解决安全问题，必须有一个跨部门的网络安全团队，分享他们在不同领域的知识和经验，评估和减轻 ICS 的风险。网络安全团队成员至少应包括组织的 IT 人员、控制工程师、控制系统操作员、网络和系统安全专家、管理层成员和物理安全部门。为保持连续性和完整性，网络安全团队应向控制系统供应商和/或系统集成商进行咨询。网络安全小组应直接向场站管理者（例如，工厂主管）或公司的 CIO / CSO 报告，后者应对 ICS 网络安全承担全部的责任和问责。一个有效的 ICS 网络安全方案应使用“纵深防御”战略，即分层的安全机制，例如任何一个机制失败的影响被最小化。

在一个典型的 ICS 中的“纵深防御”战略包括：

- 制定专门适用于ICS的安全策略，程序，培训和教育材料。
- 基于国土安全咨询系统威胁级别来考虑ICS的安全策略和程序，随着威胁程度的增加部署逐渐增强的安全机制。
- 解决从架构设计到采购到安装到维护退役的ICS整个生命周期的安全。
- 为ICS实施多层网络拓扑结构，在最安全和最可靠的层进行最重要的通信。
- 提供企业网络和ICS网络之间的逻辑分离（例如，在网络之间架设状态检测防火墙）。
- 采用DMZ网络体系结构（即，防止企业和ICS网络之间的直接通信）。
- 确保关键部件和网络冗余。
- 为关键系统设计优雅降级（容错），以防止灾难性的级联事件。
- 禁用ICS设备中经测试后确保不会影响ICS运作的未使用的端口和服务。
- 限制对ICS网络和设备的物理访问。
- 限制ICS的用户权限，只开放为执行每个人的工作所必须的权限（即建立基于角色的访问控制和基于最小特权原则配置每个角色）。
- 考虑为ICS网络和企业网络的用户分别使用独立的身份验证机制和凭据（即ICS网络帐户不使用企业网络的用户帐户）。

- 利用现代技术，如智能卡的个人身份验证（PIV）。
- 在技术上可行的情况下实施安全控制，如入侵检测软件、杀毒软件和文件完整性检查软件，预防、阻止、检测和减少恶意软件的侵入、曝露和传播，无论是针对或来自ICS，或在其内部。
- 在确定适当的地方对ICS的数据存储和通信应用安全技术，如加密和/或加密哈希。
- 在现场条件下进行了所有安全补丁包测试后，如果可能的话，在安装到ICS之前先迅速部署到测试系统上。
- 在ICS的关键领域跟踪和监测审计踪迹。

NIST 与公共和私营部门的 ICS 团体合作创建了工业控制系统安全项目，为将 NIST SP 800-53“联邦信息系统和组织安全控制建议”中的安全控制应用于 ICS 开发了具体的指南。

虽然在 NIST SP 800-53 的附录 F 中描述的大部分控制适用于 ICS，一些控制确实需要通过增加以下一项或多项来提供 ICS 专用的解释和/或增强：

ICS补充指南为组织就NIST SP 800-53附录F中的安全控制在ICS及这些专门系统运行的其他环境中的应用和增强提供了附加的信息。补充指南还提供了一些信息，关于为什么一个特定的安全控制或控制增强可能不适用于某些ICS环境，而可能是一个候选项（即，适用范围指南和/或补偿控制）。ICS补充指南不会取代原来在NIST SP 800-53附录F中的补充指南。

ICS增强（一个或多个），对一些ICS原来可能需要的控制提供了增强增扩。

ICS增强版补充指南，就控制增强如何适用于或不适用于ICS环境提供指导。

这份 ICS 专用指南包含在 NIST SP 800-53，第 3 修订版，附录一：“工业控制系统 - 安全控制，增强和补充指南”中。该文件的第 6 条还为 800-53 安全控制如何应用于 ICS 提供了初步指导意见。如果有初步建议和指导的话，会出现在每节的概述框中。NIST 计划在 2011 年 12 月出一个 NIST SP 800-53 更新版（NIST SP 800-53，第 4 修订版），包括当前在工业控制系统领域中的安全控制，控制增强，补充指导，以及剪裁和补充指南的更新。

此外，本文件的附录 C 对许多当前正在联邦机构、标准组织、产业集团和自动化系统供应商中进行的许多活动提供了一个概述，以便为 ICS 领域的安全提供有效的建议做法。

确保 ICS 安全的最成功的方法是，收集业界建议的做法，在管理层、控制工程师和操作员、IT 组织和一个可信的自动化顾问之间发起一个积极的、协同的努力。这支团队应从联邦政府、行业组织、厂商、标准化组织正在进行的附录 C 所列的活动中提取丰富的可用信息。

1. 简介

1.1 管理机构

国家标准与技术研究院（NIST）的开发推进其法定职责，本文件根据联邦信息安全管理法案（FISMA）2002 年，公共法 107-347 和国土安全总统指令（HSPD - 7）2003 年 7 。

NIST 发展的标准和准则，包括的最低要求，所有机构的业务和资产提供足够的信息安全负责，但这些标准和准则不适用于国家安全系统。这一方针的管理和预算办公室（OMB）通告 A - 130，第 8B（3）办公室的要求是一致的，“保证机构信息系统”，在 A－130 的分析，附录四：对重点路段的分析的安全。A－130，附录三提供参考信息。

这一方针已准备为联邦机构使用。它可用于在自愿基础上的非政府组织，并不受版权保护，虽然归属需要。

在这个文件中的任何内容，应采取相矛盾的标准和准则方面对联邦机构的强制性和约束力，由商务部根据法定权限局长，也不应改变或取代现有的主管部门，工商及科技局局长主任解释这些准则行政管理和预算局，或任何其他联邦官员。

1.2 目的和范围

本文件的目的是为工业控制系统（ICS）的安全保障提供指导，包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）及其他执行控制功能的系统。该文件提供了一个对 ICS 和典型系统拓扑的概述，确定了这些系统的典型威胁和

漏洞，并提供建议的安全对策，以减轻相关的风险。因为有许多不同类型的 ICS，具有不同程度的潜在风险和影响，该文件为 ICS 安全提供了许多不同的方法和技术。该文件不应该单纯的被用作一个保护特定系统的清单。我们鼓励读者在他们的系统中执行风险评估，并对建议的指导方针和解决方案进行裁剪，以满足其特定的安全、业务和运营要求。

本文件的范围包括通常在电、水和污水处理、石油和天然气、化工、制药、纸浆和造纸、食品和饮料以及离散制造（汽车、航空航天和耐用品）等行业应用的 ICS。

1.3 读者

本文档涵盖了 ICS 的具体细节。该文件在本质上是技术性的，但是，它提供了必要的背景，了解所讨论的议题。

目标受众是多种多样的，包括以下内容：

- ✧ 控制工程师，集成商和建筑师设计或实施安全 IC
- ✧ 系统管理员，工程师和其他信息技术（IT）专业人员谁管理，补丁或安全 IC
- ✧ 执行 ICS 的安全评估和渗透测试的安全顾问
- ✧ 负责为 ICS 的经理人
- ✧ 高级管理人员正试图了解影响和后果，因为他们的理由和适用的 ICS 网络安全方案，以帮助减轻影响的业务功能
- ✧ 研究人员和分析师们正试图了解 ICS 的独特的安全需求
- ✧ 厂商正在开发的产品将作为一个 ICS 的一部分部署

本文档假定读者熟悉与一般计算机安全的概念，如在网络和使用基于 Web 的检索信息的方法使用的通信协议。

1.4 文档结构

本指南的其余部分分为以下主要章节：

第 2 章提供对 SCADA 和其他 ICS 的概述，及其安全需求的重要性。

第 3 章提供对 ICS 和 IT 系统之间的差异的讨论，以及威胁、漏洞和事件。

第 4 章提供对开发和部署一个 ICS 安全计划的概述，以减轻由于第 3 章中确认的漏洞而引起的风险。

第 5 章提供将安全集成到典型 ICS 网络架构中的建议，重点是网络隔离实践。

第 6 章提供对 NIST 特别出版物 800-53“联邦信息系统和组织安全控制建议”中定义的管理、运作以及技术控制的汇总，并就如何将这些安全控制应用于 ICS 提供了初步指南。

该指南还包含几个附录与辅助材料，具体如下：

附录 A 提供了本文档中使用的缩略语和缩写列表。

附录 B 提供了本文档中使用的术语表。

附录 C 提供了一些当前 ICS 安全活动的清单和简短描述。

附录 D 提供了一些正在为 ICS 开发的新兴安全功能的清单。

附录 E 提供 FISMA 实施项目的概述和配套文档，以及 FISMA 与 ICS 的相关性。

附录 F 提供了一个用于开发本文件的引用列表。

2. 工业控制系统概述

工业控制系统（ICS）是几种类型控制系统的总称，包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）和其它控制系统，如在工业部门和关键基础设施中经常可以看到的撬装式的可编程逻辑控制器（PLC）。ICS 通常用于诸如电力、水和污水处理、石油和天然气、化工、交通运输、制药、纸浆和造纸、食品和饮料以及离散制造（如汽车、航空航天和耐用品）等行业。这些控制系统是美国关键基础设施运作的关键，通常是高度相互关联和相互依存的系统。要注意的是大约有 90％的国家关键基础设施是私人拥有和经营的。联邦机构也经营了上面提到的许多工业流程；其他例子包括空中交通管制和材料处理（例如，邮政邮件处理）。本节提供对 SCADA、DCS、PLC 系统的概览，包括典型的架构和组件。还有一些插图用于描绘网络连接和每个系统的典型部件，以帮助了解这些系

统。请记住，ICS 通过整合 DCS 和 SCADA 系统的属性而模糊了两者之间的差异，因此实际实现中可能是混合的。请注意，本节中的图并不代表一个安全的 ICS。架构安全和安全控制分别是在本文件的第 5 章和第 6 章讨论。

2.1 SCADA，DCS，PLC 的概述

SCADA 系统是用来控制地理上分散的资产的高度分布式的系统，往往分散数千平方公里，其中集中的数据采集和控制是系统运行的关键。它们被用于分配系统，如供水和污水收集系统，石油和天然气管道，电力电网，以及铁路运输系统。一个 SCADA 控制中心对跨长途通信网络的场站执行集中的监视和控制，包括监测报警和处理状态数据，在现场的。根据从远程站点收到的信息，自动化或操作员驱动的监督指令可以被推送到远程站点的控制装置上，后者通常被称为现场设备。现场设备控制本地操作，如打开和关闭阀门和断路器，从传感器系统收集数据，以及监测本地环境的报警条件。

DCS 被用来控制工业生产过程，如发电、炼油、水和废水处理、化工、食品、汽车生产。DCS 被集成为一个控制架构，包含一个监督级别的控制，监督多个、集成的子系统，负责控制本地化过程的细节。产品和过程控制通常是通过部署反馈或前馈控制回路实现的，关键产品和/或过程条件被自动保持在一个所需的设置点周围。为了实现所需的产品和/或过程围绕一个指定设定点的公差，在场地部署特定的 PLC，并在 PLC 上的比例、积分和/或微分设置被调整为提供所需的公差，以及在过程干扰期间的自我校正率。DCS 系统被广泛应用于基于过程的产业。

PLC 是基于计算机的固态装置，控制工业设备和过程。虽然 PLC 是整个 SCADA 和 DCS 系统中使用的控制系统组件，它们通常在较小的控制系统配置中作为主要组件，用于提供离散过程的操作控制，如汽车装配生产线和电厂吹灰控制。PLC 被广泛应用于几乎所有的工业生产过程。

基于过程的制造业通常利用两个主要过程：

连续制造过程。这些过程连续运行，往往会转换以制造不同档次的产品。典型的连续制造过程包括电厂、炼油厂的石油和化工厂的蒸馏过程中的燃料或蒸汽流量。

批量制造过程。这些过程有不同的处理步骤，在大量的物料上进行。有一个批处理过程的明显开始和结束步骤，可能在中间步骤中有简短的稳态操作过程。典型的批量制造过程包括食品制造业。

离散制造业通常在单个设备上执行一系列步骤，创造的最终产品。电子和机械部件装配和零件加工是这种类型的行业的典型例子。

基于过程和基于离散的行业都使用相同类型的控制系统、传感器和网络。有些设施是一个基于离散和过程制造的混合。

虽然在分销和制造业使用的控制系统的运作非常相似，他们在某些方面有所不同。主要区别之一是，与地理上分散的 SCADA 场站相比，DCS 或 PLC 控制系统通常在位于一个更密闭的工厂或工厂为中心的区域。 DCS 和 PLC 通信通常使用局域网（LAN）的技术，与 SCADA 系统通常所使用的长途通信系统相比，更可靠和高速。事实上，SCADA 系统是专门设计用来处理长途通信带来的挑战，如使用各种通信媒体产生的延迟和数据丢失。DCS 和 PLC 系统通常采用比 SCADA 系统更大程度的闭环控制，因为工业过程的控制通常比分配过程的监督控制更为复杂。就本文件的范围而言，这些差异可以被视为极微妙的，因为这里我们关注的是如何将 IT 安全集成到这些系统中。在本文件的后续部分，SCADA 系统、DCS 和 PLC 系统将被称为 ICS，除非特定的参考是特别为其中某一个系统定制的（例如，用于 SCADA 系统的现场设备）。

2.2 ICS 的操作

一个 ICS 的基本操作如图 2-1 所示。

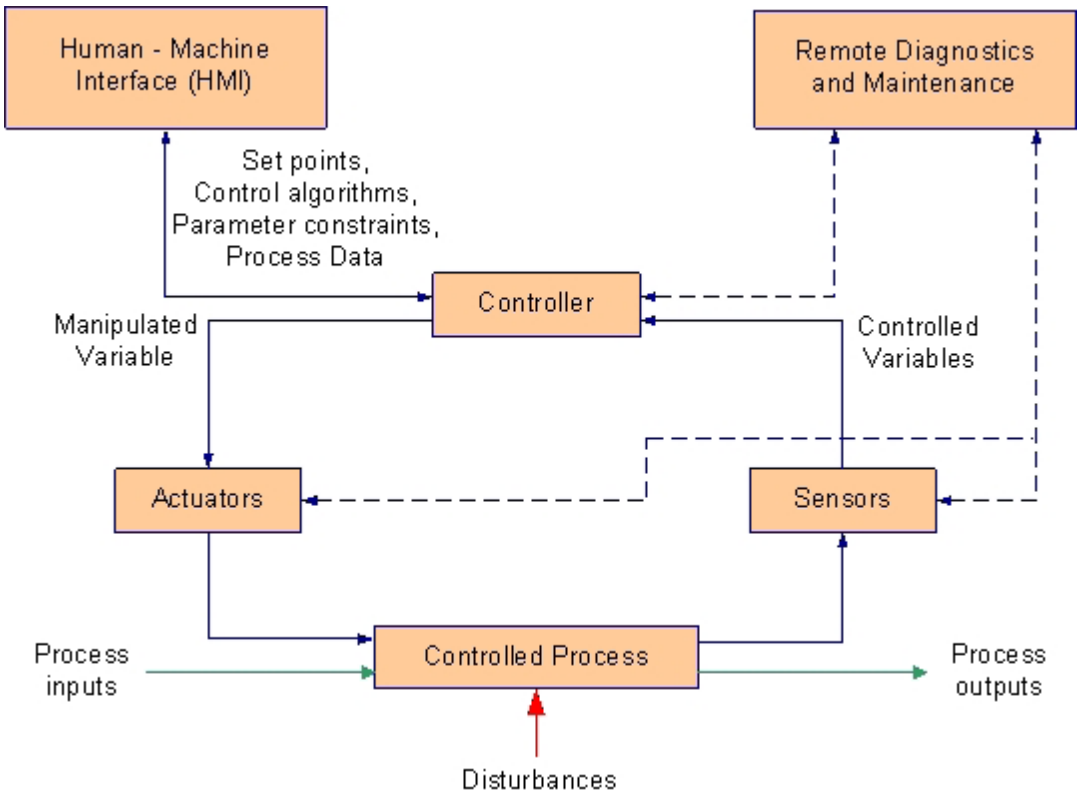


图2-1 ICS操作

其关键组件包括以下内容：

控制回路。控制回路包括测量传感器，控制器硬件如 PLC，执行器如控制阀，断路器，开关和电机，以及变量间的通信。控制变量被从传感器传送到控制器。控制器解释信号，并根据它传送到执行器的设置点产生相应的调节变量。干扰引起控制过程变化，产生新的传感器信号，确定过程的状态为被再次传送到控制器。

人机界面(HMI)。操作员和工程师使用 HMI 来监控和配置设置点，控制算法，并在控制器中调整和建立参数。HMI 还显示进程状态信息和历史信息。

远程诊断和维护工具。用于预防、识别和恢复运行异常或故障的诊断和维护工具。

一个典型 ICS 由控制回路、人机界面、远程诊断和维护工具组成，并使用分层的网络架构上的网络协议集合来构建。有时，这些控制回路是嵌套和/或级联的，也就是说一个循环的设置点是建立在由另一个循环确定的过程变量的基础上的。督导级循环和低层次循环在一个具有从几毫秒到几分钟不等的周期时间的过程期间连续运行。

2.3 主要 ICS 元件

为了支持随后的讨论，本节定义用于控制和联网的关键 ICS 组件。其中一些组件可以被笼统地描述为可使用在 SCADA 系统、DCS 和 PLC 中，有的则是唯一针对其中某一个。附录 B 中的条款汇编包含了一个更详细的控制和网络组件列表。此外，第 2.4 节的图 2-5 和图 2-6 显示了采用这些组件的 SCADA 实施的例子，在 2.5 节的图 2-7 显示了一个 DCS 实现的例子，在第 2.6 节的图 2-8 显示 PLC 系统实现的例子。

2.3.1 控制元件

以下是一个 ICS 的主要控制元件清单：

控制服务器。控制服务器承载与较低级别的控制设备进行通信的 DCS 或 PLC 监控软件。控制服务器通过 ICS 网络访问下属的控制模块。

SCADA 服务器或主终端单元(MTU)。SCADA 服务器担任 SCADA 系统的主设备。远程终端单元和 PLC 设备（如下所述）位于远程场站，通常作为从设备。

远程终端装置（RTU)。RTU，也称为遥测遥控装置，是特殊用途的数据采集和控制单元，被设计为支持 SCADA 远程站点。RTU 是现场设备，往往配备无线电接口以支持有线通信不可用的远程站点。有时，PLC 被实现为现场设备，担任 RTU 的工作；在这种情况下，PLC 通常就被称为一个 RTU。

可编程逻辑控制器（PLC)。 PLC 是一种小型工业计算机，最初设计为执行由电器硬件（继电器，开关，机械定时器/计数器）执行的逻辑功能。PLC 已经演变成为控制器，具有控制复杂过程的能力，它们被大量地用在 SCADA 系统和 DCS 中。在现场级别使用的其他控制器为过程控制器和 RTU；它们提供与 PLC 相同的控制，但是为特定的控制应用而设计的。在 SCADA 环境中，PLC 是经常被用来作为现场设备，因为它们比特殊用途的 RTU 更经济，多用途，灵活和易配置。

智能电子设备（IED)。IED 是一种“智能”传感器/执行器，包含采集数据、与其他设备通信和执行本地过程和控制所需的智能。IED 可以组合一个模拟输入传感器，模拟输出，低层次的控制能力，通信系统，以及一台设备中的程序存储器。在 SCADA 和 DCS 系统中使用 IED，可以在本地级别实现自动化控制。

人机界面（HMI）。HMI 是一套软件和硬件，允许操作人员监控一个处于控制下的过程的状态，修改控制设置以更改控制目标，并在发生紧急情况时手动取代自动控制操作。HMI 还允许控制工程师或操作员配置控制器中的设置点或控制算法和参数。HMI 还向操作员、管理员、经理、业务伙伴和其他授权用户显示过程状态信息、历史信息、报告和其他信息。位置、平台和接口可能相差很大。例如，HMI 可以是控制中心的专用平台，无线局域网上的笔记本电脑，或连接到互联网的任何系统上的浏览器。

历史数据。历史数据是一个集中的数据库，记录 ICS 内的所有过程信息。在这个数据库中存储的信息可以被访问，以支持各种分析，从统计过程控制到企业层面的规划。

输入/输出（IO）服务器。 IO 服务器作为一个控制组件，负责收集、缓冲来自控制子元件如 PLC、RTU 和 IED 等的过程信息，并提供对过程信息的访问。一个 IO 服务器可以驻留在控制服务器上或一个单独的计算机平台上。IO 服务器也可用于与第三方控制元件的接口，如 HMI 和控制服务器。

2.3.2 网络组件

在控制系统层次结构内部的每一层上都有不同的网络特性。跨越不同 ICS 实现的网络拓扑结构，与使用基于互联网的 IT 和企业一体化战略的现代系统是不同的。控制网络已经与企业网络合并，让控制工程师可以从控制系统网络外部监测和控制系统。该连接也可以让企业高层决策者获得对过程数据的访问。以下是一个 ICS 网络的主要组成部分的清单，无论使用何种网络拓扑：

现场总线网络。现场总线网络将传感器和其他设备连接到 PLC 或其他控制器。现场总线技术的使用，消除了对控制器和每个设备之间的点到点连线的需要。设备使用各种协议与现场总线控制器进行通信。在传感器和控制器之间发送的消息可唯一确定每个传感器。

控制网络。控制网络负责连接监控级别的控制模块与较低级别的控制模块。

通讯路由器。路由器是一种通信设备，在两个网络之间传输消息。路由器常见用途包括将一个局域网连接到广域网，为 SCADA 通信将 MTU 和 RTU 连接到远程网络介质。

防火墙。防火墙可以保护网络上的设备，通过监测和控制通信数据包，使用预定义的过滤策略。防火墙也有助于管理 ICS 网络的隔离策略。

调制解调器。调制解调器是用于串行数字数据和适用于通过电话线传输设备进行通信的信号之间的转换设备。调制解调器通常用在 SCADA 系统中，以建立远程 MTU 和远程现场设备之间的串行通信。它们还用在 SCADA 系统、DCS 和 PLC 中以获得对运行和维护功能的远程访问，如输入命令或修改参数，以及用于诊断的目的。

远程接入点。远程接入点是控制网络的不同设备、区域和位置，为了远程配置控制系统和访问过程数据。例子包括使用个人数字助理（PDA）通过一个无线接入点访问局域网上的数据，并使用一台笔记本电脑和调制解调器连接并远程访问 ICS 系统。

2.4 SCADA 系统

SCADA 系统被用来控制分散的资产，对其而言，集中的数据采集与控制一样重要。这些系统被用于配水系统和污水收集系统，石油和天然气管道，电力设施的输电和配电系统，以及铁路和其他公共交通系统。SCADA 系统将数据采集系统与数据传输系统和 HMI 软件集成起来，为大量的过程输入输出提供集中的监控系统。SCADA 系统被设计为收集现场的信息，传输到中央计算机设施，并向操作员显示图形或文字的信息，从而使操作员能够从一个中央位置实时监视或控制整个系统。根据单个系统的复杂性和设置，对任何单独系统的控制、操作或任务都可自动进行或遵照操作员的命令执行。

SCADA 系统包括硬件和软件两方面。典型的硬件包括放置在控制中心的 MTU，通信设备（例如，广播、电话线、电缆或卫星），以及一个或多个由控制执行器和/或监视传感器的 RTU 或 PLC 构成的地理上分散的场站。MTU 的存储和处理由 RTU 输入和输出的信息，而 RTU 或 PLC 控制本地过程。通信硬件实现 MTU 与 RTU 或 PLC 之间的信息和数据的来回传输。其软件部分告诉系统监视什么和何时监视，什么参数范围是可以接受的的，当参数变化超出可接受的值时启动什么响应。IED，例如一种保护继电器，可直接与 SCADA 服务器通信，或者一个本地的 RTU 可以轮询 IED 以收集数据，并把数据传递给 SCADA 服务器。IED 提供直接的接口来控制

和监视设备和传感器。IED 可直接接受 SCADA 服务器的轮询和控制，且在大多数情况下具有本地程序，允许 IED 在没有 SCADA 控制中心的直接指示时也能进行工作。 SCADA 系统通常被设计为容错系统，在系统架构中内置了显著的冗余。

图 2-2 显示了 SCADA 系统的组件和总体配置。控制中心设有一个 SCADA 服务器（MTU）和通信路由器。其他控制中心组件包括 HMI（人机界面），工程师工作站和历史数据等，都通过局域网进行连接。控制中心收集并记录场站收集到的信息，在 HMI 上显示信息，并可能会基于检测到的事件产生行动。控制中心还负责集中告警，趋势分析和报告。场站负责对执行器的本地控制的和对传感器的监视。场站往往配备远程访问能力，使场站操作员通常可以在一个单独的拨号调制解调器或广域网连接上执行远程诊断和维修。在串行通信上运行的标准和专有的通信协议是用于在控制中心和场站之间传输信息的，使用如电话线、电缆、光纤、无线电频率如广播、微波和卫星等遥测技术。

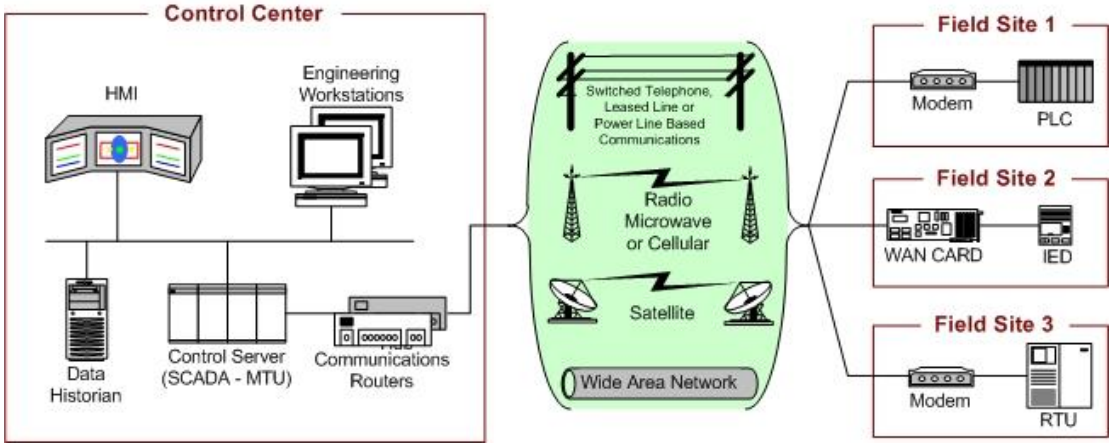


图2-2 SCADA系统总体结构

MTU - RTU 通讯架构在不同的具体实现上有所差异。可使用的不同架构，包括点对点、串行、串行-星型、多节点等，如图 2-3 所示。点对点是最简单的功能类型，但是，它是昂贵的，因为每个连接都需要独立的通道。在一个串行配置中，使用的通道数量减少了；然而，通道共享会对 SCADA 系统操作的效率和复杂性产生影响。同样，串行-星型和多节点配置为每个设备使用一个通道也会导致效率下降和系统复杂性增加。

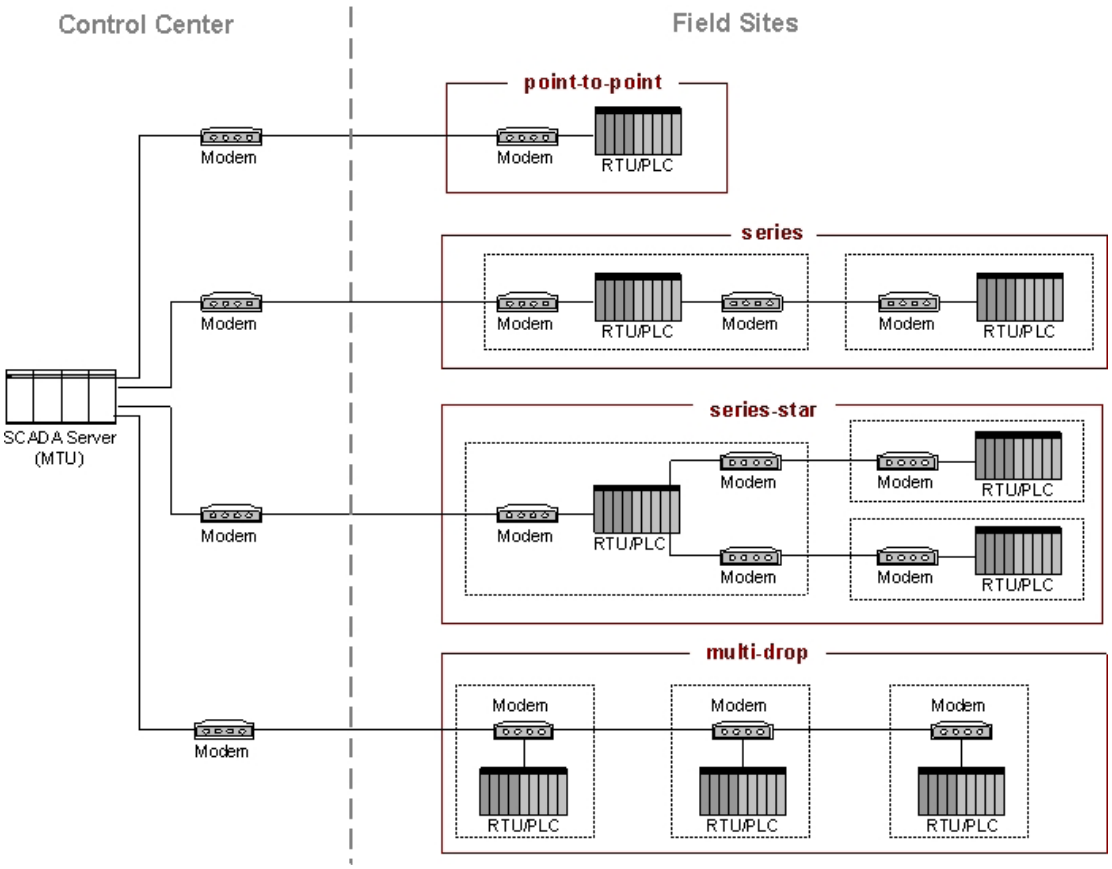


图2-3 基本的SCADA通信拓扑

如图 2-3 所示的四个基本架构，可以通过使用专用通讯设备来管理通信交换以及消息交换和缓冲而得到进一步增强。大型 SCADA 系统，包含了数百个 RTU，通常会部署子 MTU 以减轻主 MTU 的负担。这种类型的拓扑结构如图 2-4 所示。

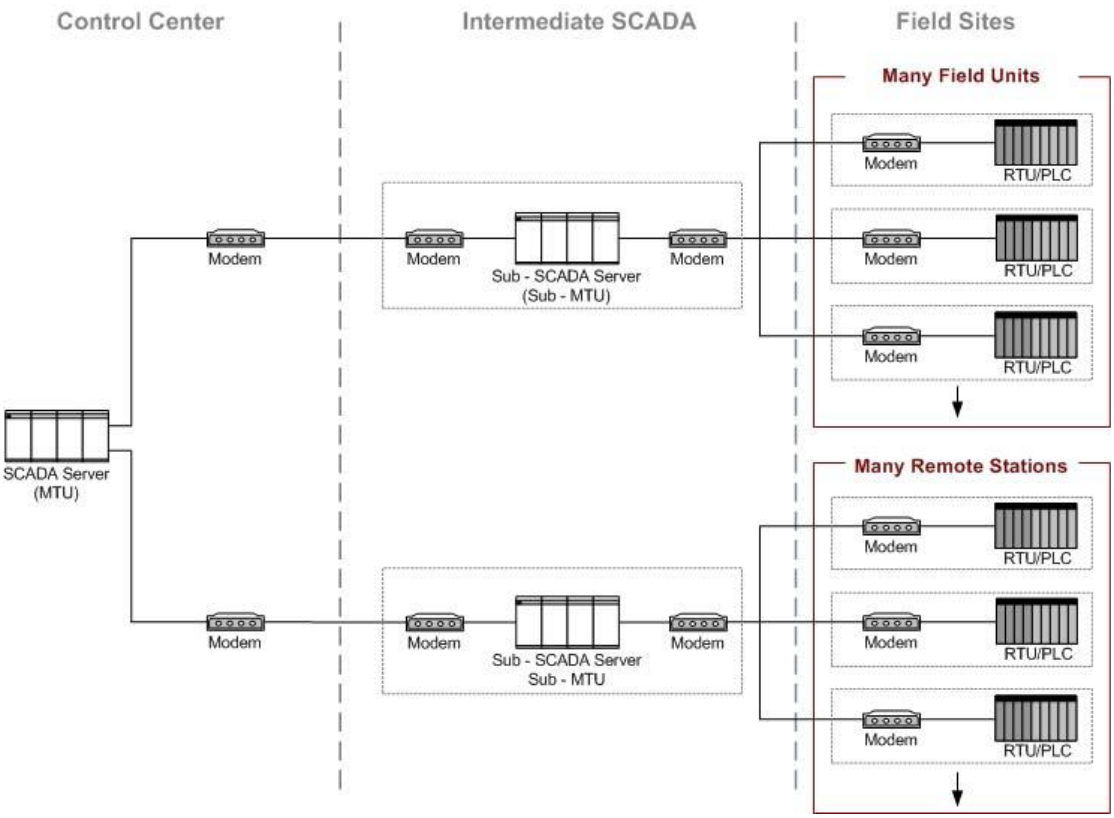


图2-4 大型SCADA通信拓扑

图 2-5 显示了 SCADA 系统实现的一个例子。这个 SCADA 系统由一个主控制中心和 3 个场站构成。第二个备份控制中心提供主控制中心故障时的冗余。所有的控制中心和场站之间的通信采用点对点连接，其中有两个连接使用无线电遥测。第三个场站是在控制中心本地，使用广域网（WAN）进行通信。位于主控制中心上方的一个区域控制中心提供一个更高级别的监督控制。企业网络可以通过广域网访问所有控制中心，并且场站也可以被远程访问以进行故障排除和维护操作。主控制中心按定义的时间间隔（如 5 秒、60 秒）轮询场站设备的数据，并可以根据需要发送新的设置点给现场设备。除了轮询和发布高层次的命令，SCADA 服务器也监视来自场站报警系统的优先中断。

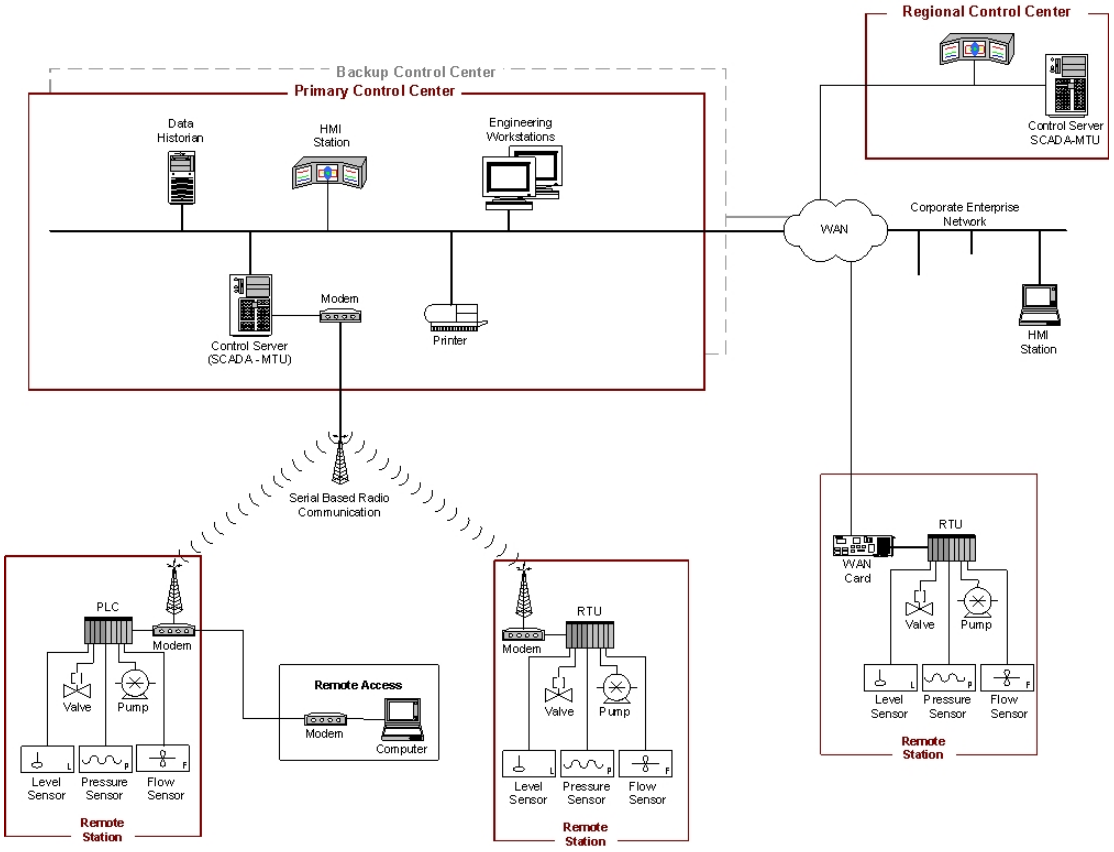


图2-5 SCADA系统实现举例 (分布式监控)

图 2-6 显示了一个对铁路监测和控制的实现示例。这个例子中包括了一个部署了 SCADA 系统的铁路控制中心和铁路系统的三个路段。SCADA 系统轮询铁路路段以获得列车、信号系统、牵引电气化系统、自动售票机等的状态信息。这些信息也被传递到位于铁路控制中心的 HMI 站点的操作员控制台上。SCADA 系统还监控铁路控制中心的操作员的输入并分发高级操作员命令给铁路路段组件。此外，SCADA 系统监视个别铁路路段的条件，并根据这些条件发出指令（例如，关闭一辆列车以防止它进入一个已经确定被洪水淹没的区域或被另一列火车占用的区域）。

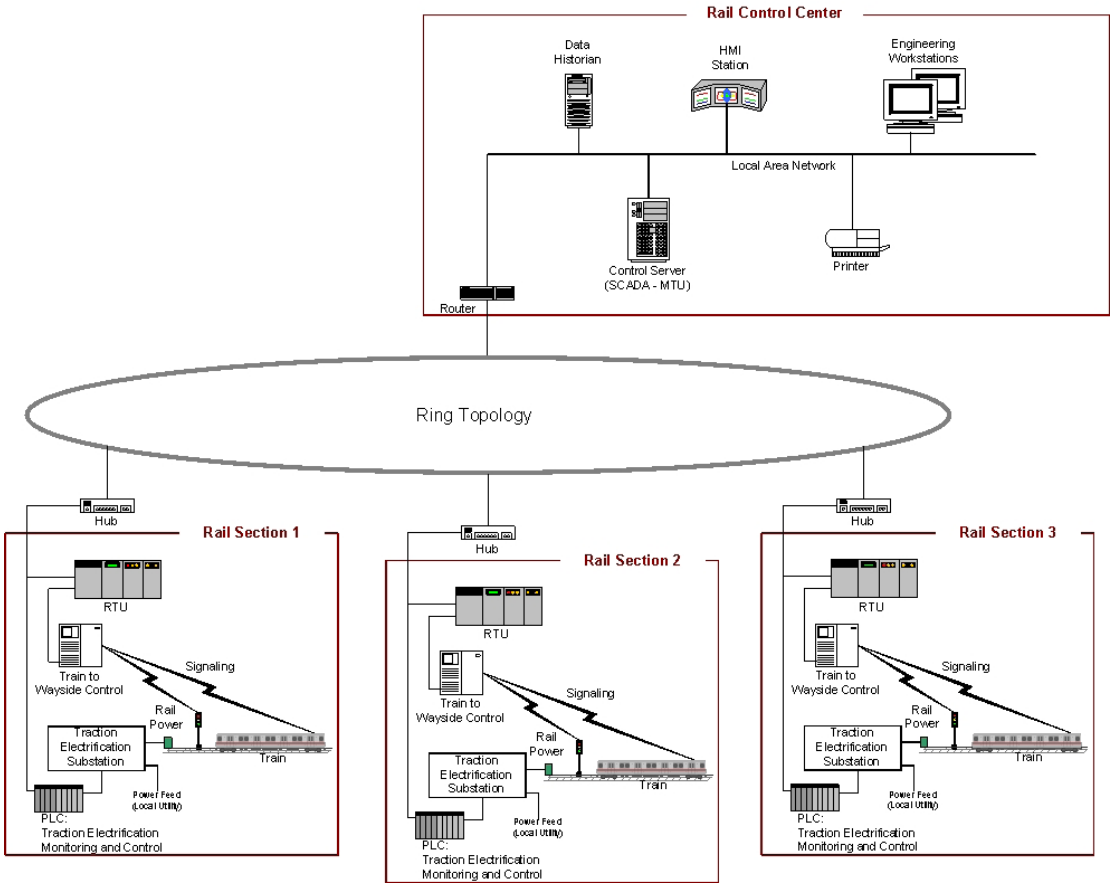


图2-6 SCADA系统实现举例(铁路监控)

2.5 分布式控制系统（DCS）

DCS 系统用于控制在同一地理位置的生产系统，如炼油厂，水和污水处理，发电设备，化学品制造工厂，和医药加工设施等行业。这些系统通常是过程控制或分立部分的控制系统。一个 DCS 使用一个集中的监控回路来调解一组分担着贯穿整个生产过程的全部任务的本地控制器。通过将生产系统模块化，DCS 降低了单一故障对整个系统的影响。在许多现代系统中，DCS 是与企业网络的接口，为企业的运营者提供生产视图。

图 2-7 描述了一个 DCS 实现的例子，显示了 DCS 的组件和总体配置。这个 DCS 包括从底层生产过程到公司或企业层面的整个设施。在这个例子中，监督控制器（控制服务器）通过控制网络与其下属通信。监控台发送设置点给分布的场站控制器，并向后者请求数据。分布式控制器根据控制服务器的命令和过程传感器的反馈控制它们的过程执行器。

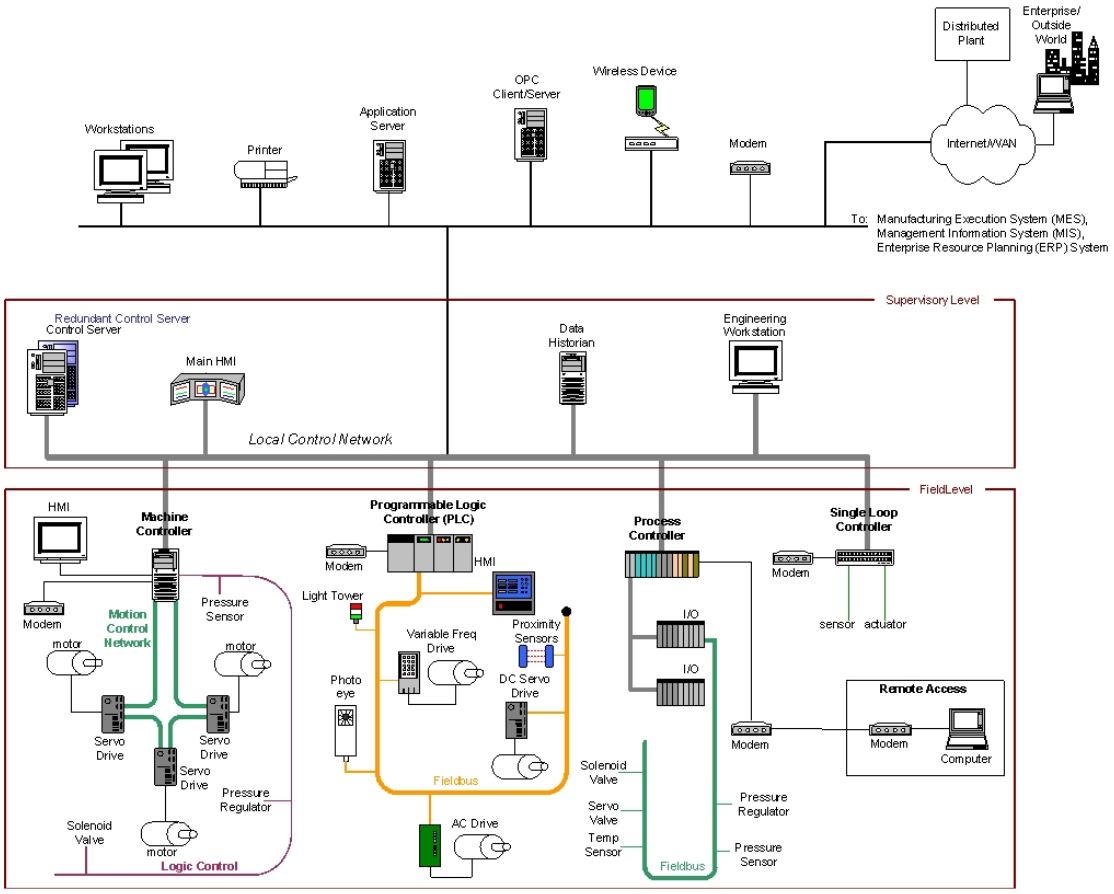


图2-7 DCS实现举例

图 2-7 给出了一个 DCS 系统上的低级控制器的例子。图中所示的现场控制设备包括一个 PLC，一个过程控制器，一个单回路控制器和一台机器控制器。单回路控制器的接口传感器和执行器使用点对点连线，而其他三个现场设备集成到现场总线网络上，与过程传感器和执行器进行连接。现场总线网络消除了控制器和单个现场传感器和执行器之间的点对点接线需要。此外，现场总线允许比控制更多的功能，包括现场设备的诊断，并可以实现在现场总线内的控制算法，从而避免了每个控制操作到 PLC 的信号回路。由工业集团设计的标准工业通信协议，如 Modbus 和 Fieldbus 往往被用在控制网络和现场总线网络上。

除了监管级和现场级控制回路，中间级别的控制也可能存在。例如，在一个 DCS 控制一个独立部件制造工厂的情况下，可以为厂房内的每个单元格设置一个中间级监控器。该监控器将包括一个制造单元，包含处理一个部件的机器控制器和处理原料库存和最终产品的机器人控制器。可能有几个这样的单元在主 DCS 监控环路下管理现场级控制器。

2.6 可编程逻辑控制器（PLC）

PLC 可用在 SCADA 和 DCS 系统中，作为整个分级系统的控制部件，通过如在上节中所述的反馈控制，提供对过程的本地管理。当用在 SCADA 系统中时，它们提供与 RTU 相同的功能。当用在 DCS 中时，PLC 被实现为监控机制内的本地控制器。PLC 也被实现为更小的控制系统配置的主要组件。PLC 具有一个用户可编程的存储器，用于存储指令以实现特定功能，如 I / O 控制、逻辑、定时、计数、三种模式的比例-积分-微分（PID）控制、通信、算术以及数据和文件处理。图 2-8 显示的制造过程由 PLC 通过现场总线网络控制。PLC 可通过工程师工作站上的一个编程接口访问，数据存储在一个历史数据库中，全部通过 LAN 连接。

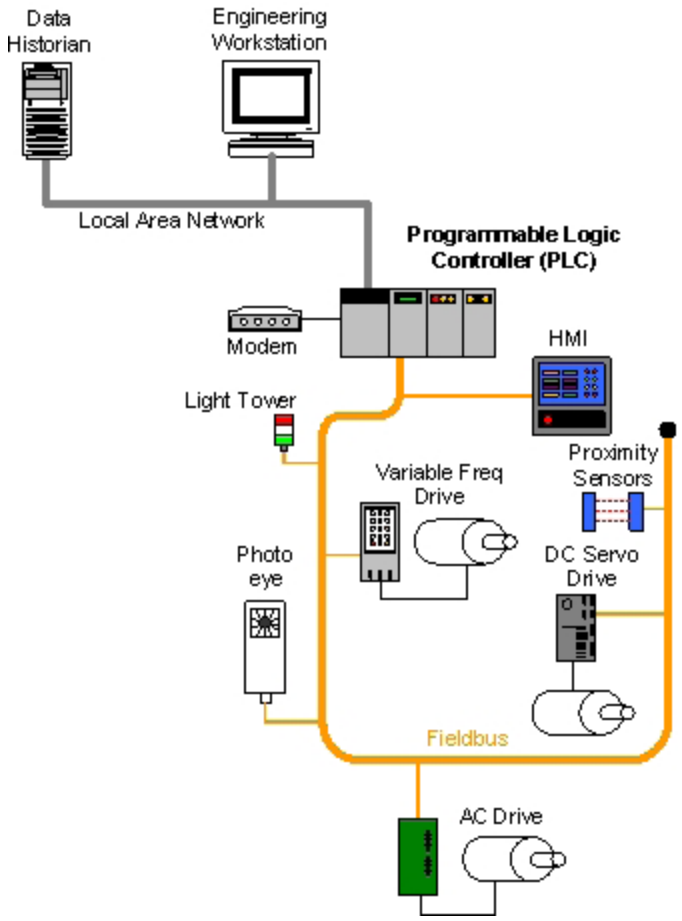


图2-8 PLC 控制系统实现举例

2.7 工业部门和他们的相互依存性

电力输配电网络行业利用地理上分散的 SCADA 控制技术操作高度相互关联的和动态的系统，包括数以千计的公共和私营机构和农村合作社，从而为最终用

户供电。SCADA 系统通过在一个集中的位置从远程现场控制站点收集数据，并发向其出指令，从而实现对电力配送的监视和控制。SCADA 系统也可用于监测和控制水、油和天然气的配送，包括管道、船舶、卡车、铁路系统以及污水收集系统。

SCADA 系统和 DCS 往往是通过网络连接在一起。这种情况出现在电力控制中心和发电厂。虽然发电厂的运作是由 DCS 控制，但 DCS 必须与 SCADA 系统通信，协调产量与输配电需求。

美国关键基础设施通常被称为一个“系统的系统”，因为其各工业部门之间存在的相互依赖性以及业务合作伙伴之间的互连。关键基础设施是高度互联的，并以复杂的方式互相依赖着，不仅在物理上，也通过信息和通信技术的主机。在一个基础设施中发生的事件，可以通过级联和故障升级等直接或间接影响其他基础设施。

电力通常被认为是相互依存的关键基础设施中最普遍的中断来源之一。举一个例子，一个级联故障，可以因为一个用于电力传输 SCADA 系统的微波通信网络的中断而触发。监测和控制能力的缺乏可能会导致大型发电单位不得不采取脱机，事件将导致传输变电所的功率损耗。这种损失可能会导致严重的不平衡，引发整个电网级联故障。这可能会导致大面积停电，可能会潜在影响依赖于电力网格的石油和天然气生产、炼油业务、水处理系统、污水收集系统和管道运输系统。

3. ICS 特性，威胁和脆弱性

在今天使用的很多 ICS 是多年前开发的，在公共和私人网络、桌面计算或互联网成为业务运营的通用组件之前很长时间。这些系统被设计为满足性能、可靠性、安全性和灵活性的要求。在大多数情况下，他们是与外部网络物理隔离的，基于专有硬件、软件和通信协议，它们包括基本的错误检测和纠错能力，但缺乏在今天的互联系统中所需的安全通信能力。虽然有人关注可靠性、可维护性和可用性（RMA），但在解决统计性能和故障时，对这些系统内的网络安全措施的需求是没有预料到的。当时，ICS 安全就意味着物理上保护对网络和控制系统的控制台的访问。

ICS 的发展平行于 1980 年代和 1990 年代的微处理器、个人电脑和网络技术

的演进，在 1990 年代后期基于互联网的技术开始进入到 ICS 的设计中。这些 ICS 的变化将它们暴露给新的威胁类型，并显著增加了 ICS 受到损害的可能性。本节介绍了 ICS 的独特的安全特性，在 ICS 实现中的漏洞，和 ICS 可能面临的威胁和事故。3.7 节会介绍几个实际的 ICS 网络安全事故的例子。

3.1 ICS 和 IT 系统的比较

最初，ICS 与 IT 系统没有一点相似之处，ICS 是运行专有控制协议、使用专门硬件和软件孤立的系统。现在用广泛使用的、低成本的互联网协议（IP）设备取代专有的解决方案，从而增加了网络安全漏洞和事故的可能性。随着 ICS 采用这种解决方案，以促进企业连接和远程访问能力，并正在使用行业标准的计算机、操作系统（OS）和网络协议进行设计和实施，它们已经开始类似于 IT 系统了。这种集成支持新的 IT 能力，但相比原先的系统，它对 ICS 提供的与外界的隔离大大减少，产生了保护这些系统的更大需求。虽然安全解决方案已经被设计来处理这些典型的 IT 系统安全问题，但是在引进这些相同的解决方案到 ICS 环境中时，必须采取特殊的防护措施。在某些情况下，需要为 ICS 环境量身定制新的安全解决方案。

ICS 有许多区别于传统 IT 系统的特点，包括不同的风险和优先级别。其中包括对人类健康和生命安全的重大风险，对环境的严重破坏，以及金融问题如生产损失和对国家经济的负面影响。 ICS 有不同的性能和可靠性要求，其使用的操作系统和应用程序对典型的 IT 支持人员而言可能被认为是不方便的。此外，安全和效率的目标有时会与控制系统的设计和操作的安全性发生冲突（如，需要密码验证和授权不应妨碍或干扰 ICS 的紧急行动。）下面列出了一些 ICS 的特殊安全考虑：

性能要求。ICS 通常是时间要求紧迫的，关注由单个安装所指示的延迟和抖动的可接受水平标准。有些系统要求确定性的响应。高吞吐量对 ICS 通常是没有必要的。相比之下，IT 系统通常需要高吞吐量，但通常可以承受某种程度的延时和抖动。

可用性要求。许多 ICS 过程在本质上是连续的。控制工业生产过程系统的意外停电是不能接受的。停电往往必须有计划且提前预定时间（天/周）。全面的部

署前测试是必不可少的，以确保 ICS 的高可用性。除意外停电外，许多控制系统也不能做到在不影响生产的情况下轻易地停止和启动。在某些情况下，正在生产的产品或正在使用的设备比被转达的信息更重要。因此，典型的 IT 战略，如重新启动一个组件，由于其 ICS 的高可用性、可靠性和可维护性要求的不利影响，通常是不被接受的解决方案。一些 ICS 会采用冗余组件，且常常并行运行，当主要组件不可用时保证连续性。

风险管理要求。在一个典型的 IT 系统中，数据保密性和完整性通常是被关心的首要问题。对于 ICS 而言，人身安全和容错（以防止损害生命或危害公众健康或信心），合规性，设备的损失，知识产权损失，以及产品的丢失或损坏等，才是主要的关注点。负责操作、保护和维护 ICS 的人员必须了解 safety 和 security 之间的重要联系。

体系架构安全焦点。在一个典型的 IT 系统中，安全的首要重点是保护 IT 资产的运行，无论是集中的或分散的，还有就是在这些资产中存储或相互之间传输的信息。在某些体系架构中，集中存储和处理的信息是更为关键的，要给予更多的保护。而对于 ICS，边缘客户端（如 PLC，操作员工作站，DCS 控制器）更需要仔细保护，因为它们是对结束过程的控制直接负责任的。ICS 中央服务器的保护仍然是非常重要的，因为中央服务器可能对每一个边缘设备产生不利影响。

物理相互作用。在一个典型的 IT 系统中，没有物理与环境之间的互动。ICS 可以与在 ICS 域中的物理过程和后果有非常复杂的相互作用，这可以体现在物理事件中。必须测试所有被集成到 ICS 中的安全功能（例如，在一个可参照的 ICS 上的离线），以证明它们不损害 ICS 的正常功能。

时间要求紧迫的响应。在一个典型的 IT 系统中，不需要太考虑数据流就可以实现访问控制。对于一些 ICS 而言，自动响应时间或对人机交互的系统响应是非常关键的。例如，在 HMI 上要求提供密码认证和授权时必须不能妨碍或干扰 ICS 的紧急行动。信息流必须不被中断或受到影响。对这些系统的访问，必须有严格的物理安全控制。

系统操作。ICS 的操作系统（OS）和应用程序可能无法容忍典型的 IT 安全实践。老系统特别容易受到资源不可用和计时中断的危害。控制网络往往比较复杂，需要不同层次的专业知识（例如，控制网络通常由控制工程师管理，而不是

IT 人员)。软件和硬件都更难以在操作控制系统网络中升级。许多系统可能没有所需的功能，包括加密功能，错误记录，和密码保护。

资源的限制。ICS 和它们的实时操作系统往往是资源受限的系统，通常不包括典型的 IT 安全功能。在 ICS 组件上可能没有计算资源用来在这些系统上加装流行的安全功能。此外，在某些情况下，不允许用第三方安全解决方案，是因为根据 ICS 供应商许可和服务协议，一旦在没有供应商的确认或批准下就安装了第三方的应用程序，可能会丢失服务支持。

通信。在 ICS 环境中用于现场设备控制和内部处理器通信的通信协议和媒体通常与通用的 IT 环境不同，可能是专有的。

变更管理。变更管理对维持 IT 和控制系统的完整性都是至关重要的。未打补丁的软件代表了系统的最大漏洞之一。IT 系统的软件更新，包括安全补丁，根据适当的安全策略和程序，通常都是实时应用的。此外，这些程序往往是使用基于服务器的工具自动实现的。ICS 的软件更新往往就无法及时实施，因为这些更新需要由工业控制应用程序的供应商和应用程序的最终用户充分测试后才能实施，而且 ICS 的中断往往必须是事先规划和预定好时间（天/周）的。 作为更新过程的一部分，ICS 可能还需要重新验证。另一个问题是，许多 IC 采用了旧版本的操作系统，而供应商不再提供支持。因此，可用的修补程序可能不适用。变更管理也适用于硬件和固件。当变更管理过程应用于 ICS 时，需要由 ICS 专家（例如，控制工程师）与安全和 IT 人员一起进行仔细评估。

管理的支持。典型的 IT 系统允许多元化的支持模式，也许支持不同的但相互关联的技术架构。对于 ICS，服务支持通常是由一个单一的供应商提供，可能就没有多元化的和从其他供应商处获得的具有互操作性的支持解决方案。

组件寿命。典型的 IT 组件的寿命一般为 3 至 5 年，主要是由于技术的快速演变。对于 ICS 而言，在许多情况下，技术是为非常特殊的用户和实现而开发的，所部署的技术的生命周期通常在 15 至 20 年，有时甚至时间更长。

组件访问。典型的 IT 组件通常是本地的和容易访问的，而 ICS 组件可以分离、远程部署，并需要大量的物力以获得对它们的访问。

表 3-1 总结了一些 IT 系统和 ICS 之间的典型差异。

表3-1 IT系统和ICS的差异总结

分类	信息技术系统	工业控制系统

性能需求	非实时 响应必须是一致的 要求高吞吐量 高延迟和抖动是可以接受的	实时 响应是时间紧迫的 适度的吞吐量是可以接受的 高延迟和/或抖动是不能接受的
可用性需求	重新启动之类的响应是可以接受的的 可用性的缺陷往往可以容忍的，当然要取决于系统的操作要求	重新启动之类的响应可能是不能接受的，因为过程的可用性要求 可用性要求可能需要冗余系统 中断必须有计划和提前预定时间（天/周） 高可用性需要详尽的部署前测试
管理需求	数据保密性和完整性是最重要的的 容错是不太重要的 – 临时停机不是一个主要的风险 主要的风险影响是业务操作的延迟	人身安全是最重要的的，其次是过程保护 容错是必不可少的，即使是瞬间的停机也可能无法接受 主要的风险影响是不合规，环境影响，生命、设备或生产损失
体系架构安全焦点	首要焦点是保护 IT 资产，以及在这些资产上存储和相互之间传输的信息。 中央服务器可能需要更多的保护	首要目标是保护边缘客户端（例如，现场设备，如过程控制器） 中央服务器的保护也很重要
未预期的后果	安全解决方案围绕典型的IT 系统进行设计	安全工具必须先测试（例如，在参考 ICS 上的离线），以确保它们不会影响 ICS 的正常运作
时间紧迫的交互	紧急交互不太重要 可以根据必要的安全程度实施严格限制的访问控制	对人和其他紧急交互的响应是关键 应严格控制对 ICS 的访问，但不应妨碍或干扰人机交互
系统操作	系统被设计为使用典型的操作系统 采用自动部署工具使得升级非常简单	与众不同且可能是专有的操作系统，往往没有内置的安全功能 软件变更必须小心进行，通常是由软件供应商操作，因其专用的控制算法，以及可能要修改相关的硬件和软件
资源限制	系统被指定足够的资源来支持附加的第三方应用程序如安全解决方案	系统被设计为支持预期的工业过程，可能没有足够的内存和计算资源以支持附加的安全功能
通信	标准通信协议 主要是有线网络，稍带一些本地化的无线功能的 典型的 IT 网络实践	许多专有的和标准的通讯协议 使用多种类型的传播媒介，包括专用的有线和无线（无线电和卫星） 网络是复杂的，有时需要控制工程师的专业知识

变更管理	在具有良好的安全策略和程序时，软件变更是及时应用的。往往是自动化的程序。	软件变更必须进行彻底的测试，以递增方式部署到整个系统，以确保控制系统的完整性。 ICS 的中断往往必须有计划，并提前预定时间（天/周）。 ICS 可以使用不再被厂商支持的操作系统。
管理支持	允许多元化的支持模式	服务支持通常是依赖单一供应商
组件生命周期	3-5 年的生存期	15-20 年的生存期
组件访问	组件通常在本地，可方便地访问	组件可以是隔离的，远程的，需要大量的物力才能获得对其的访问

ICS 可用的计算资源（包括 CPU 时间和内存）往往是非常有限的，因为这些系统，旨在最大限度地控制系统资源，很少甚至没有额外容量给第三方的网络安全解决方案。此外，在某些情况下，第三方安全解决方案根本不被允许，因为供应商的许可和服务协议，而且如果安装了第三方应用程序，可能发生服务支持的损失。另一个重要的考虑因素是 IT 网络安全和控制系统的专业知识通常不是属于同一组人员的。

综上所述，ICS 和 IT 系统之间的业务和风险的差异，产生了在应用网络安全和业务战略时增长的复杂性需求。一个由控制工程师、控制系统运营商和 IT 安全专业人员构成的跨职能团队，应当紧密合作以理解安装、操作与维护与控制系统相关的安全解决方案时可能产生的影响。工作于 ICS 的 IT 专业人员在部署之前需要了解信息安全技术的可靠性影响。在 ICS 上运行的一些操作系统和应用可能无法正常运行商业现行（COTS）的 IT 网络安全解决方案，因其专用的 ICS 环境架构。

3.2 威胁

控制系统面临的威胁可以来自多种来源，包括对抗性来源如敌对政府、恐怖组织、工业间谍、心怀不满的员工、恶意入侵者，自然来源如从系统的复杂性、人为错误和意外事故、设备故障和自然灾害。为了防止对抗性的威胁（以及已知的自然威胁），需要为 ICS 创建一个纵深的防御策略。表 3-2 列出了针对 ICS 的可能的威胁。请注意此列表中是按字母顺序排列而不是按威胁大小。

表3-2 针对ICS的对抗性威胁

威胁代理	描述
Attackers 攻击者	攻击者入侵网络，只为获得挑战的快感或在攻击社团中吹牛的资本。虽然远程攻击曾经需要一定的技能或计算机知识，但是攻击者现在却可以从互联网上下载攻击脚本和协议，并向受害网站发动它们。因此，虽然攻击工具越来越高级，它们也变得更容易使用。许多攻击者并不具备必要的专业知识来威胁困难的目标如美国的关键网络。然而，攻击者遍布全球，构成了一个比较高的威胁，其造成的孤立的或短暂的中断可引起严重损害。
Bot-network operators 僵尸网络操纵者	僵尸网络操纵者即攻击者；然而，他们侵入系统不是为了挑战或炫耀，而是将多个系统联合起来发动攻击和散布钓鱼，垃圾邮件和恶意软件攻击。有时在地下市场可以获得被攻破的系统和网络的服务，例如，购买一次拒绝服务攻击或使用发送垃圾邮件或钓鱼式攻击的服务器。
Criminal groups 犯罪集团	犯罪团伙试图攻击系统以获取钱财。具体来说，有组织的犯罪集团利用垃圾邮件，网络钓鱼，间谍软件/恶意软件进行身份盗窃和在线欺诈。国际企业间谍和有组织的犯罪集团也通过自己的能力进行工业间谍活动和大规模的货币盗窃，并聘请或发展攻击人才，从而构成对美国国家的威胁。一些犯罪团伙可能用网络攻击威胁某个组织从而试图勒索金钱。
Foreign intelligence services 外国情报服务	外国情报部门使用网络工具作为他们的信息收集和间谍活动的一部分。此外，一些国家正在积极发展信息战学说、程序和能力。这类能力使单一的实体就能造成显著的和严重的影响，通过扰乱供电、通信和支持军事力量的经济基础设施，其后果可能会影响美国公民的日常生活。
Insiders 内部人员	心怀不满的内部人员是计算机犯罪的主要来源。内部人员可能并不需要大量的计算机入侵相关知识，因为他们对目标系统的了解，往往使他们能够不受限制地访问系统从而对系统造成损害或窃取系统数据。内部威胁还包括外包供应商以及员工意外地引入恶意软件到系统中。内部人员可能包括员工、承包商或商业合作伙伴。 不适当的策略、程序和测试也会导致对 ICS 的影响。对 ICS 和现场设备的影响程度可以是从琐碎的到重大的损坏。来自内部的意外影响是发生概率最高的事件之一。
Phishers 钓鱼者	钓鱼者是执行钓鱼计划的个人或小团体，企图窃取身份或信息以获取金钱。钓鱼者也可以使用垃圾邮件和间谍软件/恶意软件来实现其目标。
Spammers 垃圾邮件发送者	垃圾邮件发送者包括个人或组织，他们散布不请自来的电子邮件，包含隐藏的或虚假的产品销售信息，进行网络钓鱼计划，散布间谍软件/恶意软件，或有组织的攻击（例如 DoS）。
Spyware/malware authors 间谍/恶意软件作者	具有恶意企图的个人或组织通过制作和散布间谍软件和恶意软件进行对用户的攻击。已经有一些破坏性的电脑病毒和蠕虫对文件和硬盘驱动器造成了损害，包括 Melissa 宏病毒，Explore.Zip 蠕虫，CIH（切尔诺贝利）病毒，尼姆达，红色代码，Slammer

	（地狱），和 Blaster（冲击波）。
Terrorists 恐怖份子	恐怖份子试图破坏、中断或利用关键基础设施来威胁国家安全，造成大量人员伤亡，削弱美国经济，并损害公众的士气和信心。恐怖分子可能使用网络钓鱼或间谍软件/恶意软件，以筹集资金或收集敏感信息。恐怖分子可能袭击一个目标，以从其他目标上转移视线或资源。
Industrial spies 工业间谍	工业间谍活动，旨在通过秘密的方法获得知识产权和技术诀窍

3.3 ICS 系统潜在的脆弱性

本章所列举一些脆弱性是在工业控制系统（ICS）中可能会遇到的，这些脆弱性排列的先后顺序不代表发生的可能性或影响的级别大小。为了有助于信息安全决策，这些脆弱性被划分成策略与程序类、平台类和网络类脆弱性，大多数在工业控制系统中常出现的一些脆弱性都可与归集到这几类中，但也有一些例外，对于一些特殊的工业控制系统脆弱性，也可能不包含在以上分类中。关于工业控制系统中出现的漏洞的详细信息，在美国计算机应急小组（US-CERT）控制系统网站上有详细的研究。

在研究安全漏洞时，容易全身心投入并非常有兴致地去研究并发布一些漏洞信息，但到最后可能会发现这些漏洞的影响很小。如附件E中所述，FIPS199标准中已对信息和信息系统进行了安全事件分类，分类的依据是根据对信息和信息系统的影响程度，这些信息和信息系统是组织完成业务使命所依赖的，也是组织需要保护和日常维护的。

对于工业控制系统安全漏洞带来的风险需要有一套风险评估的方法，安全风险的大小，同黑客挖掘到漏洞并找到针对该漏洞的攻击程序的可能性，以及一旦发生攻击行为后对信息资产的影响大小密切相关，此外，该漏洞造成的风险大小还同以下一些因素相关，包括：

- 计算机、网络架构及环境条件
- 已部署的安全防护措施
- 黑客发起攻击的技术难度
- 内部嗅探的可能性

- 事故的后果
- 事故的成本

这些风险评估的细节在后续的第 4-6 章中有进一步详述。

3.3.1 策略和程序方面的脆弱性

安全漏洞在工业控制系统中常见到，主要是由于安全策略及程序文件不完全、不适合或文件的缺失，包括安全策略及实施指南（实施程序）等。安全策略程序文档，包括管理支持等，是安全工作的基础，通过正确的引导与实施，企业安全策略的完善能够减少安全漏洞隐患，比如通过调制解调器连接到工业控制系统时口令的使用与维护要求。表 3-3 描述了工业控制系统中可能存在的策略与程序方面的安全漏洞：

表 3-3 策略和程序上的脆弱性

漏洞	描述
工业控制系统安全策略不当	对于工业控制系统，由于安全策略不当或策略不具体，造成安全漏洞常有发生。
没有正式的工业控制系统安全培训和安全意识培养	书面的、正式的安全培训以及安全意识培养设计的目的是为了使全体职员了解最新的计算机安全标准和最佳实践，并使组织的安全策略与程序同步更新。
安全架构和设计不足	安全管理工程师由于安全培训机会较少，对产品不够熟悉，直到目前为止供应商还没有把一些安全特征移植到产品中。
对于工业控制系统，没有开发出明确具体、书面的安全策略或程序文件	具体、书面的安全策略或程序文件应当制定并对全体员工进行培训，这是一个正确的安全建设的根基。
工业控制系统设备操作指南缺失或不足	设备操作指南应当及时更新并保持随时可用，这些操作指南是工业控制系统发生故障时安全恢复所必须的组成部分。

安全执行中管理机制的缺失	负有安全管理责任的员工应当对安全策略与程序文件的管理、实施负责。
工业控制系统中很少或没有安全审计	独立的安全审计人员应当检查和验证系统日志记录并主动判断安全控制措施是否充分，以保证合乎 ICS 安全策略与程序文件的规定。审计人员还应当经常检查 ICS 安全服务的缺失，并提出改进建议，这样能够使安全控制措施更有效。
没有明确的 ICS 系统业务连续性计划或灾难恢复计划	组织应当准备业务连续性计划或灾难恢复计划并进行定期演练，以防基础设施重大的软硬件故障发生，如果业务连续性计划或灾难恢复计划缺失，ICS 系统可能会造成业务中断和生产数据丢失。
没有明确具体的配置变更管理程序	ICS 系统硬件、固件、软件的变更控制程序和相关程序文件应当严格制定，以保证 ICS 系统得到实时保护，配置变更管理程序的缺失将导致安全脆弱性的发生，增大安全风险。

3.3.2 平台方面的脆弱性

ICS 系统由于程序瑕疵、配置不当或维护较少而出现一些安全的脆弱性，包括 ICS 系统硬件、操作软件和应用软件，通过各种安全控制措施的实施，可以缓解因安全脆弱性问题导致的安全风险，比如，操作系统和应用程序补丁，物理访问控制，安全防护软件（如病防护软件），下表是一些潜在的平台方面的脆弱性的描述。

- 表 3-4.平台配置方面的脆弱性
- 表 3-5 平台硬件方面的脆弱性
- 表 3-6.平台软件方面的脆弱性；
- 表 3-7.平台恶意软件防护方面的脆弱性；

表 3-4.平台配置方面的脆弱性

脆弱性	描述
操作系统安全漏洞被发现后供应商可能没有开发出相应的补丁程序	由于 ICS 系统软件及操作系统更新的复杂性，补丁程序的更新必须面对广泛的回归测试，从测试到最终发布之间有较长的漏洞暴露周期。
操作系统和应用软件补丁程序没有及时安装	老版本的操作系统或应用软件可能存在最新发现的安全漏洞，组织的程序文件中应当明确如何维护补丁程序；
操作系统和应用软件补丁程序没有进行广泛测试	操作系统和应用软件补丁程序没有进行广泛测试就安装上线，可能会对 ICS 系统的正常运转产生影响，组织的程序文件中应当明确对新出现的补丁程序进行广泛测试；
使用缺省配置	如使用缺省配置可能会导致不安全或不必要的端口或服务没有关闭；
关键配置文件没有存储备份措施	组织应当在程序文件中明确对配置文件进行存储与备份，以防偶然事故的发生，防止黑客对配置文件进行更改，造成业务中断或业务数据的丢失。组织应当在程序文件中明确如何维护 ICS 系统的安全配置信息；
移动设备数据未保护	如果敏感数据（如密码，电话号码)被明文储存在手提设备例如笔记本电脑，掌上电脑等，这些设备被卡丢失或被盗，系统安全可能存在风险。需要建立政策、程序、机制来保护移动设备上的数据。
密码策略不当	在使用密码时需要定义密码策略，包括密码强度、更改周期等，如果没有密码策略，系统可能没有适当的密码控制措施，使未授权用户更可能擅自访问机密信息。考虑到 ICS 系统及员工处理复杂密码的能力，组织应当吧密码策略作为整体 ICS 安全策略的一个组成部分来制定。
未设置密码	在 ICS 各组件上应实施密码访问策略，以防止未经

	授权的访问。密码相关的漏洞，包括没有密码： ✧ 登录系统（如果系统有用户帐户） ✧ 系统开机（如果系统有没有用户帐户） ✧ 系统的屏幕保护程序（如果 ICS 组件，随着时间的推移无人值守） 密码认证策略不应妨碍或干扰 ICS 的应急响应活动。
密码丢失	密码应保密，以防止未经授权的访问。密码披露的例子包括： 张贴在众目睽睽下，靠近本地系统 和其他人共享用户个人帐户密码 通过社会工程学，黑客获取通讯密码 通过未受保护的通信链路发送未加密的密码
密码猜解	弱口令很容易被黑客或计算机算法猜解，从而获得未经授权的访问。例子包括： ✧ 很短的密码，简单（例如，所有的小写字母），或以其他方式不符合典型的强度要求。密码强度也取决于对具体 ICS 能力，以处理更严格的密码 ✧ 默认的供应商的密码 ✧ 在指定的时间间隔不更改密码
没有访问控制措施	访问控制措施不当可能会导致给ICS用户过多或过少的特权。以下举例说明每一种情况下： 系统默认访问控制策略允许系统管理员权限 系统配置不当，操作人员无法在紧急情况下采取应急响应措施 应制定访问控制策略，作为ICS安全策略的一部分，

表 3-5.平台硬件方面的脆弱性

脆弱性	描述
安全变更时没有充分进行测试	许多 ICS 的设施，尤其是较小的设施，没有检测设备，业务系统的安全性变更测试必须在现场环境下进行。
对关键设备没有充分的物理保护措施	访问控制中心，现场设备，便携设备，媒体，和其他 ICS 组件需要被控制。许多远程站点往往没有人员和物理监测控制措施。
未授权用户能够接触设备	ICS 设备的物理访问，应只限于必要的人员，同时考虑到安全的要求，如紧急关机或重新启动。未授权访问 ICS 设备可能会导致下列情况： ✧ 物理盗窃数据和硬件 ✧ 数据和硬件的物理损坏或毁坏 ✧ 擅自变更功能的环境（例如，数据连接，可移动媒体擅自使用，添加/删除资源） ✧ 物理数据链路断开 ✧ 难以检测的数据拦截（击键和其他输入记录）
不安全的远程访问 ICS 组件	调制解调器和其他远程访问措施的开启，使维护工程师和供应商获得远程访问系统的能力，应部署安全控制，以防止未经授权的个人，从进入到 ICS。
双网卡（NIC）连接网络	使用双网卡连接到不同网络的机器可能会允许未经授权的访问和传递数据从一个网络到另一个。
未注册的资产	要维护 ICS 的安全，应该有一个准确的资产清单。一个控制系统及其组成部分的不准确，可能为非授权用户访问 ICS 系统留下后门。
无线电频率和电磁脉冲（EMP）	用于控制系统的硬件是脆弱的无线电频率和电磁脉冲（EMP）。影响范围可以从暂时中断的指令和控制电路板的永久性损害。
无备用电源	对于关键资产如果没有备用电源，电力不足将关闭

	ICS 系统，并可能产生不安全的情况。功率损耗也可能导致不安全的默认设置。
环境控制缺失	环境控制的缺失可能会导致处理器过热。有些处理器将关闭以自我保护;有些可能会继续工作，但在输出功率较小，产生间歇性的错误;如果过热的话有的只是融化，。
关键设备没有冗余备份	关键设备没有冗余备份可能导致单点故障的发生。

表 3-6.平台软件方面的脆弱性

脆弱性	描述
缓冲区溢出	ICS 系统软件可能会出现缓冲区溢出，黑客可能会利用这些来来发起各种攻击
安装的安全设备没有开启防护功能	随产品安装的安全功能是无用的，如果他们不启用或至少确定被禁用
拒绝服务攻击	ICS 系统软件可能会受到 DOS 攻击，可能会导致合法用户不能访问，或系统访问响应延迟。
因未定义、定义不清，或“非法”定义导致操作错误	一些ICS在执行操作指令时对输入的数据包缺乏有效检测，这些数据包的格式不正确或含有非法或其他意外的字段值。
过程控制的 OLE（OPC），依赖于远程过程调用（RPC）和分布式组件对象模型（DCOM）	没有更新的补丁，对于已知的 RPC / DCOM 漏洞来说 OPC 是脆弱的。
使用不安全的全行业 ICS 协议	分布式网络协议（DNP）3.0，MODBUS，PROFIBUS，以及其他协议，应用于多个行业，协议信息是公开的。这些协议通常很少或根本没有内置的安全功能
明文传输	许多 ICS 的协议传输介质之间的明文传输的消息，使得它们很容易被对手窃听。
开启了不必要的服务	许多平台上运行着有各种各样的处理器和网络服

	务。不必要的服务很少被禁用，可能会被利用。
专有软件的使用已经在会议和期刊上讨论过	在国际 IT、ICS 和“黑帽”会议讨论过，并在技术论文，期刊或目录服务器上已发表过。此外，ICS 维修手册可从供应商那里获得。这些信息可以帮助黑客成功地对 ICS 发起攻击。
软件配置和设计上认证和访问控制措施不足	未经授权的访问，配置和编程软件，可能会损坏设备。
没有安装入侵检测/防护设备	安全事件的发生可能会导致系统可用性的损失；IDS/ IPS 软件可能会停止或防止各类攻击，包括 DoS 攻击，也识别攻击内部主机与蠕虫感染者，如。IDS / IPS 系统软件必须在部署之前进行测试，以确定它不会影响 ICS 系统的正常运行。
日志未维护	如果没有适当和准确的日志记录，可能无法以确定是什么原因造成安全事件的发生。
安全事故未及时发现	日志和其他安全设备已安装，他们可能不是建立在实时监测的基础上，因此，安全事故可能不能迅速发现和处理。

表 3-7.恶意软件保护方面的脆弱性

脆弱性	**描述**
防恶意软件未安装	恶意软件可能会导致性能下降，失去了系统的可用性，并捕捉，修改，或删除数据。恶意软件保护软件，如杀毒软件，是需要，以防止被恶意软件感染的系统。
防恶意软件版本或特征码未更新	未更新的防恶意软件版本和定义可能会使系统恶意软件攻击威胁离开系统的开放新的恶意软件威胁。
防恶意软件安装前未进行广泛的测试	防恶意软件安装前未进行广泛的测试可能会对 ICS 系统正常运转产生影响。

3.3.3 网络方面的脆弱性

在 ICS 中的漏洞可能会出现缺陷，错误配置，或对 ICS 网络及与其他网络的连接管理不善。这些漏洞可以通过各种安全控制消除或者弱化，如防御深入的网络设计，网络通信加密，限制网络流量，并提供网络组件的物理访问控制。

本节中的表描述了潜在的平台漏洞：

- 表 3-8。网络配置漏洞
- 表 3-9。网络硬件漏洞
- 表 3-10。网络边界漏洞
- 表 3-11。网络监控和记录漏洞
- 表 3-12。通信中的漏洞
- 表 3-13。无线连接中的漏洞

表 3-8 网络配置方面的脆弱性

脆弱性	描述
网络安全架构	ICS 系统网络基础架构常常根据业务和运营环境的变化而发展变化，但很少考虑潜在的安全影响的变化。随着时间的推移，安全漏洞可能会在不经意间在基础设施内的特定组件中产生，如果没有补救措施，这些漏洞可能成为进入 ICS 的后门。
未实施数据流控制	数据流的控制，如访问控制列表（ACL），需要限制哪些系统可以直接访问网络设备。一般来说，只有指定的网络管理员应该能够直接访问这些设备。数据流的控制应确保其他系统不能直接访问设备。
安全设备配置不当	使用默认配置，往往导致不安全和不必要的开放端口和利用的网络服务的主机上运行。配置不当的防火墙规则和路由器 ACL，可以允许不必要的流量通行。

网络设备配置文件未保存或备份	一旦网络发生偶然的或黑客发起的配置变更事件，需要有可行的操作程序，以维护网络系统的高可用性，并防止业务数据的丢失。文件化的程序应制定来维护网络设备的配置设置。
数据传输中口令未加密	密码通过传输介质明文传输，易被黑客嗅探，并获得对网络设备的未授权访问。这样黑客可能破坏 ICS 的操作或监控 ICS 网络活动。
网络设备密码长期未修改	密码应定期更换，这样，如果未授权用户获得密码，也只有很短的时间访问网络设备。未定期更换密码可能使黑客破坏 ICS 的操作或监视器 ICS 的网络活动。
访问控制措施不充分	黑客未授权访问网络系统可能会破坏 ICS 的操作或监视器 ICS 的网络活动。

表 3-9 网络硬件方面的脆弱性

脆弱性	描述
网络设备物理防护不足	应该对网路设备的物理访问进行控制，以防止破坏网络设备。
不安全的物理接口	不安全的通用串行总线（USB）和 PS / 2 端口可以允许未经授权的拇指驱动器，键盘记录等外设的连接
物理环境控制缺失	环境控制的缺失可能会导致处理器过热。有些处理器会关闭，以保护自己，有的只是融化，如果他们的过热。
非关键人员对设备和网络连接的访问	应只限于必要的人员对网络设备的物理访问。不当访问网络设备可能会导致下列任何一项： ✧ 物理盗窃的数据和硬件 ✧ 数据和硬件的物理损坏或毁坏

	✧ 未经授权的更改（例如，改变 ACL 来允许攻击进入网络安全环境） ✧ 未经授权的截取和操纵的网络活动 ✧ 物理数据链路断线或未经授权的数据链接连接
关键网络设备没有冗余备份措施	关键网络设备没有冗余备份措施可能导致单点故障

表 3-10 网络边缘方面的脆弱性

脆弱性	描述
未定义网络边界	如果没有一个明确的安全边界的界定，那么要确保必要的安全控制措施的正确部署和配置是不可能的，这可能会导致未经授权的对系统和数据的访问。
未安装防火墙或防火墙策略配置不当	防火墙配置不当可能允许不必要的数据传输，这可能会导致几个问题，包括允许攻击数据包和恶意软件在网络之间传播，容易监测/其他网络上的敏感数据，造成未经授权的系统访问。
专网中存在非法流量	合法和非法流量有不同的要求，如确定性和可靠性，所以在单一网络上有两种类型的流量，使得更难以配置网络，使其符合控制流量的要求。例如，非法流量可能会无意中消耗网络带宽资源，造成业务系统的中断。
专网中没有运行专用网络协议	专网中运行一些 IT 服务，如域名服务（DNS），动态主机配置协议（DHCP），这些协议常应用在 IT 网络中。专网中运行这些服务会导致 ICS 网络对 IT 网络的依赖较大，而 IT 网络对系统的可靠性和可用性要求没有 ICS 专网要求高。

表 3-11 网络监控和日志方面的脆弱性

脆弱性	描述
防火墙和路由器日志未开启	如果没有合适、详细的日志信息，将不可能分析出什么原因导致安全事件的发生。
ICS 网络中没有安全监控设备	如果没有定期的安全监控，事故可能被忽视，导致额外的破坏和/或中断。需要定期的安全监测，以确定安全控制的问题，如配置错误和失效，

表 3-12 网络通信方面的脆弱性

脆弱性	**描述**
未识别关键监测点和控制路径	非法连接 ICS 网络可能会在 ICS 网络中留下攻击后门
采用了未加密的标准的、正是的网络通信协议	黑客可以使用协议分析仪或其他设备对网络协议进行分析，以监控 ICS 网络活动，一些协议如 Telnet，文件传输协议（FTP），网络文件系统（NFS）协议等容易被黑客进行解码分析。使用这样的协议更容易为对手进行攻击 ICS 和操纵 ICS 网络提供便利。
用户、数据与设备认证手段不足	许多 ICS 协议没有任何级别的身份验证措施。未经身份验证，黑客可能多次攻击并修改或伪造数据、设备，如伪造传感器和用户身份。
网络通信数据完整性校验不足	大多数工业控制协议中没有数据完整性校验，黑客可能操纵通信数据。为确保通信数据完整性，ICS 可以使用较低层协议（如 IPSec）提供数据完整性保护。

表 3-13 无线网络连接方面的脆弱性

脆弱性	描述
无线客户端和接入点的认证措施不足	无线客户端和接入点之间需要很强的相互认证，以确保客户端不连接到恶意接入点，也确保黑客无法连接到 ICS 网络。
无线客户端和接入点之间的数据传输保护措施不足	无线客户端和接入点之间的敏感数据，应使用很强的加密措施，以确保黑客无法获得未加密的数据进行未经授权的访问。

3.4 风险因素

目前有几个因素导致 ICS 控制系统风险的日益增加，这些在第 3.4.1 至 3.4.4 更详细讨论：

- 采用标准化的协议和技术，安全漏洞已知
- 连接到其他网络控制系统
- 不安全和非法的网络连接
- ICS 系统相关技术信息的广泛普及。

3.4.1 标准的协议和技术

ICS 的厂商已经开始开放其专有协议和发布他们的协议规范，使第三方厂商建立兼容的配件。组织也从专有系统迁移到更便宜的系统，如 Microsoft Windows 和 Unix - like 的操作系统以及常见的网络协议，如 TCP / IP 的标准化技术，以降低成本和提高性能。这种开放式系统的演变还由于另一种标准的 OPC 协议的使用，它使控制系统和基于 PC 的应用程序之间建立交互。使用这些开放的协议标准具有经济性和技术优势，但也增加了 ICS 的网络事件的脆弱性。这些标准化的协议和技术，很容易受到黑客挖掘漏洞并有效利用。

3.4.2 网络连接扩大

随着组织的信息系统管理模式的发展、业务及操作需求变化，ICS 系统和企业的 IT 系统常出现互联现象。远程访问的需求，促使许多组织建立连接到 ICS 系统，这样 ICS 维护工程师和技术支持人可以远程监视和操控 ICS 系统。许多组织也增加了企业网络和 ICS 网络之间的连接，让组织的决策者，以获得有关其业务系统的状态的关键数据，并发送产品生产指令或分发指令。在早期的实践中，这可能通过客户应用程序软件或通过 OPC 服务器/网关来实现，然而，在过去十年里，已通过传输控制协议/ Internet 协议（TCP / IP）网络和标准化 IP 的应用，如文件传输协议（FTP）或可扩展标记语言（XML）的数据交换来实现。通常情况下，这些连接是在没有相应的安全风险的充分认识情况下实施的。此外，企业的网络往往是战略合作伙伴网络和互联网连接。控制系统也使更多的广域网和互联网将数据传输到远程或本地站和单个设备。ICS 系统网络与企业网络的连接增加了访问控制上的脆弱性。除非适当的安全设备的部署，这些漏洞可能把 ICS 网络架构的各个方面暴露给黑客组织，并可能导致来自互联网的各种安全威胁，包括蠕虫病毒、恶意软件等。例如在控制系统威胁的变化情况，一位不愿透露姓名的能源组织的内部调查结果如下：

- 大多数经营单位的管理者，相信他们的控制系统没有连接到企业网络。
- 审计结果显示，大部分控制系统通过某些方式与企业网络连接。
- 企业网络只能保障一般业务处理系统的安全，而不能保障安全性要求极高的系统。

随着业务环境复杂性的增加，IT 系统的目标和过程控制系统的目标有根本性的区别， IT 系统通常将性能、保密性和数据完整性作为首要需求，而 ICS 系统则将人类和设备安全作为其首要责任，因此，系统的可用性和数据完整性的具有较高核心级。其他的区别，在 3.1 节的讨论，包括可靠性要求的差异，事件的影响，性能预期，操作系统，通信协议，以及系统架构。这可能意味着在安全建设实践存在显著差异。

3.4.3 不安全和恶意的连接

许多 ICS 供应商已经交付拨号调制解调器系统提供远程访问，以减轻技术支持人员进行远程维护的负担。有时远程访问提供了系统管理员级别的访问权限，如使用一个电话号码，或访问控制凭据（例如，有效身份标识，和/或密码）。黑客可能使用战争拨号器进行暴力破解，寻找破解密码的手段以获得远程访问系统。用于远程访问的密码往往设置比较简单，且用户可能长时间没有更改。这些类型的连接可能使系统变得非常脆弱，因为远程用户可以通过供应商安装的调制解调器以较高级别的身份访问 ICS 系统。

组织往往在不经意间留下的访问链接，如拨号调制解调器进行远程诊断，维护，和监测。此外，控制系统越来越多地利用无线通信系统，它可能是脆弱的。没有采取认证和/或加密保护的访问链接可能给远程访问控制系统增加安全风险。这会导致用户在数据的完整性以及系统的可用性之间做平衡和折中，这两者都可能对公众及 ICS 设施安全性产生影响。在部署加密之前，首先要确定加密是否是一种专用 IC 应用合适的解决方案。第 6.3.4.1 章节对 ICS 环境中使用加密提供了更多的信息。

企业网络和 ICS 之间互连需要许多不同的通信标准的集成，其结果往往是在两个独立的系统中设计了可以进行数据传输的基础设施通道。由于集成不同的系统的复杂性，控制工程师们往往很难承受因评估安全风险而增加的工作量。许多控制工程师几乎没有任何安全培训，ICS 组织中也常缺乏 IT 安全人员参与设计。因此，未保护企业网络免受未经授权的访问的安全访问控制措施经常是比较少的。此外，底层协议的机制可能不能很好地理解，从而漏洞可能存在，甚至可能会抵消安全措施的防护效果。如 TCP / IP 协议及其他协议没有进行分析，这可能导致在网络层或应用层的安全事件的发生。

3.4.4. 公开的信息

信息公开主要指 IC 设计，维护，通信等很容易在互联网上获得信息，如在产品选择上，开放标准的使用等。 ICS 的供应商也卖工具包，以帮助第三方开发软件，实现了在 ICS 环境中使用各种公开标准。也有许多前雇员，供应商，承

包商和其他最终用户使用过相同的 ICS 设备，他们了解 ICS 系统内部运作机制。例如，有人利用自己对 ICS 系统的深层了解制造了 Maroochy Shire 污水外溢事件，众多 ICS 网络安全事件之一， 该事件的其它信息在 3.7 节中油描述。

信息和资源提供给潜在的对手和来自世界各地的入侵者，有了这些信息，攻击者可能用很少的控制系统的知识，采用自动攻击和数据挖掘工具，使用出厂设置的默认密码，就可以获得未经授权的访问控制系统的控制权，这些默认密码是从来没有改变过的。

3.5 安全事件举例

对 ICS 系统有一些可能的安全事件的例子，比如：

- 通过延迟或阻塞通过企业或控制网络的信息流以控制系统的运转，从而对控制系统网络的可用性进行影响，或者通过对一些本地服务发起拒绝服务攻击以中断数据流，IT 本地服务（如 DNS）；
- 未经授权更变 PLC 的编程指令，远程终端装置（RTU），DCS 系统或 SCADA 控制器，报警阈值等，从而可能导致设备损坏（如果超出容错极限），未经授权的更改，过早关闭进程（如过早关闭传输线），造成环境的事件，甚至禁用控制设备。
- 虚假信息发送到控制系统的操作者，要么导致未经授权的更改，或操作者采取不合适的手段；
- 控制系统软件和配置信息被篡改，产生不可预知的结果；
- 安全系统运转受到干扰；
- 恶意软件（如病毒、蠕虫、木马等）传播到 ICS 系统；
- 关键信息（如生产产品的原料和指南）或工作指令被更改后对产品、设备或人员带来损害。

此外，ICS 控制系统覆盖了广泛的地理区域，该区域往往没有工作人员值守，没有监控手段。如果这种远程系统在物理上暴露，黑客可能建立一个连接返回到控制网络。

以下是两个有待证实的 ICS 安全事故的案例：

- 使用战争拨号器，简单的计算机程序连续拨号，寻找网络上的调制解调器，黑客发现连接在电力传动控制系统上的可编程断路器，破解密码，获得对断路器的访问控制，并更改控制器的设置从而导致当地停电和设备损坏。黑客降低了一些断路器的设置，从 500 安培（A）到 200A，停止这些线路的服务，并分流到邻近线的线路上。与此同时，黑客提高了临近的控制设备的设置到 900A，防止断路器跳闸，从而使线路超负荷运转。这将导致变压器等关键设备的重大损坏，造成在漫长的修复时间而中断。
- 一个服务大都市区的电厂已经和企业网络进行了隔离，并安装了最先进的防火墙，部署了入侵检测和保护措施。一名工程师轻易在当地一所大学继续教育研讨会网站下载文件并无意中引入了 ICS 控制网络中，就在早上业务高峰时间，操作员屏幕变为空白，系统关闭。

虽然这些情景是假设的，他们所代表的 ICS 潜在事故场景。 3.7 节提供了几个实际的 ICS 事件摘要。

3.6 安全事故来源

关于 ICS 控制系统安全事件的准确的统计数据很难统计。然而，在行业内大家都注意到这样一个现实，在传统的 IT 系统中漏洞增长的趋势和在工业控制系统中发现的漏洞增长趋势有一些相似之处。有一个安全组织（RISI）3，其目的是跟踪网络安全性质的事件，直接影响 ICS 和流程库。这包括，如意外的网络相关的事件，以及未经授权的远程访问，DoS 攻击和恶意软件渗透，如恶意事件。收集数据，通过研究为公众所知的事件，并从各成员组织未公开报告中收集数据，这些成员组织都希望能够远程访问数据库。每个安全事故案例都是根据可靠程度进行调查和评估过。

收集到得数据包括以下一些内容：

- 事件标题
- 事件日期

- 报告的可靠性
- 事件类型（例如，事故，病毒）
- 行业（如石油，汽车）
- 事件来源（如互联网，无线，调制解调器）
- 报告人
- 系统和硬件类型的影响
- 事件的简要说明
- 对组织的影响
- 采取措施，以防止复发
- 引用。

截至 2006 年 6 月，119 起事件案例已调查核实并记录在数据库中，15 起事件仍有待调查。其中，13 起事件标记为恶作剧或不太可能发生的事件，并从研究数据中删除。图 3-1 显示了 1982 年至 2006 年事件的趋势，这表明在 2001 年左右开始的事件急剧增加。现代 ICS 系统的复杂性留下了许多漏洞以及攻击向量。攻击可能来自许多地方，包括通过企业网络或间接直接通过互联网，虚拟专用网（VPN），无线网络，以及拨号调制解调器。

其他来源的事件信息显示 ICS 控制系统事件在增加。目前尚不清楚是否有更多的事件发生或只是更多的事件被发现和报告。

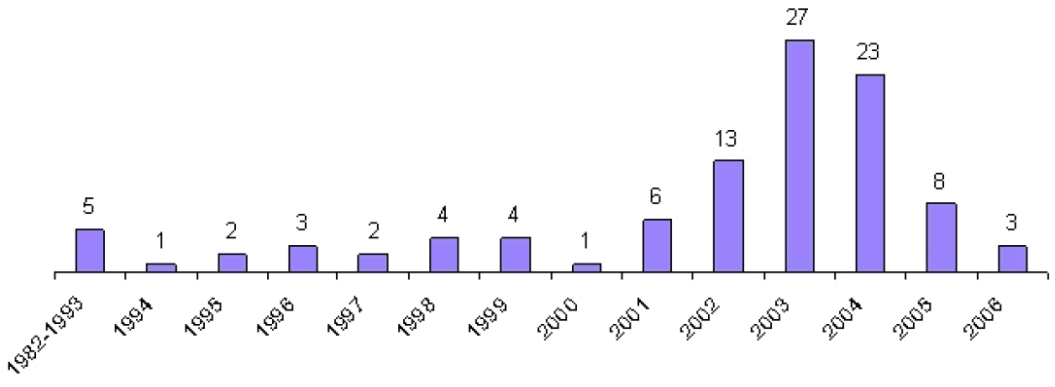


图 3-1 ICS 系统每年安全事件统计

ICS 系统安全事件主要有以下几类：

- 故意有针对性的攻击，如未经授权访问文件，执行拒绝服务，或欺骗的电子邮件（即伪造电子邮件发送者的身份）
- 非故意后果或设备损害，来自蠕虫，病毒或控制系统故障
- 无意的内部安全的后果，如不适当的测试业务系统或未经授权的系统配置的变化。

三类安全事件中，有针对性的攻击发生的频率最少。有目标的攻击可能是最具破坏性的，但还需要详细了解系统及基础配套设施。因此，最有可能的威胁类型是无意威胁和心怀不满的员工，前雇员，或组织工作的人。

3.7 收录的安全事件

正如在 3.6 节中提到的，有三大类的 ICS 事故，包括蓄意攻击，无意攻击或蠕虫，病毒或控制系统发生故障，无意的内部安全损害，如不适当的测试业务系统或未经授权的系统配置的变化，从这些类别的事件的报道包括以下内容：

3.7.1 内部有目标攻击事件

- 伍斯特空中交通通讯事故。 1997 年 3 月，一个马萨诸塞州伍斯特市少年，使用拨号调制解调器使公共电话交换系统部分发生瘫痪。这导致机场控制塔电话通信发生中断，影响机场安全，机场消防，气象服务，机场地面运输等。此外，该塔用于激活跑道灯的主要无线电发射机和另一个发射器被关闭，对监视飞行进展有很大影响。该攻击也使拉特兰附近的 600 个家庭和商业机构的电话通信系统发生中断。
- Maroochy 污水泄露事件。在 2000 年春天，一个开发制造业软件程序的澳大利亚组织的前雇员应聘当地政府的一个工作，但遭到了拒绝。被拒绝的心怀不满的雇员在超过了为期两个月的的时间内，据说多达 46 次使用无线电发射机，远程入侵污水处理系统的控制。他改变了电子数据，特别是污水处理泵站，造成系统操作故障，最终释放到附近的河流和公园约 264000 加仑未经处理的污水。
- Stuxnet 蠕虫。Stuxnet 蠕虫是针对 Microsoft Windows 的电脑系统的，

在 2010 年 7 月，其攻击目标专门针对工业控制软件和设备。该蠕虫最初肆意蔓延，但攻击目标为特定的 SCADA 系统，该系统对具体的工业生产过程进行控制和监视。

3.7.2 无意特定目标的攻击事件

- CSX 的列车信号失灵。 2003 年 8 月，Sobig 计算机病毒的传播导致感染该病毒的铁路信号灯关闭，该铁路横跨美国东海岸。该病毒感染佛罗里达州的总部计算机系统，并关闭铁路信号灯，干扰调度。据美铁发言人 Stessel 透露，有 10 个火车在上午受到影响。由于信号灯关闭，匹兹堡大学和佛罗伦萨、南卡罗来纳州之间的列车停止，并从弗吉尼亚州的一个区域的火车到华盛顿和纽约发生两个多小时的延迟。长途列车也被延迟 4 到 6 小时之间。
- 戴维斯 Besse8。 2003 年 8 月，核管理委员会证实，在 2003 年 1 月，已知的 Microsoft SQL Server 蠕虫在俄亥俄州橡树港感染了闲置的戴维斯 Besse，核电厂的私人电脑网络，导致安全监控系统停用近五年小时。此外，工厂的过程中电脑失败，前后历时约六小时后恢复。蠕虫还感染了至少 5 个其他公用设施的控制网络上的通信据，受到如此迅速地传播后造成通信流量堵塞。
- 东北电网瘫痪。 2003 年 8 月，在第一能源的 SCADA 系统由于有足够的态势感知电网的关键业务的变化的能力而拒绝控制室操作员的指令。此外，由于对拓扑结构变化的信息没有充分把握，缺乏业务连续性分析，西部地区的 ICS 系统发生业务连续性中断，俄亥俄州北部区域中的几个关键的 345 千伏输电线路与树木接触，这最终发生连锁反应导致 345 千伏和 138 千伏线路过载。共有 61800 兆瓦的电量发生损失。
- Zotob 蠕虫。 2005 年 8 月，一轮互联网蠕虫感染导致戴姆勒 - 克莱斯勒的美国汽车制造厂 13 台设备下线隔离将近一个小时，感染了微软 Windows 系统补丁的设备已经安装了补丁程序。在伊利诺伊，印第安纳，威斯康星，俄亥俄，特拉华州和密歇根州的大量设备被迫离线。虽然蠕虫病毒影响的主要是 Windows 2000 系统，它也影响到一些早期版本的 Windows XP。症状包括反复关闭计算机并重新启动。Zotob 蠕虫及其变种造成的重型设备制造商卡

特彼勒公司，飞机制造商波音公司，和美国几家大型新闻机构的电脑停止运行。

- Taum Sauk 蓄水坝事件。 2005 年 12 月，Taum 索克水蓄水坝遭受了灾难性的失败，释放一亿加仑的水。水库发生故障被填满水库的容量或可能已被溢出。目前掌握的失效原因是夜间蓄水池满后抽水泵没有停止工作，继续抽水，导致池水溢出。根据大坝 AmerenUE 仪表读取的监测数据与远程监控的监测仪表数据不同，该站是通过微波发射塔网络与大坝连在一起的，Taum 大坝现场没有人员值守。
- 贝灵汉华盛顿汽油管道失效。 1999 年 6 月，90 万升汽油（237,000 加仑）从 16“管道泄漏，点燃 1.5 小时，造成 3 人死亡，8 人受伤，大量财产损失。管道故障加剧了控制系统无法进行控制和监视功能。 “在事件发生前夕和在事件中，SCADA 系统表现不佳，抑制管道控制器对异常管道运行状态进行监测并及时响应。”NTSB 在 2002 年 10 月颁布的报告中提出了一个重点建议，推荐利用场外开发和测试系统对 SCADA 数据库的变化情况进行测试。

3.7.3 内部无明确攻击目标的事件

- 漏洞扫描事件。一旦对正在运转的 SCADA 网络（该网络控制 3 米（9 英尺）的机械臂）进行 ping 扫描，这只机械臂变得活跃并出现 180 度左右摇摆。 机械臂控制器在 ping 扫描开始前为待机模式下运转。在另一起事件中，ping 扫描正在执行对 ICS 网络上的网络和主机进行扫描，并造成了生产工厂中集成电路制造设备出现挂起。这个事件造成价值 50,000 元的晶元的损失。ICS 脆弱性评估的其他指导，请参阅第 4.2.6 节。
- 渗透测试事件。天然气公用事业聘请 IT 安全咨询机构，其企业 IT 网络进行渗透测试。咨询机构在渗透测试时不小心进入直接连接到 SCADA 系统的网络，结果导致 SCADA 系统和实用程序被锁住，四个小时内天然气管道无法输气，导致四个小时的服务中断。

4. ICS 系统安全程序开发与部署

正如在 3.1 节所述，ICS 和 IT 系统之间存在较大的差异，这将影响 ICS 系统采用何种安全控制措施。因此，组织应制定和部署 ICS 安全策略与程序，这些安全策略和 IT 安全策略与程序应当是一致的，但必须符合 ICS 的技术和环境的具体要求和特点。组织应定期审查和更新他们的 ICS 安全计划和方案，以适应新技术，业务，标准和法规的变化。

本节提供了 ICS 安全计划的开发和部署的概述。 4.1 节介绍了如何建立一个 ICS 安全计划的商业案例，包括业务方面的建议内容。 4.2 节讨论的一个全面的 ICS 安全计划发展，并提供部署方案的几个主要步骤信息。该文件的第 5 和 6 对可能涉及到的具体的安全控制措施进行了说明。

4.1 业务影响分析

ICS 在实施网络安全方案的第一步是制定一个有吸引力的、满足组织独特需求的商业案例。商业案例应该获取高层管理者对业务方面所关注的问题，这些是问题在其它很多类似风险处理中具有相同经验。业务价值分析提供了对业务的影响分析，和创建一个综合的网络安全方案的财务理由。它应包括有关以下内容的详细信息：

- 收益，包括改善控制系统的可靠性和可用性，创建一个集成的安全方案
- 如果一个网络安全方案在 ICS 系统中没有落实，带来的潜在的成本和损害的情况
- 在实施，运作，监控，审查，维护等环节有高层的指导与支持，以该进网络安全方案
- 制定，实施和维持安全程序所需的成本和资源

在提出商业管理案例之前，应该有审慎的、动态的安全实施和成本计划。例如，简单地要求一个防火墙是不够的，有很多原因可以说明。

4.1.1 收益

负责任的风险管理政策应测量和监测 ICS 系统所面临的安全威胁，以保障员工的利益，公众，股东，客户，供应商和社会的利益。风险分析可以权衡成本和收益，这样组织能作出保护措施明智的决定。此外，降低风险，行使尽职尽责的调查，也有利于组织：

- 提高控制系统可靠性和可用性
- 提高员工的士气，忠诚度和保留
- 减少社会各界的关注
- 增加投资者的信心
- 降低法律责任
- 提升企业的形象和声誉
- 帮助保险的覆盖范围和成本
- 改善投资者和银行的关系。

一个强大的安全和网络安全管理方案是一个可持续的商业模式的根本。

4.1.2 潜在影响

随着企业对互联互通依赖的增加，应进一步强调安全系统的重要性。DoS 攻击和恶意软件（如蠕虫，病毒等）已太常见了，已经影响 ICS 系统。此外，在一些关键的基础设施的计算机系统出现故障后可能有显著的物理影响。影响的主要类别如下：

- 物理影响。物理影响包括 ICS 失效的直接后果。最重要的潜在影响，包括人身伤害和生命损失。其他影响包括财产损失（包括数据）和潜在的对环境的破坏。
- 经济的影响。对经济的影响是从 ICS 事件引起的物理影响的连锁效应。物理影响，可能导致系统操作的影响，这反过来又造成设施或组织更大的经济损失。在规模较大，这些影响可能带来负面影响的地方，区域，国家，或可能是全球经济。
- 社会影响。另一个连锁效应，是国家或公共组织的信心丧失后带来的后

果，这可能被多次忽略。然而，这是一个很现实的目标，可通过 ICS 事件来反应。

下面列出了一个 ICS 事件的潜在后果。请注意，此列表中的项目都不是独立的的。事实上，一个后果的发生可以导致另一个后果的出现。例如，有害物质的释放可能会导致受伤或死亡。

- 恐怖主义行为对国家安全的影响
- 在一个网站或多个网站同时产生生产数据丢失
- 员工受伤或死亡
- 社会公众人受伤或死亡
- 设备损坏
- 有害物质的释放，转移，或盗窃
- 对环境的损害
- 违反监管要求
- 产品污染
- 刑事或民事法律责任
- 专有或机密信息的损失
- 品牌形象或客户信任的损失

任何形式的不良事件都会给一个组织的价值造成损失，但安全和安全事故，相比其他类型的事件而言，对所有利益相关者，员工，股东，客户，社区组织经营，都有较长期的负面影响。

4.1.3 业务影响分析的关键组成部分

业务影响分析有四个主要组成部分：较高优先级的威胁，较高优先级的业务后果，较高优先级的商业收益和可估算的每年对业务的影响。

4.1.3.1 较高优先级的威胁

在 3.2 节中提供的潜在威胁的清单需要细化到这些威胁，该组织认为可能实际影响安全设施。例如，食品和饮料的组织可能无法找到一个可信的恐怖主义威胁，但可能更关注的是病毒，蠕虫和心怀不满的员工。

4.1.3.2 较高优先级的业务影响

4.1.2 节中提供的业务的潜在后果的列表需要进一步提炼，以使高级管理人员会发现最引人注目的后果。例如，在相对较低的温度和压力，没有处理有毒或易燃材料，通常一个组织食品和饮料加工其产品可能不会对设备损坏或环境影响有关，但可能更多关注生产供应和退化损失产品的质量。合规性也可能引起人们的关注。个人不得减少可能产生的后果，以避免采取适当的安全风险缓解行动。

萨班斯 – 奥克斯利法案要求企业的领导人签署遵守信息的准确性和保护企业信息，大多数内部和外部审计事务所必须做尽职调查的示范，以满足股东和其他组织的利益相关者。通过实施全面的网络安全方案，管理行使尽职调查。

4.1.3.3 较高优先级的业务收益

改进的控制系统的安全性和控制系统特定的安全政策有可能提高控制系统可靠性和可用性。这也包括因不适当的测试、策略、系统的错误配置等对 ICS 系统造成的影响减至最低。

4.1.3.4 估算每年的业务影响

在业务影响列表中优先级最高的项目，应进行评估，以获得估计每年对业务的影响大小，最好但未必仅在财务方面。例如，对于食品和饮料的机构，该组织可能在其内部发生病毒事件，网络信息安全人员评估的结果就是一些具体的财务损失。如果内部网络和控制网络是相互关联的，可以想象的是，来自控制网络的病毒事件，可能导致对业务的相同影响。 NIST SP800-39[19]和 ISO / IEC 27002 提供额外的指导。

4.1.4 业务影响分析的资源

有助于形成商业案例的主要资源是在贸易和标准组织、咨询公司和从事风险管理和运营的内部资源。在贸易和标准组织的外部资源往往可以提供有用的提示，是什么因素最强烈地影响了他们的管理，并在其组织内部哪些是最有用的资源。针对不同的行业，这些因素可能会有所不同，但在其他风险管理专家可以扮演的角色方面可能有相似之处。附录 C 提供了一些在 ICS 安全当前活动的清单，并简短描述。

内部和风险管理工作相关的资源（例如，信息安全，健康，安全和环境风险，人身安全，业务连续性等），在组织中相关事件处理经验的技术上，提供了巨大的支持。这些资源是从优先的威胁和评估业务的影响的角度来看是有用的。这些资源也可以提供信息，管理人员集中处理哪些风险，因此，管理员可能是最合适的，或接受作为一个冠军。在控制系统的工程和运营内部资源可以提供控制系统是如何在组织内部署的细节，如以下的见解：

- 网络通常是如何隔离的
- 部署了哪些远程访问连接
- 如何设计高风险的控制系统或安全仪表系统
- 通常采用了什么样的安全措施

4.1.5 向领导介绍商业案例

企业的领导将负责审批和推动网络安全政策，分配安全角色，并实现跨组织的网络安全方案。整个计划的资金通常可以分阶段进行。虽然可能需要一定的资金，开始网络安全的建设，另外的资金待安全漏洞和建设需求进一步明确后再追加。此外，还应考虑 ICS 系统初期安全建设与后期升级换代的成本（包括直接和间接）。

通常情况下，获得管理层收购来解决这个问题的一个好方法是使一个成功的第三方实际的例子的商业案例落地。商业案例管理中，其他组织也面临同样的问题，然后提出他们发现了一个解决方案，以及是如何解决的。这往往会促使管理层自问，是什么解决的办法，以及如何适用于他们的组织的管理。

4.2 开发一套综合的安全程序文件

在 ICS 系统中有效地实施安全建设，需要定义和执行一个全面的计划，涉及安全的各个方面，从确定目标到日常的日常运作和持续审计合规性和改善。本节介绍了制定一个安全计划，其中包括以下的基本过程：

- 获得高级管理人员支持
- 建立和培养一个跨职能的团队

- 定义纲领和范围
- 定义特定的 ICS 的政策和程序
- 定义和 ICS 的资产
- 进行风险和脆弱性评估
- 定义缓解控制措施
- 提供培训和提高 ICS 的工作人员的安全意识

在 ANSI/ISA-99.02.01 工业自动化和控制系统的安全提供了更多的各个步骤的详细信息：建立一个工业自动化控制系统安全计划。

组织安全计划的实施，是从高层开始的。网络安全高级管理人员必须表现出明确的承诺。网络安全是一个组织的责任，尤其是领导成员在业务、流程和管理方面负有的责任。从组织高层那里获得的充足的资金和指导，会使组织在实施安全方案时更容易实现合规性，运转更顺畅，比没有获得支持的方案有更多成功的可能。

每当一个新的系统设计和安装，在整个生命周期过程中都需要考虑安全性，从架构到采购，安装到维护退役。那种认为产品上线后是安全的假设有很多严重的风险。如果在系统部署前没有足够的时间和资源，那么在以后解决安全问题可能会耗费很多时间。

4.2.1 高层管理者的支持

高级管理人员引进和参与 ICS 安全计划是 ICS 安全计划成功的关键。高级管理人员需要在一定的水平上，包括 IT 和 ICS 操作。

4.2.2 建立和训练一支跨职能的团队

这是一个跨部门的网络安全团队，分享他们的不同领域的知识和经验，以减轻 ICS 的风险。网络安全团队至少应该包括组织的 IT 人员，控制工程师，控制系统的操作，安全课题专家和管理人员。安全知识和技能应包括网络架构和设计、安全的程序和操作、安全基础设施的设计和运作。网络安全团队的连续性和完整性，也应包括控制系统供应商和/或系统集成商。网络安全小组应直接向现场管理（例如，设备管理员）或公司的 CIO/ CSO 汇报，接受完整的 ICS 网络安全的

责任和问责。管理一级的问责制将有助于确保网络安全工作的持续开展。

控制工程师在保护 ICS 系统安全中将起到很大的作用，如果他们没有 IT 部门和管理者的合作与支持，工作将很难开展。IT 已具有多年的安全实践，其中大部分是可应用在 ICS 中。控制工程和 IT 的文化往往具有显著的不同，对双方来说都是未知的，跨文化的理解和整合将在安全设计和操作中至关重要的。

4.2.3 定义纲领和范围

网络安全小组应建立企业的安全策略，该安全策略定义了安全组织的角色，责任，系统的所有者和使用者做负有的责任。该小组应建立安全计划的目标，业务影响分析，业务支撑的所有电脑系统和网络，所需的预算和资源，职责分工等。范围的定义包括业务、培训、审计、法律和法规的要求，以及时间表和责任。

对组织的 IT 业务系统可能已经有一个操作程序或需要开发。该小组应确定哪些现有的做法对 ICS 系统有影响，哪些活动是具体的的做法。从长远来看，如果团队能与组织中的其他人有类似的目标共享资源，这将对安全活动产生积极的影响。

4.2.4 定义 ICS 详细的安全策略和程序

策略和程序是每一个成功的安全体系的根本，ICS 的特定的安全策略和程序应与现有的运作/管理策略集成。这些政策越浅显易懂，他们就越有可能在各级实施。策略和程序应确保安全保护措施和是当前现状一致，以抵御不断变化的威胁，也有利于教育。在清楚地了解了各个系统的风险后，网络安全小组应审查现有的安全政策，看他们是否足以应对当前 ICS 安全风险。如果需要，现有的策略应修改或创建新的策略，以解决桌面和业务系统的安全问题。很少组织有足够的资源来强化 ICS 系统所有可能面临的威胁；管理层要引导安全策略的变更，根据风险评估，将设置安全的优先级和目标，使组织的威胁所造成的风险减至最低。需要制定支持策略的程序文件，使策略在 ICS 中的实施更充分和适当。安全程序文件应当形成文档、并经过测试，并根据策略和技术的变化定期更新。ICS 的安全策略和程序制定中应考虑国土安全咨询机构安全威胁级别定义，随着安全威胁

的增加部署相应的安全设备抵御日益增长的安全姿势。

4.2.5 定义 ICS 系统和网络资产清单目录

网络安全小组应确定内部和连接到 ICS 内的计算机系统、网络及应用。应该把重点放在系统上，而不是仅仅设备上，并应包括的 PLC，DCS，SCADA 系统，作为人机界面等，使用监控设备和仪器系统。使用路由协议或拨号访问的资产应当记录在案。作 ICS 的资产标识，信息应记录在一个标准的格式。该小组应审查和更新每年 ICS 资产清单。

有几个商业企业目录的工具，它可以识别在网络上的所有硬件和软件资产。在识别 ICS 的资产之前必须小心使用这些工具；项目组应先进行一个评估，如何使用这些工具，对工作产生怎样的影响。工具评估可能包括类似，非生产环境的环境测试，以确保该工具不会对生产系统产生不利影响。虽然这种影响可能在 IT 系统中可以接受，但在 ICS 系统中却不可以。在第 4.2.6 节提供扫描和库存工具的其他信息和指导。

4.2.6 进行漏洞与风险评估

因为每个组织的资源是有限的，组织应进行 ICS 系统的风险评估，根据对业务系统的潜在影响，利用其评估结果把 ICS 系统的优先级区别出来。然后对该组织中最高优先级的系统进行脆弱性评估，低优先级的系统可以看成是可以接受的风险。脆弱性评估将有助于确定可能会对 ICS 的保密性，完整性和可用性有影响的安全漏洞，以及与相关的网络安全风险和缓解方法，以减少系统的风险。

由于存在设备中断的可能性，漏洞扫描器应在 ICS 生产网络中谨慎使用。一个主要原因是可能会对 ICS 产生偶然的 DoS 攻击。漏洞扫描器通常通过广泛的探测尝试验证，模型攻击行为对系统和网络设备进行扫描。 ICS 的设计和建造到现实世界的过程或设备的自动化控制，如果由于错误指令，他们可以执行错误的操作，将造成产品损失，设备损坏，人员伤害甚至死亡。

下面的例子展示了危害：

- 当在一个活跃的 SCADA 网络上进行 ping 扫描时，被 ICS 控制的 9 英尺长

的机械臂的变得活跃并进行 180 度左右摇摆。在 ping 扫描开始前 ARM 控制器在待机模式。

- 在 ICS 网络执行一个 ping 扫描，以确定在线的主机，结果造成了系统的控制锁定，导致晶元价值 50,000 元的破坏。
- 天然气公用事业聘请 IT 安全咨询机构，对其企业 IT 网络进行渗透测试。咨询机构不小心进入 ICS 网络，这是直接连接到 SCADA 系统的一部分。渗透测试锁定了 SCADA 系统和实用程序，导致天然气管道无法传输燃气，造成中断四个小时。

在 ICS 内部查找一个安全漏洞，需要一个同典型的 IT 系统不同的方法。在大多数情况下，在 IT 系统上的设备可以重新启动，恢复，或短时中断对客户提供的服务，而对 ICS 控制一个物理过程，因同现实世界直接相关，一些操作对时间的要求极高，而另一些则可以在较为宽松的时间内完成。

进行漏洞扫描系统或网段时，也有一般执行的几个步骤。每个步骤都列在表 4-1，除了通常的 IT 措施外，在 ICS 系统中可采取的一些建议操作，以使任何测试的结果更安全。这些技术可能使工作较为困难，但应有助于减轻与主动扫描相关的问题。

表 4-1 ICS 漏洞评估建议的操作

扫描对象	常用的 IT 手段	建议的 ICS 手段
主机、节点和网络	PING 扫描（如 NMAP 扫描）	● 检查路由器配置文件或路由表 ● 进行物理校验（物理线路等） ● 部署网络入侵检测措施（如 SORT） ● 定义 IP 子网，防止自动化程序扫描
开启的服务	端口扫描（如 NMAP）	● 做本地端口检查（如 NETSTAT） ● 扫描备用机，或非生产系统或测试用机
服务漏洞	漏洞扫描（如 NESSUS）	● 版本标识检查；

		● 扫描备用机，或非生产系统或测试用机

以上所建议的 ICS 手段的共性是，他们不会对生产经营网络产生大流量，或对生产系统产生抵触。这些侵扰程度较低的方法，如果不是全部都可以收集，更积极的方法无需在测试过程中造成失败的风险。另一个要考虑的因素时，选择 ICS 的测试方法同 IT 系统相比，ICS 系统容量比较小。 ICS 系统已远远大于他们的 IT 同行的寿命，因此，他们的硬件往往是远远落后于技术发展水平，并可以很容易地超负荷。此外，ICS 系统通常是在传统的网络上需要低延时运行速度缓慢，可能在主动测试过程中被产生的流量所淹没。

当任何一个 ICS 系统进行评估操作时，ICS 的人员必须意识到测试已经发生，并准备立即解决出现的任何问题。如果手动控制系统是可行的，在安全测试中能够执行手动控制的人员应在场。此外，安全审计师需要了解被测 ICS 系统，测试所涉及的风险，并跟踪 DOS 攻击对 ICS 系统的无意影响。

4.2.7 定义风险缓解控制措施

组织应分析详细的风险评估，确定每个风险缓解的成本，比较成本与风险的发生，并选择那些缓解控制成本小于潜在风险的解决措施。因为它通常是不切实际或不可能消除所有风险，组织应着眼于降低对 ICS 系统影响最大的风险因素。

特定风险的控制，不同类型的系统有不同的控制措施。例如，IC 系统中用户身份验证控制可能比企业工资管理系统和电子商务系统不同。组织应在使用以上措施时进行记录和沟通。组织一旦制定了风险控制措施，可能会采用“速战速决”的解决方案来解决发现的风险，低成本，高价值的做法，可以显着降低风险。这些解决方案的例子是互联网接入访问控制和垃圾邮件防护。组织应识别，评估，并实施适当的快速修复解决方案，为尽快降低安全风险，实现快速收益。能源部（DOE） 《改善 SCADA 网络安全的 21 个步骤》的文件，可以作为一个具体行动纲要来采用，以提高 SCADA 和其它 ICS 系统的安全。

4.2.8 提供培训机会，加强安全意识

安全意识是 ICS 事件预防的重要组成部分，尤其是当它涉及到社会工程威胁。社会工程是用来操纵个人以泄露私人信息，如密码等。这些信息可能影响系统的安全。

实施 ICS 安全计划可能对员工使用计算机软件、应用程序以及电脑桌面的方式带来一些变化。组织应设计有效的培训和宣传方案，帮助员工了解新的访问和控制方法是必需的，他们可以使用，以降低风险和对组织的影响。培训方案也表明管理层的承诺和网络安全方案的价值。从接触到这种类型的培训人员的反馈来看，安全培训是安全计划中非常宝贵的资源。

5. 网络结构

为工业控制系统安全(ICS)部署设计网络架构时，我们常常建议将 ICS 网络和办公网络分开，事实上这两种网络的性质并不一样：因特网接入，FTP，e-mail，远程接入在典型的办公网中是允许的，而 ICS 网络中则不行。在办公网中，对网络设备、安装以及软件变化的精密控制不大可行。如果在让 ICS 网络运作与办公网上层，那么它往往能承受一次 DoS 攻击。如果将两种网络分开，那些在办公网中发生的安全问题则不会影响 ICS 网络。

实际上，ICS 网络和办公网的连接是必须的，而这种连接又是一个重大安全风险，设计与实现这一连接时必须谨慎考虑。如果两种网络必须相连，我们强烈建议通过防火墙和 DMZ，使连接尽可能最小化，最简化。所谓 DMZ 是指一个与防火墙直连的独立网段，包括 ICS 数据接入办公网这样的服务都需要通过这个独立网段。只有这些系统被允许接入办公网。由于几乎没有额外的连接，只有极少的一些接入需要通过防火墙，比如为特定连接打开某些端口。接下来的部分将描述接入必须经过的节点。

5.1.防火墙

防火墙是种能够确保网络服务安全的设备或系统。现在，我们常常在网络联通和 TCP/IP 协议相关问题中讨论防火墙和防火墙环境的应用。尽管如此，防火墙在网络环境中的适用性并不包括网络连通性。例如，很多办公网使用防火墙限制一些敏感部门(财务、人力)的因特网服务。使用防火墙控制相关部门的网络连通性，可以有效的预防未经授权的非法接入以及保护敏感数据。防火墙主要分了下面几类：

包过滤防火墙：最基础的防火墙。包过滤防火墙本质上就是具有访问控制功能的路由器。这种访问控制是由一整套指令集决定的。包过滤防火墙一般作用于开放式系统互联模型(OSI)的网络层，它针对数据包发出之前一套标准，检查每个数据包的基本信息，如 ip 地址。根据这些数据包和标准，墙可以丢弃数据包，甚至将信息发回源头。由于只检查了数据报文头中很小的一部分，包过滤防火墙对网络性能低消耗，低影响的优势得以体现。

状态检测防火墙：状态检测防火墙在包过滤防火墙的基础上加入了对 OSI 传输层的感知。这种防火墙在网络层过滤数据包，判定哪些合法，并在传输层评估其内容。状态检测防火墙保留了有效会话的路径并用于决定数据包是否丢弃。它提供了较高的安全性和性能，但对于管理者而言却更为昂贵和复杂。应用于 ICS 则需要制定额外的规则。

应用网关型防火墙：这类防火墙在应用层对数据包进行检查，并且传输遵循特定规则，比如浏览器，FTP 传输。他提供了很高的安全性，但较大影响了网络开销和延迟，这在 ICS 环境中是不可容忍的。

NIST SP 800-41，Guideline on Firewalls and Firewall Policy，提供了防火墙及其策略的选择指导。

在 ICS 环境中，防火墙往往部署与 ICS 网络和办公网络之间。正确的配置可以极大的限制未经授权的访问，从而提高安全性。通过去掉不必要的网络可以潜在地改善控制网络的响应。正确的设计、配置、使用防火墙，可以显著地提高 ICS 环境的安全性。

防火墙提供了一些加强安全策略的工具，当前市场上一系列进程控制设备并不具备这一功能：

除了某些特定的通信，未受保护的 LAN 与受保护的 ICS 中设备间的通信都被阻止。这种阻止基于源、目的 ip 匹配，服务和端口，同时发生于数据包出入阶段，从而减少了通信的高风险，比如 e-mail。

所有接入 ICS 的用户都被强制安全用户认证。认证方法较为灵活，具有多种级别的保护：简单密码，复杂密码，多因素认证技术，令牌，生物测定，智能卡。具体选择何种方式，取决于 ICS 需要保护的缺陷，而不是设备的级别。

流量监控，分析和入侵检测的记录。

实施可用的策略以适应 ICS 网络而不是 IT 网络，如禁止不安全的通信，包括使用电子邮件和容易记住的用户名和组密码。

由于设计为有记录的、连接尽可能简单的网络，在遇到一些网络上的故障时，ICS 网络得以从办公网中分离出来。

还有一些其他可能的部署，包括在独立控制设备上使用基于主机的防火墙或者小型独立硬件防火墙。在改变防火墙配置管理时，这样尤其会带来严重的管理开销。

在 ICS 环境中部署防火墙，有一些特别需要注意的地方：

控制系统通信可能带来的延迟。

设计符合工业应用规则时经验的匮乏。过去，防火墙仅仅保护已经配置好的控制系统，默认的规则是禁止出入。只有在需要时，与被信任的系统进行连接，配置才可以修改。

硬件防火墙需要持续的支持，维护和备份。规则的设置需要审查以确保应对不断变化的安全威胁。系统性能(如防火墙日志存储空间)必须被监控，确保防火墙始终进行数据采集，并以此对抗安全侵犯。为了尽快发现并着手解决网络故障，防火墙实时监控和一些其他安全传感器是必须的。

5.2 逻辑分割控制网络

通过物理设备分置，ICS 网络与办公网在逻辑上得以分割。企业联通性有几点要注意：

ICS 网络与办公网之间的接入点要尽可能简单并有文档记录，冗余的接入点则必须记录。

状态检测防火墙被配置为，除了那些明确授权的通信，ICS 和办公网之间其他通信都将被拒绝。

除了 TCP 和 UDP 端口过滤，ICMP 类型过滤，防火墙的规则还至少需要提供对源和目的的过滤(MAC 地址的过滤)。

一个比较可行的方案是在 ICS 网络和办公网之间实施一个 DMZ 网络。将 DMZ 与防火墙相连，可以有效地限制办公网与 DMZ 之间、DMZ 与 ICS 之间的通信。办公网与 ICS 网络不允许直接连接。5.3.4 和 5.3.5 节将进一步描述这一内容。在 ICS 和外部网络实施虚拟专用网络(VPN)可以提高安全性，5.8.2 和 6.3.4.2 节给出了 VPN 使用的更多信息。

5.3.网络隔离

ICS 和办公网能够以不同的架构分割来加强网络安全，这一节描述几种架构的优缺点。5.3 节中的图表旨在表明防火墙在分割网络中位置，但不是所有的设备都必须使用。5.4 节给出了深度防御架构的指导意见。

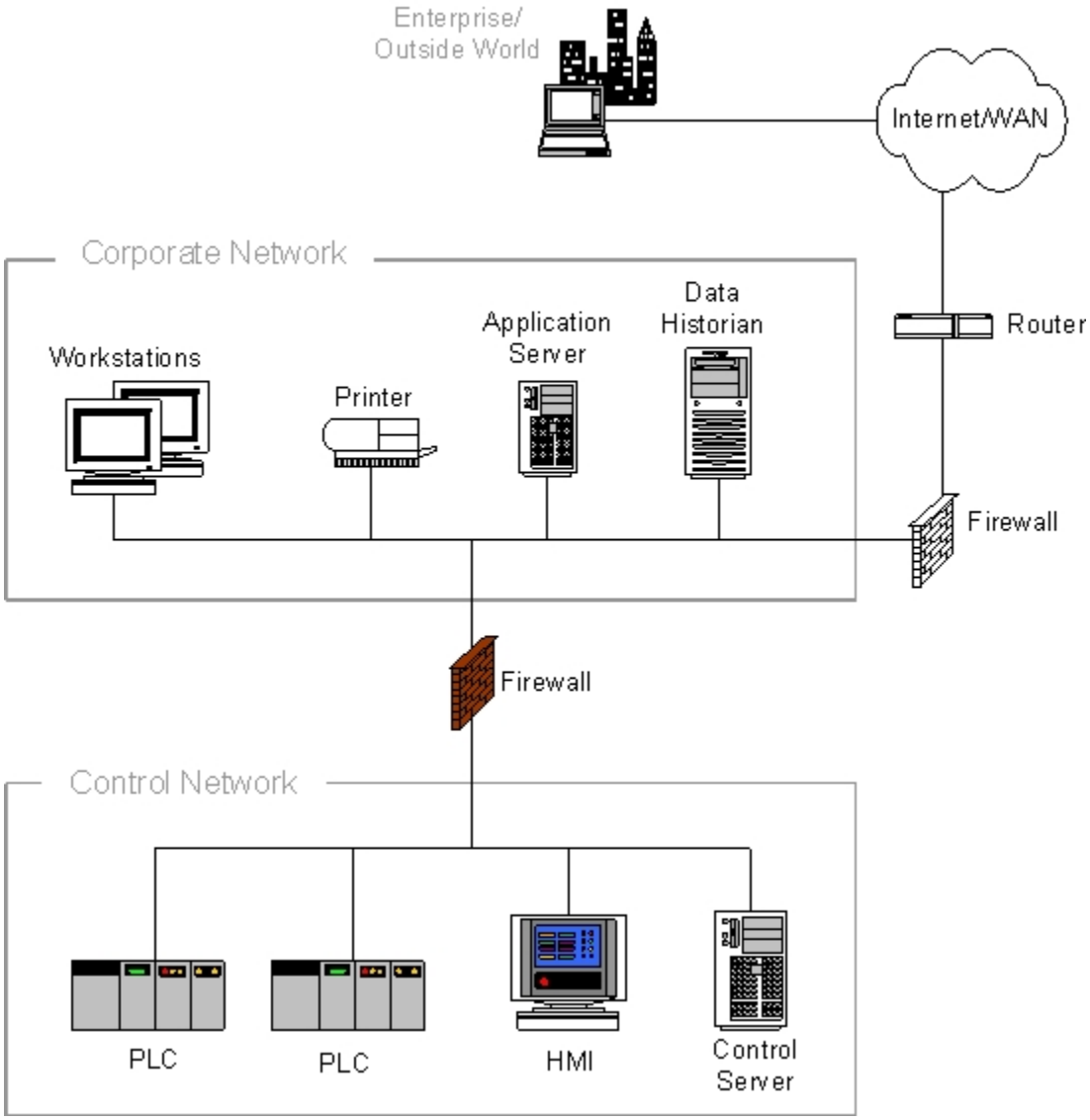
5.3.1 双宿主机/两个网络接口卡

双宿主机可以在两个网络之间传输。没有适当安全控制的一台电脑将会造成额外的威胁。为了预防这一情况，控制网络和办公网之间的防火墙必须配置为双宿模式，两种网络之间的任何通信都必须通过防火墙。

5.3.2 办公网和控制网络之间的防火墙

图 5-1 中，一个两端口防火墙在办公网和控制网络中的应用，显著地提高了安全新能。正确地配置，可以明显地降低外部攻击的成功率。

但这种设计中存在两个问题：首先，由于海量数据记录系统被设计在办公网部分，防火墙需要授权这部分数据与控制网络中的控制设备通信。来自办公网络中，一个恶意的或者不正确配置主机发送的数据包(通常表现为海量数据记录系统)，将会被转发到个别的可编程逻辑控制器(PLCs)或者分布式控制系统(DCS)。



5-1 办公网与控制网络间配置防火墙

如果海量数据记录系统被存放于控制网络部分，防火墙又必须设置一条规则，允许所有企业主机与这部分数据通信。典型的，这种通信发生在应用层，包括结构化查询语言(SQL)或者超文本传输协议(HTTP)请求，而这种应用层方面的缺陷则会对海量数据记录系统造成危害，一旦这种危害产生，控制网络中的其他节点也成为了蠕虫病毒和交叉攻击的突破口。

另一个问题在于，影响控制网络的伪造数据包被构造，可能令一些不公开的数据得以在允许的协议上传输。比如，防火墙允许 HTTP 数据包通过，特洛伊木马软件可以通过人机界面或控制网络中的笔记本远程控制，并传输数据(如捕获的密码)，伪装成合法传输。

总之，如果想要这种架构显著提高未分割网络安全性，防火墙的规则必须允

许办公网和控制网络的设备间直接通信。如果不能仔细设计并监控，将会导致安全漏洞。

5.3.3 办公网和控制网络之间的防火墙和路由器

图 5-2 提出了一个略好的设计，使用了路由器和防火墙结合的方式。路由器配置在防火墙之前，提供一些基本的包过滤服务，防火墙则利用状态检测或代理技术负责更加复杂的事物。这种设计广泛应用于面向因特网的防火墙，因为它令更快速的路由器处理了大量传入的数据包，尤其是 DoS 攻击，并降低了防火墙的负载。同时提供了更好的深度检测，对于两台不同的设备，对手必须绕道。

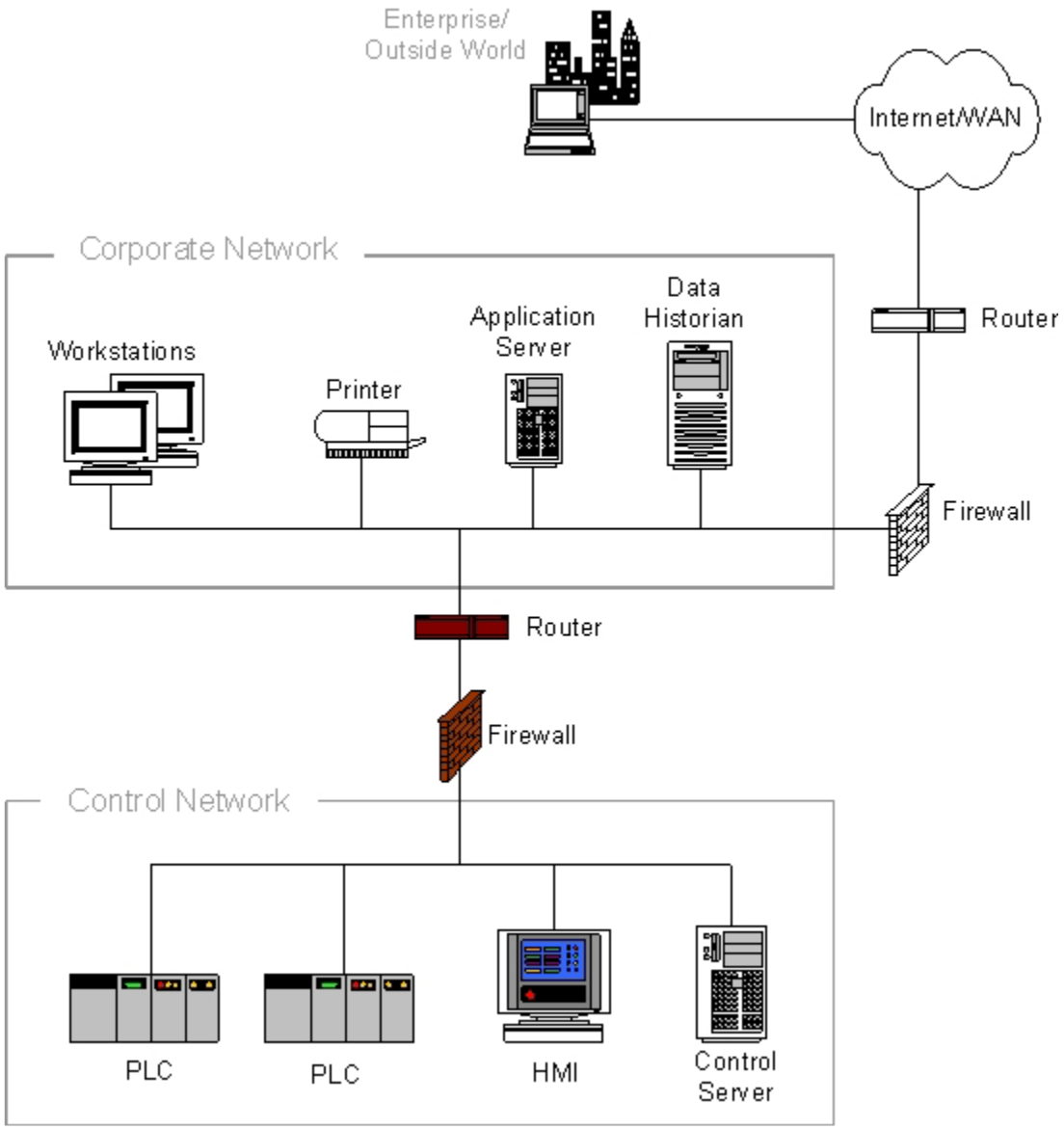


图 5-2　办公网和控制网络之间的防火墙和路由器

5.3.4 办公网和控制网络之间带 DMZ(隔离区)的防火墙

在办公网和控制网络之间建立隔离区的防火墙是一个显著地提高。每个隔离区隔离出一个或多个重要组成部分，比如海量数据记录系统，无线网络接入点或者远程、第三方接入系统。实际上，能够制造隔离区的防火墙如同构建了一个中间网络。

为了构建隔离区，除了传统的公共和私有接口外，防火墙至少需要提供 3 个接口。一个接口连接办公网，一个接口连接控制网，剩余的接口则连接 DMZ 中那些共享的不安全的设备，比如海量数据记录系统服务器，无线网络接入点，5-3 是这种架构的示意图。

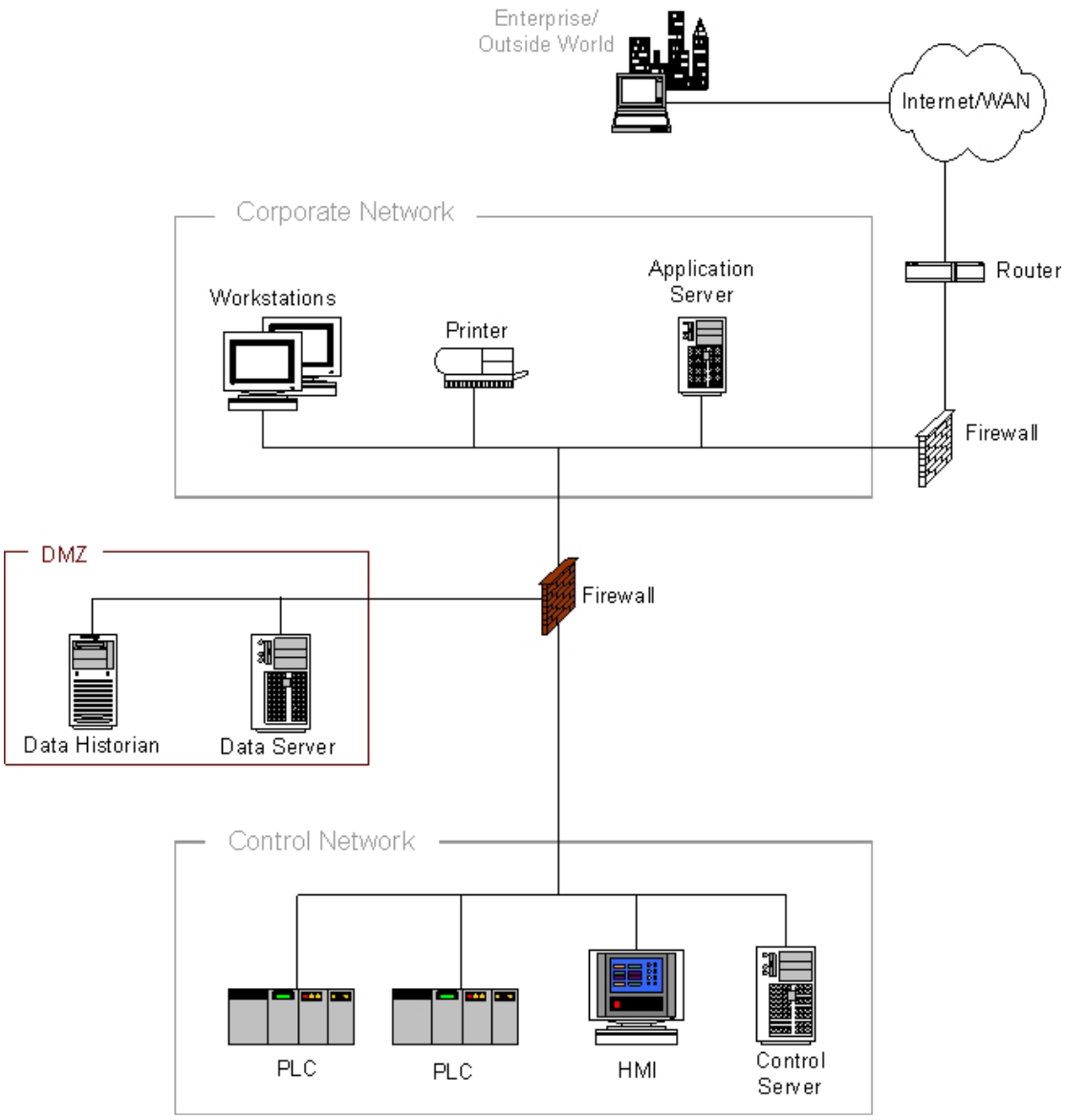


图 5-3　办公网和控制网络之间带 DMZ(隔离区)的防火墙

由于把那些可存取部分分布在隔离区，办公网和控制网之间不再直接通信，转而都以隔离区为通信目标。大多数防火墙允许存在多个隔离区，并规定隔离区之间通信的规则。如图 5-3 所示，无论是办公网输出还是控制网输入数据包都可以被防火墙丢弃，另外防火墙还能够协调包括控制网络在内的链路。规则良好地制定，控制网络与其他网络间明确细分的实施，确保了办公网和控制网络间几乎没用直接的通信。

如果一个补丁管理服务器或者防病毒服务器甚至其他安全服务器被用于控制网络，他们应该被置于 DMZ 中。有补丁管理和防病毒管理功能的控制网络，对应 ICS 环境的特定需求可以调整控制和安全更新。ICS 选择的防病毒产品与办公网选择的不一致时同样有效。比如，发生了一起恶意软件事故，而防病毒产品没

有检测到这一事件并及时阻止，看上去其他产品也许能完成这一任务。

这一架构中最主要的风险在于，如果 DMZ 中的一台主机被攻陷，它将被用于制造控制网络和 DMZ 中的攻击。通过强化并及时更新 DMZ 中的服务器，规定防火墙只接受有控制网络设备发起的与 DMZ 的通信，这种风险可以大大降低。这一架构的另一问题是额外的复杂性以及端口个数带来日益增加的防火墙消耗。对于那些更为关键的系统，优势显然大于劣势。

5.3.5 办公网和控制网络之间成对的防火墙

如图 5-4 所示，带 DMZ 的防火墙解决方案中的一个变化是在办公网和控制网络之间使用成对的防火墙。像海量数据记录系统这样的公共服务器被布置于防火墙之间，被称之为制造执行系统(MES)层。如同之前描述的，一台墙负责丢弃进入控制结构和公共数据数据包，另一台则可以防止错误的服务器连接控制网络和共享服务器对控制网络的冲击。

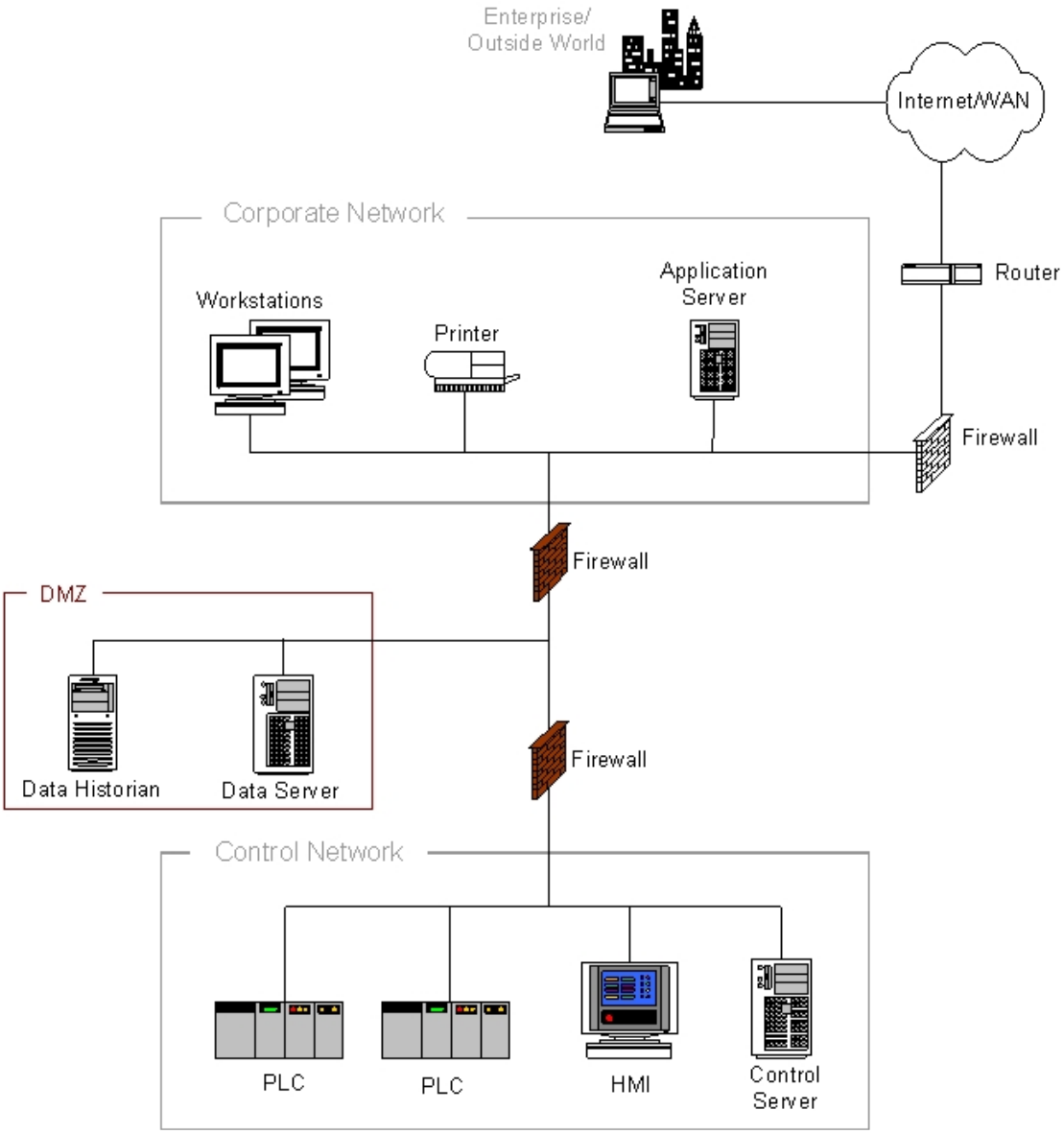


图 5-4　办公网和控制网络之间成对的防火墙

如果使用了不同厂商的防火墙，这一方案还有一个优势。由于工业组和信息技术组都可以独自管理防火墙，它们都可以拥有明确分开的设备。这一架构的主要缺点在于更多的消耗和管理的负责。对于那些对安全有严格要求或需要明确管理分离的环境，这种架构具备较强的优势

5.3.6 网络隔离总述

总之，不基于防火墙的解决方案，并不适用于办公网和控制网的隔离。两块区域的解决方案基本符合要求，单需要严格的维护。最为安全、可行的网络隔离方案则是配置至少三块区域，其中至少有一块 DMZ 区。

5.4.深度防御架构

单一的安全产品、技术或者解决方案并不能很好的处理 ICS 保护问题。多层级策略宝库两个(或更多)重叠的安全机制能够最小化单一设机制造成的不良影响，深度防御正是这种技术。深度防御架构策略包括使用防火墙，创建隔离区，带有效安全策略的入侵检测，培训计划和事件响应机制。此外，还需要对 ICS 可能面临的攻击方式有所了解：

- 网络周边的后门和漏洞
- 公共协议的缺陷
- 对现场设备的攻击
- 数据库攻击
- 通信劫持和中间人为攻击

图 5-5 是 ICS 对深度防御架构的一个应用示意图，来源于国土安全部的控制系统安全计划实践建议委员会网站上记录的文档 Control Systems Cyber Security: Defense in Depth Strategies 中。包括特定问题及相关解决措施的文档支持，也可以在上述网站中找到。该网站将继续发展，并将最新建议和相关信息及时更新。

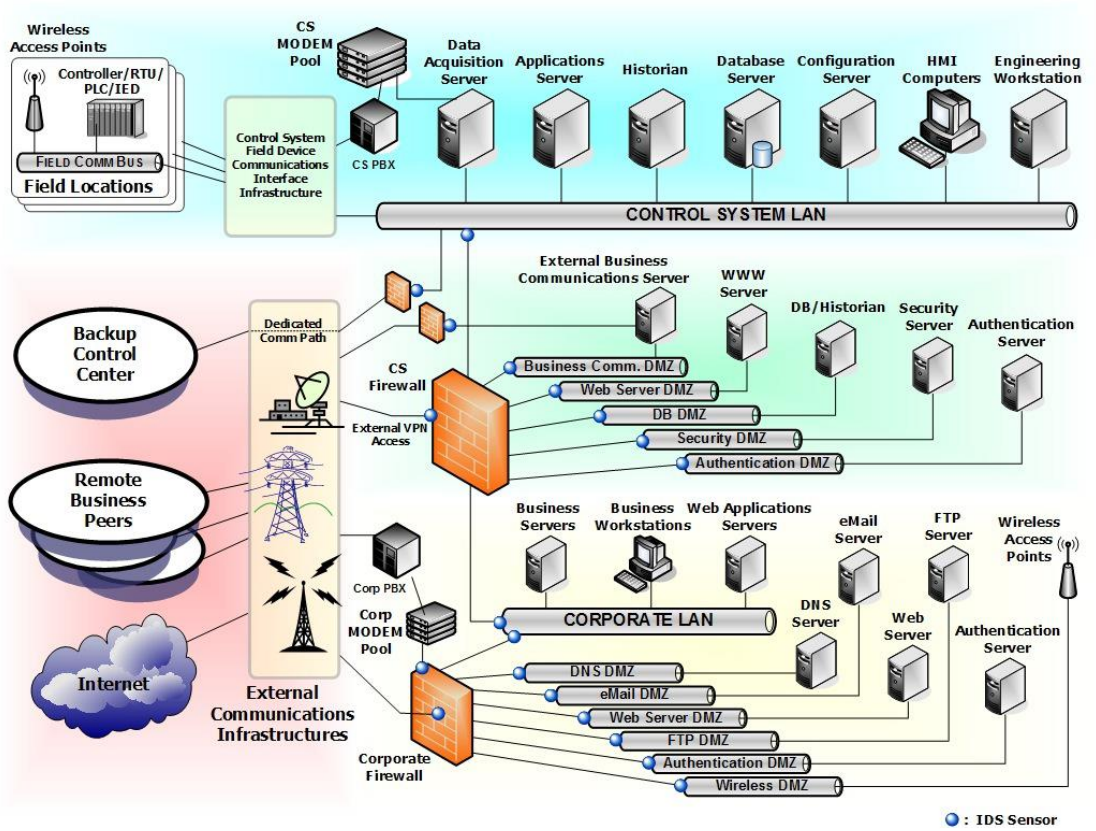


图 5-5　CSSP 建议的深度防御架构

上面提到的文档，为深度防御架构策略发展提供了指导和方向，架构策略应用于使用了控制系统网络的组织，网络需要维护多层信息架构：

- 各种现场设备的维护，遥控采集，工业级处理系统
- 通过远程数据链路或调制解调器接入设备
- 面向公共的服务或公司业务

这种架构包括了防火墙，采用隔离区以及 ICS 架构中的入侵检测能力。图 5-5 中的隔离区提供额外功能隔离和访问权限的能力，并已被证实对于那些由不同任务组成的大型网络架构是有效的。

5.5. ICS 普遍的防火墙策略

随着深度防御架构的布置，防火墙也必须制定相应规则决定通行的权限。每个组织配置防火墙最基本的前提是只允许那些必须的通信，虽然现实情况更麻烦。究竟哪些是“必须的”，允许了这些通信又对安全性有什么影响？比如，很多企业允许海量数据记录系统服务器的 SQL，但不幸的是 SQL 同时也是蠕虫病毒的温

床。工业中我们用到了很多重要的协议，如 HTTP、FTP、OPC/DCOM、EtherNet/IP、MODBUS/TCP 等，他们都有重要的安全隐患。

这节中接下来的部分将描述来自 CPNI 的一篇文档 Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks 中的一些要点。、

在公共服务器配置一台两个端口的防火墙而不设置隔离区，规则的制定则显得尤其重要。至少所有规则中都应包含 IP 地址和端口号。地址部分的规则应当阻止来自办公网地址的主机与控制网络中的一部分公共服务器(比如海量数据记录系统)的通信，任何企图进入控制网络的属于办公网的 IP 地址都是不允许的。此外，端口部分的规则要关注协议的安全性。由于潜在的网路侦听和修改，允许 HTTP、FTP 或者其他不安全的协议穿越防火墙是一种安全风险。制定规则时，控制网路外的主机对网内的主动连接应当被拒绝，只允许网内主机主动发起的连接。

另一方面，如果使用了带隔离区的架构，办公网络与控制网络中可以配置为不存在直接的连接。除了一些特殊情况，任何一方的终点都将是隔离区中的服务器。这就使得允许通过防火墙的协议更加灵活。例如，从 PLC 连接海量数据记录系统使用了 MODBUS/TCP 协议，而 HTTP 协议则用于海量数据记录系统与办公网客户端的连接。每种协议都并不是那么安全，但在这个案例中，他们都可以安全的使用，因为他们并没有被用于直连两部分网络。这一概念的一个扩展在于控制网络与办公网络通信中，使用“组合”协议的想法。当一种协议用于控制网与隔离区的通信时，它最好就别再应用于办公网络与隔离区的通信。这种设计极大地降低了像 Slammer 这样的蠕虫病毒入侵控制网络，因为对于蠕虫病毒而言，两种不同的协议就需要两种不同的形式，这还是有点困难的。

由控制网络操控对外的通信是实践中很大的一个变动，但如果管理不当，也可能带来重要的安全风险。一个例子是特洛伊木马软件使用 HTTP 协议获得了定义简单的对外规则。因此，对外规则应当和对内规则一样严格。

下面列举了一些总结：

- 对内规则是被禁止的，接入控制系统中设备的操作必须经过隔离区。
- 对外规则必须被限制，只用于必要的通信。
- 从控制网络到办公网的连接必须通过服务和端口严格控制源和目的。

除去这些规则外，防火墙还应当配置外出过滤规则，以阻止伪造的 IP 数据包从控制网络或者隔离区出逃。由防火墙的各个接口地址对比外出数据包的源 IP 地址实现这一功能。目的在于防止控制网络被通信欺骗(比如伪造 IP)，这种欺骗往往用于 DoS 攻击。这样，对于控制网络和隔离区，防火墙只认可那些拥有正确源 IP 地址的数据包。最后，控制网络中的设备接入互联网是绝对被制止的。

下面总结了防火墙规则制定中要特别注意的：

- ✧ 基础的规则是拒绝一切。
- ✧ 控制网络环境和办公网间端口通信及服务批准时，应该具体问题具体分析。对于每次数据的出入，都必须有商业理由，并且有记录在案的风险分析和责任人。
- ✧ 如果状态合适，所有允许规则应该包含 IP 地址和 TCP/UDP 指定端口。
- ✧ 所有规则都应该限制通信使用制定 IP 地址或地址段。
- ✧ 禁止所有控制网络和办公网的直连，所有通信的终点都是隔离区。
- ✧ 当一种协议用于控制网与隔离区的通信时，它就不再应用于办公网络与隔离区的通信。
- ✧ 从控制网络到办公网的连接必须通过服务和端口严格控制源和目的。
- ✧ 控制网络和隔离区的外出包，必须具备控制网络或隔离区制定正确的 IP 地址。
- ✧ 控制网路中的设备不能接入互联网。
- ✧ 即使有防火墙的保护，控制网络不可以直接接入互联网、
- ✧ 所有防火墙管理的通信都应当包含一个独立、安全管理的网络或者多因素认证的加密网络。此外对于特定管理情况，通过 IP 地址也可以对通信做出限制。

当然这些都只应被视为准则，在部署和设置防火墙规则时，对每个控制环境的仔细评估才是最必要的。

5.6.针对特定服务的防火墙规则

除了上述的通用规则，很难一一列出针对每个特定的协议的规则。对于不同

的协议，需求和建议的做法也会显著不同，这就需要一一对应的分析。工业自动化开放网络协会(IAONA)提供了实施的模板，如分析，评估工业环境中每一个常见协议的功能，安全风险，事件的最坏影响，建议措施。下面总结了 IAONA 文档中的一些要点，读者设计规则时可以参照这些文档。

5.6.1 域名系统

域名系统(DNS)主要用于域名和 IP 地址间的解析。比如，DNS 可以将一个域名“control.com”解析为 IP 地址“192.168.1.1”。大多数互联网服务都依赖于 DNS，但在控制网络中应用则较为罕见。在大多数案例中，从控制网络到办公网的 DNS 请求很少被允许，而进入控制网络的 DNS 请求则是完全被禁止的。从控制网路到隔离区的 DNS 请求则需要具体问题具体分析。建议使用本地 DNS 或主机文件。

5.6.2 超文本传输协议(HTTP)

HTTP 是 Web 浏览器在互联网应用最基本的协议。如 DNS 一样，它在大多数互联网服务上的应用也极为重要。可以看到，如同一个万能查询工具一样，它的应用也与日俱增。不幸的是，它并没有什么安全保障，许多 HTTP 应用存在可以被攻陷的安全隐患。HTTP 可以作为一种传输机制，用于手动攻击和自动蠕虫病毒。

总之，HTTP 是不能被用于办公网和控制网络间通信的。如果不禁止，防火墙上就必须配置 HTTP 代理用于阻止所有进入的脚本和 java 程序。由于其表现出的安全风险，向控制网络发出的 HTTP 连接是禁止的。如果连接控制网络的 HTTP 服务是必须的，我们也建议针对特定服务使用更为安全的 HTTPS。

5.6.3 FTP 和 TFTP

FTP 和 TFTP 用于设备间传输文件。因为其广为人知且占用很少的进程资源，它们广泛应用与各种平台，包括 SCADA 系统，DCS，PLCs 和 RTUs。可是这两种协议并不安全：FTP 的登录密码不是保密的，而 TFTP 干脆不需要登录。再者，一些 FTP 实现存在缓存区溢出的历史安全隐患。因此，应该禁止所有 TFTP 通信。

FTP 通信只能应用于对外会话或者考虑了更多安全性的情况，如基于令牌的多因素认证和加密隧道。需要的时候，应该配置像安全 FTP(SFTP)或者安全拷贝(SCP)之类更安全的协议。

5.6.4 Telnet

Telnet 协议定义了一种客户端和服务器之间交互的基于文本的通信会话方式。主要用于远程登录和对限制了资源或者限制了安全的系统的简单控制服务。其服务器端具有安全风险，因为所有远程登录，包括密码都是未加密的，而且它可以让个人通过设备远程控制。从办公网到控制网络的发起的远程登录会话必须被禁止，除非加入了基于令牌的多因素认证和加密隧道这样的安全机制。而对外远程登录会话只应用在使用了加密隧道技术(如 VPN)的特定设备。

5.6.5 简单邮件传输协议(SMTP)

SMTP 是一种应用于互联网上的 e-mail 传输协议。E-mail 信息通常包含恶意软件，控制网络中任何设备都不得接受对内 e-mail。从控制网路发往办公网的警告信息则是可以通过 SMTP 协议的。

5.6.6 简单网络管理协议(SNMP)

SNMP 用于为中心管理控制台和网络设备提供网络管理服务，网络设备包括路由器，打印机，PLC 等。尽管它广泛应用于网络管理，但其安全性也很薄弱。在第一版和第二版的 SNMP 中，读取和配置设备使用的密码没有进行加密，很多情况下，大家都知道密码且不可修改。第三版考虑更多的安全性，但收效甚微。除非是独立、安全的管理网络，第一、二版的 SNMP 应当被禁止。第三版则可以用于给 ICS 发送信息。

5.6.7 分布式对象组件模型(DCOM)

DCOM 也是一种基本协议，为用于过程控制的对象连接与嵌入(OPC)和 ProfiNet 所使用。它利用微软远程过程调用(RPC)服务，当没打补丁时拥有很多

缺陷。这些缺陷被冲击波蠕虫病毒利用。此外，OPC 利用 DCOM，动态打开广域的端口(1024-65535)，这使得防火墙很难做出防范。这种协议只能应用与控制网络与隔离区。同时建议对使用了 DCOM 的设备做出端口范围的限制。

5.6.8 SCADA 和工业协议

SCADA 和许多工业协议，如 MODBUS/TCP、EtherNet/IP、DNP3，对很多控制设备的通信是很重要的。不幸的是，这些协议设计时并未考虑安全性，通常远程控制设备接入时也不需要用户验证。这些协议只能在控制网络内使用，而不得跨网络。

5.7.网络地址转换(NAT)

某以往段中的 IP 地址在另一个网段中无法识别,这时候我们需要 NAT 服务。最初设计它是为了减少 IP 地址消耗，这样一家拥有大量需要接入互联网设备的企业就可以通过分配的很少的一部分互联网地址访问网络。

为了做到这一点，又一个前提，内网设备一般不会同时访问外网。防火墙也会对访问外网的 IP 地址数量做出控制。当内网主机试图连接外网时，防火墙重构内部的 IP 地址和端口为一个未使用的、限制性更强、对外公共的 IP 地址。防火墙必须跟踪每次连接的状态，保证内部 IP 地址和端口到外部可见的 IP 地址和端口的映射的正确。当回包到达防火墙，映射关系反转，数据包可以发送到正确的主机。

比如，控制网络中一个设备可能需要建立一个到非控制网络主机的连接(如发送一个重要的警告 e-mail)。NAT 允许控制网络重构内网主机的 IP 地址，随后回包根据内网 IP 地址被送往内网设备。特殊的，如果为控制网络分配私有网段 192.168.1.xxx 而互联网分配给企业的网络地址段位 192.6.yyy.zzz，NAT 防火墙将替代(跟踪) 控制网络设备产生的外出数据包 IP 地址为 192.6.yyy.zzz 的源地址。

生产者-消费者协议，如 EtherNet/IP 和现场总线尤其麻烦。因为 NAT 不支持基于组播的通信，而这些协议则需要提供完全的服务。

总之，NAT 提供了明显的优势，其在实际工业协议和配置上的影响也是我们在部署前应当仔细评估的。另外，由于没有直接的地址，某些协议也会被 NAT 影响。比如 OPC 使用 NAT，就需要特殊的第三方隧道软件。

5.8 ICS 和防火墙的一些具体问题

除了之前讨论的防火墙和 ICS 之间的问题，还有一些需要细节核实。本节下面的内容将描述具体的三个方面：海量数据记录系统的部署，支持 ICS 的远程登录，组播。

5.8.1 海量数据记录系统

控制网络、办公网络共享的服务器，如海量数据记录系统和资产管理服务器，对防火墙的设计和配置有明显的影响。三块区域的架构，将这些服务器放在隔离区中相对简单，而在两块区域的架构中则显得比较困难。将服务器放在办公网中，意味着很多不安全的协议需要通过防火墙，如 MODBUS/TCP 或 DCOM，这样每一个和海量数据记录系统通信的控制设备就暴露在办公网面前。相反，如果将服务器放在控制网络中，意味着同样有安全隐患的协议需要通过防火墙，如 HTTP 或 SQL，那么办公网中的每个人都可以随意接入控制网络了。

所以，最好的办法就是使用 3 块区域的架构，将数据收集器放在控制网络，海量数据记录系统放在隔离区，尽管在某些情况下，这种设计也有点问题。办公网中大量用户接入隔离区海量数据记录系统会加重防火墙的吞吐负担。一个可行的解决办法是安装两台服务器。一台位于控制网络中用于收集数据，另一台则位于办公网中，镜像第一台服务器，支持客户端序列。如何令海量数据记录系统同步的问题将被解决。这也需要防火墙为服务器之间的通信提供一个专门的通道，如果做得正确，只会存在轻微的风险。

5.8.2 远程登录

另一个 ICS 防火墙设计的问题是远程登录控制网络。任何用户远程登录控制网络时，都需要使用适当的强有力的认证机制，如基于令牌的认证。虽然控制组

可以在隔离区设置有多因素认证的远程登录系统，通常信息技术部门设置的系统则更为有效。这种情况下，我们需要信息科技远程接入防火墙的通信。

远程支持私人连接互联网或通过调制解调器应该使用加密的协议，如运行一个办公网络连接客户端，应用服务器或安全 HTTP 接入以及使用强大的认证机制，如基于令牌的多因素认证方案，以便连接到办公网。一旦连接，它们立刻在控制网络中的防火墙进行用户认证，以接入控制网络。由于企业不允许控制网络也办公网明显的直连，这就需要一个级联或继发隧道方案，以接入控制网络，如 IPsec VPN 中的安全套接层(SSL)或传输层安全(TLS)VPN。

5.8.3 组播

大部分实施在以太网的工业生产者-消费者(发布者-订阅者)协议都是基于 IP 组播的协议，如以太网/IP 和现场总线安全。IP 组播的第一个优势在于网络性能，不需要重复向组播地址传输数据，可以显著降低网络负载。第二个优势在于发送主机不需要关注每个目的主机的 IP 地址。第三点，也许对工业控制来说是最重要的一点，组播消息为控制设备组提供了更好的同步性。

如果多播数据包的源、目的之间没有路由器和防火墙，多播传输相对是无缝的。但如果源和目的不在同一网段，多播信息的传输则会困难一些。为了解决多播信息路由的问题，主机需要通过英特网组管理协议(IGMP)通知组播路由器加入(或离开)相关组。组播路由器随后得知组播组中的成员，从而决定是否接受组播信息，这里也需要组播路由协议。从防火墙管理角度来看，制定监控并过滤 IGMP 的规则，增加了防火墙的复杂度。

另一个防火墙与组播之间的问题是对于 NAT 的使用。防火墙使用 NAT，当接收到一个外部主机发送的组播数据包时，没有反响映射出内部哪个组应该接收这个数据。如果使用 IGMP，防火墙就会将数据广播给所有组，毕竟总有一个组是正确的目的。当然，严重的问题随之产生：可能一个计划外的数据包会被广播到一个重要的节点。最安全的办法就是让防火墙丢掉这个包，也就意味着组播与 NAT 似乎不大兼容。

5.9 单点失败

单点故障可以发生在 ANSI/ISO 中的任一层。一个例子是可编程逻辑控制器安全连锁控制。应该做一个找出潜在故障点的评估，并对每个故障点做风险评估。然后我们就可以假设，评估，设计，实现相应的补救办法。

5.10 冗余和容错

ICS 部件或网络被列为具有高可用性的方案。一种实现高可用性的方法是使用冗余。另外，如果一个部件失效了，他不应该使得 ICS 的网络出现整体故障，也不会在其他任意部分出现问题，比如级联事件。

控制系统应该能在 ICS 通信失效或 ICS 整体失效后执行适当的故障处理。我们应当规定通信失效的时间(5 秒无连接还是 5 分钟无连接等)，也应当更加潜在的结果，规定对工业合适的故障处理方法。

备份需要采用“深度备份”的方式。层备份(本地，设备，灾难)具备时间序列，这样最近的本地备份可以立刻使用。安全备份则可以恢复大量的安全事件。混合的备份及再生的方式和存储方法的使用，确保了备份的严格生产，安全存储，恢复数据的适当访问。

5.11 预防中间人攻击

中间人攻击需要对网络协议的知识有着一定的掌握。地址解析协议(ARP)中间人攻击是一个比较普遍的获得目标系统网络流量信息的方法。表现为对网络 ARP 缓存表控制器和工作站机器的攻击。通过控制网络中被感染的主机，攻击者伪造 ARP 表，并通知所有主机路由时必须经过某个指定的 IP 地址。通过构造 ARP 表，攻击者可以将自己置于两台目标主机之间。

ARP 中间人攻击通过非法 ARP 命令迷惑主机。这些 ARP 命令使得目标主机中的任意一台与另一台通信时，将攻击者的 MAC 地址作为自己的地址。中间人攻击成功时，被攻击的两台主机都不知道自己传输的数据经过了攻击者的主机。

当攻击者成功的将自己的主机加入到信息流中后，他们就有了对数据通信的完全控制并可以带来多种攻击方式。重演攻击是其中的一种可能，最简单的，从控制器/人机界面捕获的数据在设备控制器收到时被动态修改为实例。捕获的数据反映 ICS 中的正常操作，需要的时候可以重演一次。这就导致了攻击者能够观测到操作者在人机界面中所做的一切。攻击者可以持续的向控制器和设备发出命令，导致意外事故，而此时操作者对系统的真实情况一无所知。

另一种中间人攻击方式是向操作者发送错误的信息，形式可能是非错误或非正确的。这将会到这操作者才不需要做出反应的时候往往采取了诸如关机的措施，或者在需要做出反应时什么都没做。攻击者可以向操作者控制台发送命令以显示系统的变化，而当操作者按照正常程序试图做出更正时，往往发生意想不到的问题。有很多变动修改和重放控制数据的方法会影响系统的运作。

已发现的，在控制系统中，协议操作和中间人攻击是最普遍的操控协议安全的方法。幸好我们还有一些技术可以增加系统的安全性：

MAC 地址绑定：ARP 中间人攻击需要攻击者接入本地网络或控制本地网络中的主机。端口安全性，也被称之为 MAC 地址绑定，是一个保证交换机每个端口末梢物理连接安全的方法。高端企业级网络交换机通常会有几种 MAC 地址绑定的办法。MAC 地址绑定对防止攻击者进入内部网络是很有效的。没有端口安全性，任何公开网络都可以作为进入办公网的途径。端口安全性在管理交换机上讲制定 MAC 地址和制定端口绑定。如果 MAC 地址不匹配，通信将会被终止，攻击者也将无所作为。一些更高级的交换机则具备自动重置功能，这样原始 MAC 归还到端口后，可以重置匹配策略。

尽管端口安全性不能证明谁是攻击者，它为物理网络增加了一层安全保护。它同时保护了本地网络不被雇员和过期系统破坏。它降低了攻击者远程可控制主机的数量。这种安全策略不但预防了外部的攻击者，也提供了物理上的保护。

静态路由表：ICS 网络可以保存一张静态 ARP 表。很多操作系统都可以静态地将 MAC 地址记录到 ARP 表上。每台主机记录一张静态 ARP 表可以防止攻击者通过发送 ARP 回包修改 ARP 表欺骗主机。虽然这一技术并不适用于大型或动态办公网络，但主机数量受到限制的 ICS 网络则可以很好的用这种方式保护。

加密技术：作为一个长期的解决方案，系统设计应当在设备之间加密，这样

在控制网络中伪造数据包和反向编译协议则会变得较为困难。设备间通信时加密会使得其不易被攻击。具有强力认证机制的协议也很好的预防了中间人攻击。

监控技术：监控 ARP 欺骗提供了又一层的保护。有很多程序可以监控通过 ARP 包修改 MAC 地址的欺骗行为。

6. ICS 安全控制

安全控制是一个信息系统保护其信息的保密性、完整性和有效性而制定的管理、操作和技术控制（例如预防措施或干扰）。这一节讨论了指定在 NIST SP 800-53 中的安全控制，它作为 FISMA 项目实施的一部分而开发的。有关 FISMA 和 NIST 领导实施项目的其它信息，详见附录 E。

NIST SP 800-53 在联邦政府信息系统的支持下，提出相应的准则为信息系统选择和指定安全控制。安全控制的组织分为三个等级；管理、操作和技术控制。每个等级分为若干个成员；每个控制包括控制的定义，补充指导和可能的改进，将提高基本控制的强度。

NIST 就工业控制系统的安全项目，已经与公共和私有部门 ICS 合作，为 NIST 文件的应用指定具体的准则，包括 NIST SP 800-53 到 ICS 的安全控制。为了便于理解这种方式，正致力于使用实际的 ICS 网络安全事件开发一系列 ICS 网络安全工程案例。这些工程案例检查了 NIST SP 800-53 ICS 控制是否实施，如果已经实施了该控制，那么检查假定可能已经发生的潜在措施。下面红字部分为每组控制提供了 ICS 具体的建议和指导。

一个单独的安全产品或技术不能充分保护一个 ICS。保护一个 ICS 是基于有效安全性策略和适当配置的一组完全控制的组合。对于一个 ICS 来说，一个有效的网络安全策略必须应用深度防御——一种分层的安全机制技术，使任意一个机制失效所产生的影响最小化。以下在安全控制讨论中探讨纵深防御策略的使用和在 ICS 的应用。

6.1 管理控制

对一个 ICS 来说，管理控制是安全对策，因为其集中在风险的管理和信息安全的管理。NIST SP 800-53 在管理控制等级中定义了 5 个控制成员：

安全评估和授权(CA)：确保指定的控制得到正确实施，按照预期操作，并产生期望的结果。

规划(PL)：一个规划的开发和维护，通过执行评估，指定和实施安全控制，分配安全级别和事件响应来解决信息系统安全性问题。

风险评估(RA)：识别风险的过程是由确定事件发生的概率来操作、评估所造成的影响，其它的安全控制将减轻这种影响。

系统和服务获取(SA)：对信息系统的安全来说，资源分配维护贯穿整个系统的生命周期和基于风险评估结果的获取措施的发展，包括需求、设计标准、测试程序和相关文档。

项目群管理(PM)：提供组织级别的安全控制，而不是信息系统级别的安全控制。

在这节接下来的内容中，对这些管理控制进行详细讨论。下面红字部分提供 ICS 具体的指导和意见。

6.1.1 安全评估和授权

属于 NIST SP 800-53 评估和授权成员的安全控制，为执行周期性评估提供了基础，并提供了安全控制证书。在信息系统中，该证书实施决定了该控制能否得到正确实施，按照预期操作，并产生期望的结果来满足系统的安全需求。一个高级管理人员对接受剩余危险和授权系统操作负有责任。这些步骤完成认证过程。另外，所有的安全控制必须按照持续的原则进行监控。监控活动包括配置管理和信息系统组成控制，系统安全影响分析，安全控制持续评估和状态报告。

在以下文档中获取关于 CA 控制的详细指导：

NIST SP 800-12 提供安全政策和程序的指导

NIST SP 800-26 和 800-53A 提供安全控制评估的指导

NIST SP 800-37 提供定义信息系统界限和信息系统安全证书和的指导

6.1.2 计划

一个安全的规划是一个正式的文档，它为信息系统提供了一个安全需求概况，并且在合适的位置描述安全控制，用于满足某些需求。隶属于 NIST SP 800-53 规划成员的安全控制，为开发安全计划提供了基础。这些安全控制也解决了周期性更新安全计划的问题。在授权进入系统之前，有关信息系统的一系列规则描述了用户的责任和预期行为，用户签署同意使用条款表明他们已经读懂并同意遵守这些行为规则。

在以下文档中获取关于 PL 控制的详细指导：

NIST SP 800-12 提供安全政策和程序的指导

NIST SP 800-18 提供行为预备规则的指导

ICS 具体建议和指导：

对于 ICS 来说，一个安全的规划应该建立在适当的现有 IT 安全方面的经验、计划和实践中。但是，3.1 节所讨论的 IT 和 ICS 之间最关键的不同之处，将影响安全机制如何应用在 ICS 中。一个前瞻性的规划需要提供一个可持续安全改进的思想。无论新系统何时设计和安装，从结构到采购到安装到维护到解除，花时间解决遍及整个系统的安全问题非常必要。ICS 安全是一个快速发展的领域，要求安全规划过程中，不断探索新兴的 ICS 的安全功能，如美国 CERT 的控制系统的安全中心(CSSC)一样不断确定新的威胁。

6.1.3 风险评估

风险是一种功能，给定威胁源利用潜在安全漏洞的可能性和成功利用该漏洞所造成的影响。风险评估是一个识别组织运作、资产和个人风险的过程，该过程由识别出的漏洞所造成影响的概率所确定。一个评估包括一个安全控制评价，这个安全控制能减轻每个威胁和实施相关安全控制的成本。一个安全评估也必须比较安全成本和一个事件相关的成本。

实现可接受风险级别是一个减少事件发生概率的过程，通过减轻或消除可利用漏洞和事件所造成后果的方法实现这个过程。安全漏洞的优先顺序必须基于成本，并且提供一个业务案例，至少实施一个最小的控制系统安全性需求，降低风险到可接受级别，从而使目标受益。在试图选择和实施安全控制之前，必须进行漏洞和风险评估。

属于 NIST SP 800-53 风险评估成员的安全控制提供政策和操作步骤，开发、分发和维护一个成文的风险评估政策，描述安全控制的目的、范围、作用、责任和政策的实施步骤。基于安全目标和风险级别范围对信息系统和相关数据进行分

类。执行风险评估来识别风险和一个信息系统及其数据未经授权的访问、使用、泄露、破坏和修改或所可能导致危害的程度。这些安全控制还包括保持风险评估更新、执行周期性测试和漏洞评估的机制。

FISIM 风险架构如附录 E 图 E-1 所示。在安全分类活动和基线安全控制选择活动之后，使用安全评估过程。在安全控制细化活动中执行风险评估，确定是否需要增强所选择的安全控制或者扩展超出基线安全控制。NIST SP 800-30，信息技术系统风险管理指南（目前正在修订中）提供了一套风险评估方法，包括以下步骤：

1. 系统特性—产生一个信息系统环境图以及信息边界轮廓图
2. 威胁识别—产生一个包含能利用系统漏洞的威胁源清单的威胁声明
3. 漏洞识别—产生一个能被潜在威胁源利用的系统漏洞清单
4. 控制分析—产生一个计划控制清单，用于信息系统减轻利用漏洞的概率，降低有害事件的影响
5. 可能性测定—产生一个可能性评级（高、中或低），表明潜在漏洞可能被利用的概率
6. 影响分析—产生一个利用漏洞所导致的影响程度（高、中或低）
7. 风险测定—产生基于高、中或低度量的风险测量
8. 控制建议—产生安全控制建议和减轻风险的替代解决方案
9. 结果文档—产生一个风险评估报告，描述风险的威胁、漏洞和测量，并为控制的实施提供建议

在以下文档中获取关于 RA 控制的详细指导：

NIST SP 800-12 提供安全政策和程序的指导

NIST SP 800-39 提供管理风险评估和更新的指导

NIST SP 800-40 提供处理安全补丁的指导

NIST SP 800-115 提供网络安全测试指导

NIST SP 800-60 提供为信息类型安全分类确定的指导

ICS 具体建议和指导：

机构必须考虑在 ICS 中一个事件所导致的潜在后果。减轻风险技术由明确的政策和程序所确定，设计该技术用于阻扰事件发生和管理风险，消除或使后果最小化。物理设备潜在的退化、经济地位或者利益相关者/民族信心都能证明减轻是正当的。对于 ICS 来说，风险评估一个非常重要的方面是确定从控制网络流向办公网络的数据价值。在由这个数据确定价值决策的实例中，数据可能有非常高的价值。通过比较减轻风险的成本和后果的影响，得出减轻风险的财政理由。但是，定义适合所有安全要求的政策是不可能的。也许能实现一个非常高级别的安全控制，然而，由于功能的丧失和其它相关成本，其在大多数情况下是不合适的。一个深思熟虑的安全控制实施必须平衡风险和成本。在多数情况下，风险可能是安全的、健康的或者与环境有关的，而不是纯粹与经济相关。这个风险可能导致不可恢复的后果，而不是临时的金融挫折。

6.1.4 系统和服务获取

属于 NIST SP 800-53 系统和服务获取(SA)成员的安全控制，为满足保护信息系统准确资源获取的需求而制定政策和程序提供了基础。这些服务的获取基于安全需求和安全规范。作为获取步骤的一部分，使用系统开发生命周期的方法管理一个信息系统，包括信息安全方面的考虑。作为获取的一部分，必须在信息系统和构成组件上维持足够的文档。SA 成员也可以处理外包系统，所支持的组织指定的供应商提供足够的安全控制。供应商在这些外包信息系统的配置管理和安全测试方面负有责任。

在以下文档中获取关于 SA 控制的详细指导：

NIST SP 800-12 提供安全政策和程序的指导
NIST SP 800-23 提供使用和获取测试/评估信息技术产品的指导
NIST SP 800-27 提供信息系统安全工程原理的指导
NIST SP 800-35 提供信息技术安全服务的指导
NIST SP 800-36 提供在系统开发生命周期中安全方面的考虑的指导
NIST SP 800-65 提供将安全性融入资本规划和投资控制过程的指导
NIST SP 800-70 提供系统技术产品的配置设置的指导

ICS 具体建议和指导：

一个组织外包管理的安全需求和它所有或者一部分信息系统、网络和桌面环境的控制问题必须在合同当事人之间的约定中得到解决。影响组织安全性的外部供应商必须保持相同的安全政策和程序，保证 ICS 安全性的整体级别。在影响 ICS 安全性的案例中，第二层和第三层供应商的安全政策和程序也必须按照企业网络安全政策和程序。SCADA 和控制系统获取项目[47]开发了一个获取语言，用于当获取新系统或者维护现有系统时指定安全需求。

6.1.5 程序管理

属于 NIST SP 800-53 项目群管理（PM）的安全控制，关注的是企业范围内的信息安全要求，它与任何特定的信息系统是无关的，并且对于管理信息安全项目至关重要。

6.2 操作控制

操作控制是应对 ICS 的安全对策，主要由人代替系统实施和执行。NIST SP 800-53 定义了 9 种控制方法：

人员安全(PS)：人员职位分类、筛选、转移、罚款和终止的策略和程序，也涉及了第三方的人员安全。

物理及环境保护(PE)：用于解决物理、传输和显示访问控制的策略和程序，如空调环境控制(温度、湿度)和紧急防备(关机、电源、照明、防火)。

应急计划(CP)：维持或恢复业务运营的策略和程序，包括在紧急情况下，系统故障或灾难事件中的电脑操作。

应急管理(CM)：硬件、固件、软件和文件修改控制的策略和程序，保障了信息系统在实施过程中和实施后不被非正常修改。

维护(MA)：管理信息系统中所有维修方面的策略和程序。

系统及信息完整性(SI)：从设计缺陷，使用功能的核查数据修改，数据完整性检查，入侵检测，恶意代码检测，安全警戒和咨询控制等方面保护信息系统和数据的策略和程序。

媒体保护(MP)：确保安全处理媒体的策略和程序。控制包括访问、标签、存储、运输、杀毒、销毁和处置。

故障响应(IR)：故障响应培训、测试、处理、监测、报告和支持服务有关的策略和程序。

安全意识及培训(AT)：根据信息系统用户对系统的使用确保他们接受了适当的安全培训的策略和程序，并持续记录培训情况。

下面的内容会描述这些操作控制的细节，下面红色字内容给出了需要的对ICS 的指导和建议。

6.2.1 人员安全

NIS SP 800-53 人员安全(PS)中安全控制方法提供的策略和程序，减少了人为错误、盗窃、诈骗或其他有意无意滥用信息系统的风险。

下列文件中可以找到 PS 控制的补充指导：

NIST SP 800-12 给出安全策略程序的指导

NIST SP 800-35 给出信息技术安全服务策略程序的指导

NIST SP 800-73 给出个人身份验证接口的指导

NIST SP 800-76 给出个人身份验证识别的指导

人员安全策略主旨在于减少人为错误、盗窃、诈骗或其他有意无意滥用信息系统的风险。它有三个方面的概念：

雇佣策略：这包括雇前的筛选，如背景调查，面试过程，就业条款及条件，完整的工作和职责的描述，雇佣条款条件的详细说明，还有员工和雇主的合法权益和责任。

企业策略和实践：包括安全策略，信息分类，文档和媒体的维护和处理策略，用户培训，企业资产可用策略，员工绩效定期评估，适当的背景调查，以及其他任何策略和行为，这些策略和行为可以细述员工、雇主、访问者都做了什么。企业的策略必须记录下来，并通过各种方式让员工知道。

就业条款和条件：这部分包括明确工作岗位职责，通知员工纪律处分及处罚，并定期评估员工绩效。

ICS 具体建议和指导：

职位的分类应该根据风险的制定和筛选标准，每加入一个新员工，都要根据筛选标准筛选，被授予访问信息系统权限时也要如此。任何控制和维护 ICS 的人员都需要进行筛选。

6.2.2 物理及环境的保护

NIS SP 800-53 物理及环境保护(PE)中安全控制方法提供了物理接入信息系统的策略和程序，如指定节点的出入，媒体传输和播放。包括了物理接入，日志维护和访问者处理的控制。这一系列也包含了应对紧急保护的部署和管理，如关闭信息技术系统，备用电源和照明，温度和湿度的控制，防火防潮。

下面的文档中可以找到 PE 控制的补充指导：

NIST SP 800-12 给出了安全策略程序的指导
NIST SP 800-46 给出了电信和宽带通信的安全性的指导

物理安全性措施，旨在减少意外或蓄意的厂房资产和周围环境的损失。有形资产应该被保护好，如工具和工厂设备，环境，周围的社区，以及知识产权。知识产权又包括了如工艺过程和客户姓名在内的私有数据。物理安全性控制的部署往往受环境、安全、管理、法律和其他要求影响，一个特定的环境，必须识别和处理的要求。物理安全性控制的任务是比较大的，也需要针对保护需要。

ICS 具体建议和指导：

网络组建保护和 ICS 数据整合应当被看做厂房整体安全的一部分。对于厂房安全而言，许多 ICS 设备的安全性是紧密相连的。一个主要的目标是，在没人阻止他们的工作或没有进行紧急应变程序时，也能使人们远离危险情况。

获得控制室的物理入口或控制系统的组成部分，往往意味着获得控制系统进程的逻辑入口。同样，逻辑访问，如同主服务和控制室的电脑让攻击者尝试控制物理过程。如果计算机有移动媒体设备(软盘，光盘，外置硬盘)或 USB 端口，它们会容易攻陷。我们可以为其配备固定的媒体设备，或干脆禁用这些设备和 USB 端口。根据安全需要和风险，甚至可以对电源按钮进行控制使用。为了安全最大化，服务器应当置于被保护的地方，并有认证机制保护。同时，ICS 网络中的设备，包括交换机、路由器、网络插孔、服务器、工作站、控制器也应当安置在安全的区域，且只能有经授权的人员访问。安全区域也应符合设备对环境的要求。

物理安全的一个深度解决方案应包含下面几点：

物理位置的保护：传统的物理安全考虑，通常是指一个环状结构分层安全措施。在建筑物、设施、房间、设备或其他信息资产周边建立一些主动或被动的物理安全屏障。物理安全性控制旨在通过一些工具保护物理位置，包括围栏、壕沟、土丘、墙、路障、门或其他工具。大多厂房都有这种层级模式防止入侵，使用栅栏、设置门卫、大门、锁门。

访问控制：访问控制系统需要确保，只有授权人能够访问控制区域。访问控制系统应该很灵活。访问需求往往基于时间、培训等级、就业状态、工作分配、厂房状况和无数其他因素。系统需要能够鉴别出试图访问的人是谁(通常依靠这个人所持有的接入卡或密钥，这个人的个人识别编号或直接通过识别设备辨别)。访问控制应该高度可靠，不会影响到员工日常或紧急工作。将访问控制系统集成到过程系统中，不但可以安全访问，而且能够跟踪物理及个人资产，加快紧急事件的反应事件，保障个人安全并提高整体生产力。在一个区域内，访问网络和计算机的人员应当被限制在那些确实有需要的网络技术人员、网络工程师和计算机维护人员中。设备应当被锁保护，布线也应尽量隐蔽。考虑将所有计算机安置在安全机架，使用外围设备扩展技术与这些计算机的人机界面互联。

访问监控系统：访问监控系统包括摄像机，传感器和各类识别系统。比如通过摄像头监控停车场、便利店或航空安全。这些设备不用于防止访问一个特定区域，相反，他们存储记录，无论是否真实存在的个人、车辆、动物或其他实体。基于部署的访问监控设备的类型提供充足的照明。

访问限制系统：访问限制系统使用组合设备进行控制或防止访问受保护的资源。访问限制系统包括主动和被动的安全设备，如围墙、门、保险柜、大门和警卫。他们往往加上识别和监控系统，提供基于角色的专人和专门团体的访问。

人员和资产的跟踪：从安全角度考虑，定位人员及车辆在大型安装作业中日益重要。资产定位技术可以追踪厂房内人员及车辆的动向，确保他们留在授权区域，找出需要帮助的人员，并支持应急响应。

环境因素：处理系统和数据安全性需求时，考虑环境因素是很重要的。例如，如果一个站点的环境恶劣，系统就应当置于过滤环境中。在煤或铁的生产过程中，这一点尤为重要，因为灰尘有可能导电或导磁。如果存在振动问题，则应为系统安装橡胶外套，防止磁盘损坏和接线连接问题。此外，包含系统和媒体（例如，备份磁带，软盘）的环境应该有稳定的温度和湿度。在特定环境下，如温度和湿

度超标，过程控制系统应产生报警。

环境控制系统：为控制室配备暖气、通风和空调系统(HVAC)，以支持厂房内人员在正常工作和紧急情况下的安全，包括有毒物质的释放。为避免造成更大损失，消防系统需要精心设计。HVAC 和消防系统在增加过程控制和安全的相互依赖关系中扮演了重要的安全角色。如支持工业控制计算机的防火和 HVAC 系统需要对网络事件提供保护。

电力：ICS 可靠的电源必不可少，因此应提供不间断的电源(UPS)。如果又一个应急发电机，UPS 的电池容量也许只需要几秒钟就可以了；但如果依赖于外部电源，UPS 的电池容量可能就需要几个小时了。至少我们需要能确保系统正常关机的电池容量。

6.2.2.1、 控制中心/控制室

为控制中心/控制室提供安全必不可少，这样可以减少潜在威胁。控制中心/控制室常常不断登录主控制服务器，响应速度和持续观测是最重要的。这些区域往往包含自己的服务器，其他关键的主机节点和一些控制器。重要的是进入这些区域是有限制的，只有授权用户使用如智能磁卡或身份识别设备的方法才能进入。在极端情况下，有必要考虑控制中心/控制室的防爆或提供异地紧急控制中心/控制室，这样当控制中心/控制室无法使用时，还有备用方案。

6.2.2.2、 便携的设备

任何时候，用于 ICS 功能的功能的计算机和设备都不能离开 ICS 区。笔记本电脑，便携式工作站或手持设备应被严格保护并不能带离 ICS 网络。防病毒和补丁管理应保持更新。

6.2.2.3、 布线

控制网络布线设计和实施也在网络安全计划中。适用于办公室环境的屏蔽双绞线通信电缆，一般不大适合厂房环境，因为其容易被磁场、无线电波、极端温度、水分、灰尘和震动的干扰。工业 RJ-45 连接器需要应用在其他类型的双绞线以提供对水、灰尘和震动的保护。光缆和同轴电缆往往是更好的选择，因为他们适用于许多典型环境，包括工业控制环境中电气和无线电频率干扰情况下。电缆和连接器应当用颜色标记以区分，这样 ICS 网络和 IT 网络可以明确分开，同时减少了交叉连接的潜在风险。电缆布线控制了接入的最小化(仅授权者)，设备也应置于通风的安全处。

6.2.3 应急预案

应急预案被设计为保存或存储业务运作，包括可能在交互位置发生的紧急事件，系统当机或者灾难等计算机业务。落入到 NIST SP 800-53 应急计划 (CP) 族的安全控制通过定义角色和责任在系统崩溃或故障后分配与存储信息系统相关联的人员或动作来提供政策和程序从而实现应急预案。与应急预案一起，控件也用于应急培训、测试和计划更新，并且用于备份信息进程和存储网站。

ICS 详细建议和指导

应急预案应该包括全部范围的由网络事件导致的故障或问题。应急预案应该包括用于存储系统防止无效备份、并将系统与一切不重要的障碍和能够许可网络事件侵入的连接区分并转换为获取必要的接口和调整。员工应该接受培训并应该熟悉应急预案的内容。从对 ICS 进行恢复的负责人的角度出发，员工应该定期地复习应急预案，并对员工进行测试以确认他们仍然满足要求。组织也有与应急预案紧密相关的商业应急预案和故障恢复预案。这是因为商业应急计划和故障恢复计划对于 ICS 来说尤其重要，具体细节在以下的章节中描述。

6.2.3.1 业务持续预案

业务持续预案提出了在中断的情况下全面保持或者重建生产。这些中断以自然灾难(例如，飓风、龙卷风、地震、洪灾)、无恶意的人为事件(例如，意外设备损害、火灾或者爆炸、操作错误)、恶意的人为事件(例如，被炸弹、武器袭击或者被恶意袭击、侵入者或者病毒)、或者设备故障。从潜在的断供的角度出发，可能需要几天、几周或者几个月的典型时间周期来恢复自然灾害、或者需要几分钟或者几个小时来恢复恶意软件入侵或者机械/电力故障。由于在保障可靠性和机电可维护性方面有各自的方法，一些组织者选择用排除这些故障来源的方式来定义业务持续。业务持续也首要处理长期的商品短缺，因此一切组织者也选择在可考虑的风险范围内限制最小的中断限度。出于 ICS 网络安全目的，不推荐这些限制中的任一种。长期的短缺(灾害恢复)和短期的短缺(操作恢复)都应该被考虑。这是因为这些潜在的中断中的一部分涉及人为事件，与物理安全组织协同工作对于理解这些事件的相关风险和防止相关风险的物理安全措施是至关重要的。对于物理安全组织来获知产品网站仓库数据和可能包括更高等级风险的控制系统也是非常重要的。

在创建一个业务持续预案(BCP)来处理潜在短缺之前，明确用于各种系统的恢复事件和基于典型的商业需要而被涉及的子系统是至关重要的。有两种区别类型：系统恢复和数据恢复。系统恢复涉及通信链路和处理能力的恢复，它通常是制定的恢复时间目标（RTO）。系统恢复定义为恢复所需的通信链路和处理能力所需

的时间。数据恢复包含对过去数据描述作业或产品条件的恢复，通常指定的是恢复点目标（RPO）。这被定义为可以容忍缺失数据的最长时间段。。

一旦恢复目标被定义，则潜在中断的列表应该被创建并且恢复进程应该开始进行并被描述。对于大多数的规模较小的中断，基于致命备品目录的修复和替换动作将被充分提供来满足恢复目标。非真时，应急计划需要被完善。由于潜在的成本和这些应急预案的重要性，这些因素应该被负责业务连续预案的管理人员重新评估来确保修改的业务持续预案是正确的。一旦恢复过程被建立文档，日程表应该被更新来测试部分或者全部的恢复过程。尤其应该注意系统参数数据的备份和产品或者产品数据的证实。不仅仅在它们被生成时被测试，用于对其存储的以下过程也应该被定期检查以确定备份被保存在不会使它们无法使用的环境中，同时备份都保存在一个安全的位置，所以在需要时可以通过授权而被迅速获取。

6.2.3.2 灾害恢复计划

ICS 详细建议和指导

灾害恢复计划(DRP)对于 ICS 的应急可获得性是至关重要的。DRP 应该包括以下事项：

- ✧ 事件的所需响应或者变化期间的条件和环境会激活恢复计划。
- ✧ 在安全条件被存储之前，用所有的额外的电子连接以人为模式来操作过程。
- ✧ 角色和响应者的责任
- ✧ 用于备份的进程和过程和信息的安全存储
- ✧ 完成的和实时更新的逻辑网络示意图
- ✧ 用于将授权后的物理和网络连接到 ICS 的人员列表
- ✧ 交互过程和在包括 ICS 供应商、网络管理者和 ICS 支持人员等的紧急情况下与人员的通信步骤和列表
- ✧ 用于所有组成部分的当前参数信息

这项计划也应该明确在紧急情况下用于实时地替换组成部分的要求。如果可能，难以取得的配件应保有库存

安全计划适应定义一个全面的备份和存储政策。为了构建这项政策，以下事项应该被考虑：

- ✧ 数据或者系统的速度必须被存储。这个需求能满足一个多余系统的需求，须臾的下线计算机或者有效的文件系统备份
- ✧ 关键数据和配置的频率正在改变。这将指示备份的频率和完成率
- ✧ 在线安全和全部以及增加的备份的下线存储
- ✧ 安装介质的安全存、许可 key 和配置信息
- ✧ 确认用于执行、测试、存储和存储备份的个人责任

6.2.4 参数管理

参数管理政策和过程被用于控制对硬件、固件、软件和文档的修改以确认信息系统被保护在系统完成之前、中间、之后不被进行不适当的修改。落入 NISP SP 800-53 参数管理(CM)族的安全控制提供用于建立用于信息系统的基线控制的政策和过程。控制也被定义为保存、监控和文档参数控制变化。应该限制连接到参数设置，IT 产品的安全设置应该被满足与 ICS 操作需求相符合的最具限制性条件的模式。

ICS 详细建议和指导

一项正式的改变管理项目应该被建立并且用于确认所有对 ICS 网络的修改都满足与在资产评估和相关联的风险评估和减缓计划中定义的原始组成部分相同的安全需求。风险评估应该被履行在所有影响安全的 ICS 网络进行的变化上，其包括参数改变、网络组成部分的增加和软件的安装。对政策和过程的改变也被要求。当前 ICS 网络参数必须被熟知和被建立文档。

6.2.5 维护

落入 NIST SP 800-53 维护(MA)族的安全控制提供对信息系统的组成部分的动作路径和预防性维护。这包括维护工具(本地和远程)的利用以及维护人员的管理。

6.2.6 系统和信息保存

维护信息和信息保存保证了易损的数据没有被修改或者被未授权和未删除的管理者删除。落入到 NIST SP 800-53 系统和信息保存(SI)族的安全控制提供用于定义、报告和更改信息系统缺陷的过程。控制用于防止恶意代码进攻、垃圾软件和间谍软件防护和入侵防范，尽管这些防护措施未必适合所有 ICS 应用。当然也被提供用于接触安全戒备和公告以及对信息系统的安全功能的更改。此外，在该族内的用于防范和防止未授权的对软件和数据的更改提供对输入或者输出的数据的限制，并且对准确率、完成率和数据的有效性以及处理错误条件进行检测，尽管这些可能未必对所有 ICS 应用都适合。

ICS 详细建议和指导

控制用于防护恶意代码攻击、垃圾邮件和间谍软件以及入侵防护，但是包括在章节 6.2.6.1 至 6.2.6.3 中的用于控制的这些手段并不适用于所有的 ICS 详细建议和指导。

6.2.6.1 恶意代码攻击

防病毒产品评估文件安装在计算机的存储设备上来防止已知的恶意软件目录中的软件。如果计算机中的一个文件与已知病毒的列表中的病毒匹配，则病毒通过消除进程(例如，隔离，删除)来移除病毒，因此该病毒并不能影响其他本地文件或者通过网络通信来影响其他文件。防病毒软件被安装在工作台、服务器、防火墙和手提设备中。

ICS 详细建议和指导

防病毒工具在被安装、配置、运行整个时间后以及被适当地保存后才能高效地发挥功能来防护已知的攻击方法的状态和有效负载。当防病毒工具在 IT 计算机系统中得到普遍的安全应用后，与 ICS 的共同使用需要适应特别的包括匹配性

检测和改变管理事项和影响因素。

主要的 ICS 供应商推荐甚至支持特殊防病毒工具的使用。在某些情况下，控制系统供应商可能在他们的生产线中使用回归测试，该测试用于支持特别版本防病毒工具，并且提供相关的安装和配置文档。这对于完善参考文档和针对 ICS 影响因素的测试过程具有一定的效果，从而能够填补 ICS 和防病毒提供商文档之间的空白[55]。

一般:

Windows, Unix, Linux 系统等被使用在控制台、工程工作台、数据历史记录中，HMIs 和一般目的的 SCADA 以及备份服务器能够像商业 IT 设备一样受到安全保护：安装推动或者自动更新的防病毒软件、将管理软件和病毒被散布的防病毒服务器更新、将位于进程控制网络中的管理服务器打包、并且通过 IT 网络自动更新。

具有时间依赖性代码的所有其他服务器和计算机(DCS,PLC,仪器)的以下供应商推荐修改或者扩展操作系统或者其它变化使其不同于任何一种能够在 OFFICE 提供商或者计算机商店买到的标准 PC。期待提供商定期发布包含安全补丁的维护版本。

6.2.6.2 入侵检测和防护

对于网络的例如流量模式或者例如日志侵入或者文件来访问这样的系统的入侵检测系统(IDS)进行监控，因此他们能够辨识恶意侵入或者试图闯入系统[56]。IDS 确定例如打开一个新的端口这样的不正常动作、不正常流量模式、或者对于重要操作系统文件的改变而引起适合的安全人员的注意。

两种通常使用的 IDS 的类型：

基于网络的 IDS：这些系统在它们识别认为受到攻击的流量时监控网络和产生警惕。

基于主机的 IDS：这种软件在用户试图破坏安全时监控一个系统的一种或者更多

类型的特性，例如应用日志文件进入、系统配置改变、和系统的机密数据以及对警报和测量的响应。

ICS 详细建议和指导

有效的 IDS 部署典型地涉及基于主机和基于网络的 IDS。在现有的 ICS 环境中，基于网络的 IDS 在控制网络和与防火墙共有的共有网络中被经常安装。基于主机的 IDS 在使用了一般目的的 OS 或者例如 HMIs、SCADA 服务器和工程工作台这样的应用中被经常安装使用。正确地配置，则 IDS 能够大大加强安全管理团队防御攻击的能力。同样也能通过检测网络上的无效流量来改善控制网络的效率。然而，即使 IDS 完成，安全工具在攻击的组织模式超时时能够识别个人攻击。此外，应该注意不要混淆不常用的 ICS 动作例如持续短暂条件混同为攻击。

当前的 IDS 和 IPS 产品在检测和防护众所周知的网络攻击中是有效的，但是直到现在这些工具也没有列出 ICS 协议攻击的地址。IDS 和 IPS 供应商开始完善和共同合作用于各种 ICS 协议例如 Modbus, DNP, and ICCP 的各种 ICS 协议。[57]附录 D 提供一些紧急 IDS 能力的附录信息。

6.2.6.3 补丁管理

补丁是用于解决既存软件中特殊问题或者缺陷的额外的代码。弱点是被开发的缺陷，能够导致对于 IT 系统的未授权连接或者使用户具有比授权用户更高的优先权。

管理和使用软件补丁的系统设计能够以有效消耗的方式帮助组织改善 IT 系统的整体安全性。组织者有效地管理和使用软件补丁能够降低被开发的 IT 系统中弱点的几率。此外，它们能够节约耗费在相关弱点的事件上耗费的时间和金钱。

NIST SP 800-40 版本 2 为那些设计和完成安全补丁以及弱点管理项目和用于测试项目的有效性的组织性安全管理者提供向导来降低弱点。该向导也同样对系统管理者和用于申请和测试补丁以及用于弱点项目的安全解决方案的操作人员有用。

ICS 详细建议和指导

对于 OS 组成部件的补丁在 ICS 环境中明显需要诊断的这种情况下才会生成。补丁应该被适当地进行测试(例如在可对比的 ICS 中下线)从而确定边际效应的可接受能力。建议使用回归测试。对于补丁来说在其它软件上具有相反的效果这不是不正常的。补丁可以移除弱点，但是出于生产性或者安全性的角度，它也可能会带来更大的风险。对弱点打补丁可能也会改变 OS 或者应用程序与控制程序工作的方式，导致控制程序失去其功能。另一种事项是很多 ICS 工具的操作系统的旧版本不再被供应商支持。导致可得到的补丁可能不会被应用。组织者应该完成系统的、可计算的、和用于管理暴露弱点的可入文档的 ICS 补丁管理进程。

一旦作出安装补丁的决定，有其它工具从一个中心化的服务器来自动控制进程并且具有补丁被正确安装的证据。考虑到从用于无 ICS 应用程序中分离用于 ICS 补丁管理的自动进程。打补丁应该被安排到发生计划的 ICS 短缺期间。

6.2.7 介质保护

落入到 NIST SP 800-53 介质保护(MP)族中的安全控件提供用于对授权后的用户限制访问介质。控件也用于像分配和处理需求以及存储、传输、清洁处理(信息从数字介质中移除)、销毁和介质的清除。

ICS 详细建议和指导

介质资产包括可移除的介质和软盘、CD、DVD 和 USB 存储棒的设备以及打印出的报告和文档。物理安全控制应该记录用于安全和对这些资产的安全维护的特别需求，以及提供用于传送、处理和清楚或者销毁这些资产的特别指导。安全需求包括防止物理消耗、火灾、盗窃和无意图的分配或者环境损害的安全存储。如果对手获取对 ICS 相关联的备份介质的访问，提供用于开展攻击的有价值的数据。从备份中覆盖授权文件可能会许可密码攻击工具和提取的可用密码。此外，备份在有计划的攻击中典型地包含机器名称、IP 地址、软件版本号、用户名以及其它有用数据。

在作为 ICS 的使用一部分或者与 ICS 相连接的任何节点上任何未授权的 CD、

DVD、软盘、USB 存储器、或者相似的可移除的介质不应该被许可以组织恶意软件的介绍或者数据的物理损失和盗窃。系统组成部分使用未使用的工业标准协议、机械的政策管理软件用于加强介质防护政策。

6.2.8 事件响应

事件响应计划是预先确定的一套指令或者防止过程、响应的文档，并且限制事件结果来防护组织的信息系统。响应应该首先被测量并最主要防护“服务被提供”并不仅仅是被包含的系统。如果一个事件被发现，则会迅速进行用于估测攻击和响应的选择的风险评估。例如，一个可能的响应选择是在收到攻击时进行物理隔离系统。但是，这会导致对于不可实施的丢失的服务产生可怕影响。

落入到 NIST SP 800-53 事件响应(IR)族内的安全控制提供用户事件响应监控、处理和报告的政策和过程。安全事件的处理包括准备、检测和分析、控制、根除和恢复。控制也包括用于人员的响应训练和对信息系统的事件响应能力的测试。

ICS 详细建议和指导

尽管采取防护 ICS 的步骤，通常也会包含有意或者无意的事件。以下症状会从正常的网络问题中发生，但是当几个症状开始出现，则指明 ICS 的模式为受到攻击并且值得进一步观察。如果对手是有技能的，则很明显正在进行攻击。

事件的症状包括以下：

- ✧ 不正常的大量网络流量
- ✧ 移除硬盘空间或者空闲硬盘空间降低
- ✧ 不正常的高 CPU 使用率
- ✧ 生成新用户帐号
- ✧ 管理者等级账户的常识性和实际性的使用
- ✧ 锁定账户
- ✧ 当使用者不进行工作时使用的账户
- ✧ 清除日志文件

- ✧ 不正常的大数量事件的整个日志文件
- ✧ 防病毒或者 IDS 警戒
- ✧ 无作用的防病毒软件和其它安全控制
- ✧ 不期望的打包变化
- ✧ 连接到外部 IP 地址的机器
- ✧ 关于系统的用于请求的信息(社会工程尝试)
- ✧ 不期望的配置设定中的改变
- ✧ 不期望的系统死机

为了将这些入侵的效果最小化，需要计划一个响应。事件响应计划在如下入侵发生时被定义。NIST SP 800-61,计算机安全事件处理指导，其在事件响应计划时提供指导，其可以包括如下事项：

-

事件的分类：ICS 事件的各种类型应该被定义和分类为潜在的影响，因此应该对每个潜在的事件构建正确的响应。

-

响应动作：在一个事件中应该采取几种响应。包括不采取措施到整个系统死机(尽管 ICS 的整个死机是一个不太可能发生的响应)。采取的响应依赖于事件的类型和对 ICS 系统的影响，并且对每种类型的响应应该被提前预测。一项写完的计划将事件的类型归档，并对每种类型的响应应该被提前准备。在可能存在混淆或者由事件而导致的压力时提供指导。这个计划应该包括由各种组织采取的一步一步的动作。如果存在报告需求，这些需求要在报告应该被作出的地点标记从而降低报告混淆。

恢复动作：入侵的结果可以是较小的，或者入侵会导致 ICS 中的很多问题。风险分析家应该确定在 ICS 中被控制为失败模式的物理系统的敏感度。在每种情况下，一步一步的恢复动作应该被归档，由此系统能够尽量快速和安全地返回到正常操作。

在事件响应计划的准备期间，输入应该从各种包括操作者、工程、IT、系统支持供应商、管理、组织劳动力、合法和安全在内的各种参与者。这些参与者也

应该检查和完善计划。

6.2.9 意识和培训

落入 NIST SP 800-53 意识和培训(AT)族的安全控制提供政策和过程，该政策和过程用于确认一个信息系统的所有用户在授权进入一个授权的系统之前被提供基本信息系统安全意识和培训资料。人员培训必须被监控和归入文档。

ICS 详细建议和指导

对于 ICS 环境，必须包括控制系统特别信息安全意识和用于特别的 ICS 申请的培训。此外，一个组织必须认证、归档和培训所有具有明显 ICS 角色和责任的人员。意识和培训必须涵盖被控制的物理进程和 ICS。

安全意识是一个 ICS 事件防护的重要部分，特别在社会工程威胁来临时。社会工程是一项用于操作个人进入的个人信息，例如密码。这项信息能够被用于包括其它的安全系统。

完成一项 ICS 安全项目可能会导致在个人连接计算机项目、应用和计算机桌面本身的方式上发生变化。组织者应该设计有效的培训项目和交流手段来帮助员工理解为什么需要新的访问和控制方式，能够降低风险的想法、以及如果控制方法不被联系到一起对于组织产生的影响。培训项目示出管理的限制，和一个网络安全项目的价值。来自人员的反馈暴露了这种培训对于用于提炼许可和安全项目的范围是一种有价值的资源。

6.3 技术控制

技术控制是安全计测，其通过包含在系统的硬件、软件或者固件中的机械来完成和执行 ICS。如以下子章节中所述的细节，NIST SP 800-53 在技术控制类中定义四个控制族：

鉴定和授权(IA):通过特殊资格(例如密码、象征、生物测定)来更改用户识别的进程、或者设备来作为用于授权连接到 IT 系统中的资源的前提。

访问控制(AC):用于获取和使用信息以及相关的用于物理访问信息系统环境的信息进程服务的授权或者否定请求

审核和解释(AU):独立的记录和评估系统控制的准确性的动作的审核，以确保确立的政策和操作过程的依赖性并推荐在控制、政策和过程中必要的改变

系统和交流保护(SC):用于保护系统和数据传播组成部分的机械

这些技术控制在后面的章节中进一步讨论。如果可以，ICS 详细建议和指导将会对每个章节提供一个框架。与技术控制相关的额外的 ICS 特别指导在 ISA TR99.00.01 [33]能够查询到，EPRI 报告：监督控制和数据入侵(SCADA)系统安全指导[61]。

6.3.1 识别和授权

授权描述正确识别潜在的网络用户、主机、应用程序、和使用识别因素或者证件的结合的资源。这种授权进程的结果会成为许可或者否定进一步的工作的基础(例如当自主提款机请求 PIN)。基于授权决定，系统可以能会许可或者不许可潜在的用户访问它的资源。授权是确定谁应该许可访问特殊资源的进程；访问控制是用于加强授权的机械，访问控制在章节 6.3.2 中被描述。

存在几种用于确定一个人、设备或者系统的授权的因素，包括一些你知道的因素、一些你拥有的因素。例如，授权建立在一些已知的因素上(例如，PIN 号码或者密码)，一些占据的因素(例如，key、软件狗、智能卡)、生物学特征(例如，指纹、视觉签名)、位置(例如，全球定位系统[GPS]定位访问)、作出对时间的请求、或者这些因素的混合。一般地，越多因素被使用在授权进程中，进程则越多。当使用两个或者更多因素时，进程被认为是多因素授权。

落入到 NIST SP 800-53 识别和授权(IA)族中的安全控制提供用于识别信息系统中的用户和设备的授权。这些包括在使用的各个技术中使用的用于管理识别者和授权者的控制。(例如，标志、证明、生物识别、密码、key card)

ICS 详细建议和指导

ICS 环境中的计算机系统典型地以来于用户授权的传统的密码。控制系统提供者经常向系统提供错误密码。这些密码是因素套件并很容易被猜到并被改变，这回产生额外的安全风向。当然，目前在 ICS 环境中使用的协议一般具有不充足或者根据没有网络服务授权，除几种与 ICS 共同使用的传统密码技术之外还存在几种可获得的授权形式。包括密码授权在内的其中一些形式同与它们与 ICS 的使用相关的讨论在以下章节中记述。

6.3.1.1 密码授权

密码授权技术确定基于设备或者人类请求访问应该知道的事项的权利，例如 PIN 号码或者密码。密码授权组织被认为是权威的最简单并且最通用的形式。密码弱点应该通过使用对抗弱点、最近使用的或者通常使用的密码的活性密码检测者来被降低。另外一个弱点是第三团体盗听的情况。通过键板或者键盘输入的密码很容易被观察到或者被记录到，特别是在对手能够设置微小的无线摄像机或者打击的区域。网络服务授权经常将密码作为明码文本传输(非加密)，许可任何网络窃取工具泄漏密码。

ICS 详细建议和指导

ICS 环境具有唯一密码的一个问题是用户重置和输入密码的能力可能会受到时间压力的影响。在人类入侵主要用于控制进程的主要危机期间，操作者可能会恐慌并且难于记忆或者输入密码，以及做出任何一种会使系统被完全锁住或者耽误时间的响应。生物识别者可能具有同样的弱点。组织应该仔细考虑安全需求和在这些主要系统上授权机制的潜在后果。在不支持 ICS 的情况下或者组织者确定可取(例如，表现、安全或者依赖性受到影响)，为了完成 ICS 中的授权机械，组织者使用补偿控制，例如提供与安全能力或者对于 ICS 的防护等级相同的严密物理安全控制。指导也用于涉及 ICS 中 session 锁和 session 中断的使用。

一些 ICS 操作系统使设置安全密码很难，因为密码数量比较小并且系统仅仅许可每个访问的等级的团体密码，而非个体密码。一些工业(互联网)协议以明码文本传输，这使得密码容易被拦截。在这种事项不能被避免的情况下，对于用户来说使用加密和非加密的协议的密码是非常重要的。

以下是关于密码使用的几种常见的推荐和考虑

密码的长度、强度和综合性应该在软件的能力和根本 OS 下平衡安全和访问的操作性。

处于必需的安全角度考虑密码应该具有适当的长度和综合性。特别地，密码不应该在字典里找到或者包含可预料的到的数字或字母。

密码应该与对像重要进程中的控制台的操作接口设备相关。如果操作者被锁定或者重要事件期间延误访问，则在控制台上使用密码会导致潜在的安全事项。在密码保护不可行时，物理安全应该被操作控制。

管理密码的保存者应该是可信任的员工，并在紧急情况下可获取。管理密码的任何拷贝都必须存储在被限定访问的安全位置。

保密用户(例如网络技术、电子电器技术和管理、网络设计者/操作者)的密码应该最为安全并且应该被频繁地改变。更改管理密码的权利是应该被限定给可信任的雇员。密码更改记录特别是管理密码的更改记录应该被保存为与控制系统分离。

在具有窃取和入侵的高风险的环境中(例如缺少本地物理安全访问控制的设备中的远程操作接口)，组织者应该考虑完成具有其它形式的授权的密码授权，例如使用生物或者物理识别的需求/响应或者多因素授权。

处于用户授权目的，密码使用对于用户直接跟踪本地设备或者计算机是正常的、一般可获取的。密码不应该通过任何网络发送除非通过被特别设计为阻止回复攻击的 FIPS 加密或者解密的一些形式防止。假设用户输入到设备的密码以安全模式与网络连接。

出于网络服务授权目的，密码应该尽量被避免。存在更多的安全改变模式，例如挑战-应答或者快键授权。

6.3.1.2 挑战-应答鉴定

挑战-应答鉴定需要服务提供请求者和服务提供者提前知道“秘密”代码。当请求服务时，服务提供者向服务请求者发送一个随机号码或者字符串作为挑战。服务请求者使用秘密代码为服务提供者生成唯一的响应。如果是期待的响应，则证明服务请求者在没有将秘密暴露在网络上的情况下访问了秘密。

挑战-应答鉴定记录了传统秘密授权的安全弱点的地址。在密码(离散的或者平整的)通过网络被发送时，真正的“秘密”的一部分自身被发送。通过将秘密发送给远程设备执行授权。

6.3.1.3 物理标志授权

物理或者标志授权与密码授权相似，但是这些技术是通过测试秘密代码或者由请求访问设备或者标志所产生的 key，例如安全标志或者智能卡。越来越多地，隐私 key 被嵌入到物理设备例如 USB 软件狗中。一些标志仅仅支持单因素授权，因此标志的简单占有对于授权来说已足够。其他标志支持多因素授权，多因素授权除了占有标志外还请求 PIN 或者密码的知识。

被记录了授权地址的最初的弱点很容易复制秘密代码或者与其他人分享。将密码的平常脚本在安全系统中排除，该安全系统被保存在与 PC 或者操作站相邻的防火墙上。在没有对设备和提供进行特别访问的情况下安全标志不能被复制。一个第二益处是在物理标志内的秘密很大、物理上很安全、并且是随机产生的。这是因为它被嵌入到金属或者硅中，这与人为地输入密码没有相同的风险。如果安全标志丢失或者被盗，则授权的用户不能访问，这与传统的密码可以在没有任何迹象的情况下丢失或者被盗窃不同。

物理/标志授权的一般形式包括：

- ✧ 传统物理锁和 key
- ✧ 安全卡(例如：磁、智能芯片、光学代码)
- ✧ 由卡、钥匙链或者张贴标签形式的无线电频率设备
- ✧ 带有附在 USB、计算机连续或者并排的端口上的安全密钥的软件狗
- ✧ 一次性授权代码生成器

对于单因素授权，最大的缺点是物理性地持有标志单元访问被授权(例如，发现丢失的钥的人能够访问他们打开的任何物质)。在与第二形式授权结合时，物理/标志授权更加安全，例如被存储的 PIN 与标志一起使用。

ICS 详细建议和指导

多因素授权是用于从 ICS 防火墙外部访问到 ICS 应用的可接受到的一次有益实践。

物理/标志授权在 ICS 环境中具有较强角色的潜在性。访问卡或者其他标志是用于计算机访问的有效授权形式，只要计算机在安全区域内(例如，一旦操作者使用适合的第二授权来访问室内，则卡可单独用于控制动作)

6.3.1.4 生物授权

生物授权技术通过大概确定人类请求访问的唯一生物特征来决定授权。可用的生物特征包括手指细节、面部识别、视网膜和虹膜的签名、语音模式、输入模式和掌形。

像物理标志和智能卡一样，生物授权加强软件解决方案例如密码授权，其通过提供额外的授权因素和移除记忆复杂秘密中的人类因素。此外，因为生物因素对于给定的个人是唯一的，生物授权记录丢失或者被盗窃的物理标志和智能卡的生物授权的地址。

生物授权的所述事项包括

区别真假(例如，如果从聚硅酮橡胶中区别真正的人类手指或者从被记录的声音中区分真正的人类声音)

生成类型-I 和类型-II 错误(分别拒绝一个有效的生物图像的可能性和接受无效的生物图像的可能性)。生物授权设备应该在这两种可能性之间被配置为最低，也被认为是转向错误率。

一些生物设备对像温度和湿度这样的处理环境因素是非常敏感的

记录雇员在安全眼睛和/或手套上设备的工业应用可能会影响生物扫描

重新训练偶然“漂移”超时的生物扫描。人类生物特性可能也会超时改变，定期的扫描训练成为需要。

需要面对面的技术支持和用于设备训练的改变，这与通过电话能够设定的密码或者通过接收机被处理的访问卡不同。

由于已知的合法用户暂时不能感应设备而否定对控制系统的必要访问。

变得可接受。与其他因素相比用户更倾向于考虑某些生物授权设备。例如，视觉扫描在接受能力的范围内被考虑，在接受能力的范围内指纹扫描被更多地考虑。在选择各种生物授权技术时生物授权设备的用户需要考虑对于目标团体的社交接受能力。

ICS 详细建议和指导

生物设备使会丢失或者被借的其他形式的授权成为有用的第二检测形式。与机遇标志的访问控制或者使用生物联合的生物授权或者机遇标志的雇员始终增加安全等级。可能的应用处于被环境控制且物理上安全的控制室内。

6.3.2 访问控制

落入到 NIST SP 800-53 访问控制(AC) 族内的安全控制提供仅仅由授权的用户、项目、进程或者其它系统提供用于声明系统资源的使用的政策和过程。该族定义用于管理信息系统用户的控制，包括建立、激活、修改、复查、失效和删除帐户。控制包括访问和加强事项，例如责任的分离、最低优先权、不必要的登录尝试、系统使用通知、事先登录通知、同时 session 控制，session 锁和 session 中断。也存在以下控制：其控制记录便携和远程设备的用户以及个人拥有的信息系统来访问信息系统和远程访问能力的用户以及无线技术的完成。

如果新的联邦个人识别码(PIV)被用做一个识别标志，访问控制系统应该符合 FIPS 201 和 NISI SP 800-73 并且雇用密码识别或者生物识别中的任一个。在基于标志的访问控制使用加密识别时，访问控制系统应该符合 NIST SP 800-78 的要求。在基于标志的访问控制使用生物识别时，访问控制系统应该符合 NIST SP 800-76 的要求。

访问控制技术是过滤和拦截技术，其被设计为授权被确定的设备或者系统之间的直接和可调节的信息流。以下章节揭示集中访问控制技术和与 ICS 的使用。

6.3.2.1 基于角色的访问控制(RBAC)

RBAC 是一项使用大数量的智能设备来降低复杂性和网络中安全管理的成本的技术。在 RBAC 这种，通过角色、的使用安全管理被简单化，并限制授权用户访问等级。RBAC 在组织中降低成本，因为雇员改变角色和责任比改变角色和责任内的责任更频繁，这是可被接受的。

ICS 详细建议和指导

RBAC 在降低维护个人设备访问等级和降低错误时被用于提供统一手段来管理访问 ICS 设备。RBAC 应该被用于限制 ICS 用户优先权来做仅仅被要求履行的每个人的工作(例如，配置基于最小优先权的方针的每个角色)。

6.3.2.2WEB 服务器

WEB 和互联网技术被添加到 ICS 产品的广范围种类中，其原始是它们会使信息更容易获取并使产品对用户更加友好和更加易于远程配置。然而，它们也会增加 cyber 风险和产生需要被记录地址的新安全弱点。

ICS 详细建议和指导

SCADA 和历史软件供应商典型地提供 web 服务器作为产品选择，因此控制室外的用户能够访问 ICS 信息。在很多情况下，软件组成部分例如 ActiveX 或者 Java applets 被安装或者下载到每个访问 web 服务器的客户端机器上。某些产品例如 PLC 和其它控制设备通过嵌入式 WEB、FTP、和 e-mail 服务器来获取，使它们更加易于远程配置并且许可它们在某种条件产生时生成 e-mail 通知和报告。更灵活地，使用 HTTPS 而不是用 HTTP，使用 SFTP 或者 SCP 而不是用 FTP，拦截回归 FTP 和 e-mail 流量等。

6.3.2.3 虚拟本地局域网络(VLAN)

VLAN 将物理网络区分为小型逻辑网络和简单网络设计从而来增加实施、改变管理性。VLAN 以太网交换机的配置来获取。每个 VLAN 包括与其它 VLAN 分离流量的单一广播区域。就像使用交换机来替换集线器来降低冲突，使用 VLAN 来

限制广播流量和许可逻辑子网络来扩大复合的物理定位。有两种 VLAN 的目录。静态，经常涉及到交换端口被分配给 VLAN 的端口，因此能够对于终端用户是显而易见的。

动态，终端设备与交换机协商 VLAN 特别或者确定基于 IP 或者硬件地址的 VLAN

尽管不止一个 IP 子网络会同时存在于 VLAN 上，但一般的推荐是子网络与 VLAN 为一对一关系。这项实践需要路由器或者加入到多个 VLAN 中的多层交换机的使用。很多路由器和防火墙支持标签框架，因此单个物理接口能够被用于在多个逻辑网络中使用。VLAN 不是以防火墙或者 IDS 被安装的方式而被典型地安装到地址主机或者网络弱点中。然而，在被正确地配置时，VLAN 也许可交换机加强安全措施和在以太网层中隔离流量。适当地将网络分层也能够缓和广播风暴的风险，广播风暴是由端口扫描或者蠕虫动作产生的。

交换机容易受到像 MAC 地址欺骗、表溢出和反生成树协议攻击，该协议依赖于设备和其自身的配置。VLAN 跳跃攻击，用于阻止框架的未授权端口受到攻击的能力已经使用交换机诈骗或者双倍胶囊框架示出。这些攻击不能被远程操作并且需要本地物理连接到交换机。例如 MAC 地址的多种特征的过滤、基于端口的授权使用 IEEE 802.1x、和特定供应商推荐的减轻攻击的做法，这取决与设备和执行。

ICS 详细建议和指导

VLAN 已经被有效地安装在 ICS 网络中，每个自动单元被分配给单独的 VLAN 来限定不必要的流量诈骗，并且许可同一 VLAN 上的网络设备扩大多个交换机[33]。

6.3.2.4 拨号调制解调器

ICS 系统具有严格的依赖性和可获得性要求。在存在故障和修复时，技术资源可能没有物理地处于控制室或者设施中。因此，ICS 经常使用调制解调器来使供应商、系统综合者或者控制工程师来维护系统拨号或者诊断、修复、配置和执行网络或者组成部分中的维护。当允许授权人员轻易访问时，如果拨号调制解调

器不安全，则它们也可以会被未授权用户秘密地进入。

拨号经常使用授予远程用户访问目标系统的权利(管理者或者根用户)的远程控制软件。这种软件一般具有应该被仔细检查和配置的安全选择。

ICS 详细建议和指导

在拨号调制解调器被安装在 ICS 中时考虑到使用回调系统。这确保了拨号者通过使调制解调器建立基于拨号者的信息和存在被授权的用户名单的 ICS 中的回调号码的工作连接。

确认错误密码已经被改变并且强度较高的密码处于每个调制解调器的位置上

物理地识别调制解调器用于控制室内操作者

如果确认了适当的日志则配置远程控制软件来使用唯一的用户名称和密码、高强度的授权和加密。由远程用户使用这种软件应该实时地频繁地被监控。

如果可行的话，在不用时断开调制解调器或者考虑通过设定一个给定时间的自动进程来断开调制解调器。应该指出的是，有些时候调制解调器的连通是运营商合法的运维服务的一部分。个人应该注意断开/移除调制解调器是需要重新签订合同的。

6.3.2.5 无线

ICS 内的无线使用是一项必须由组织确定的基于风险的选择。一般来说，wireless LANs 应该仅仅安装在健康、安全的环境中，并且很少涉及金融。NIST SP 800-48 and SP 800-97 提供关于无线网络安全的指导。

ICS 详细建议和指导

Wireless LANs

在安装之前，应该进行无线调查来确定天线定位和使无线网络的最小暴露的强度。调查应该考虑到以下事实：攻击者能够使用有效的直接天线，该天线在期待的标准区域内增加了 wireless LANs 的区域。法拉第笼和其他方法也被用于将指

定区域外的无线网络的暴露最小化。

无线用户的访问应该使用安全授权协议(例如，使用 TLS [EAP-TLS]的可扩展的授权协议[EAP])来利用 IEEE 802.1X 授权，上述安全授权协议是给用户和用户证书或者用户服务(RADIUS)服务器中的远程授权拨号。

用于无线工作设备的无线访问点和数据服务器应该被定位在一个被文档化和与 ICS 网络最小连接(如果可能则是单连接)的分离的网络上。

无线访问点应该被配置为具有唯一的服务设置识别器(SSID)，使 SSID 不能广播，并且在最小限度上过滤 MAC。

无线设备，如果被使用在 Microsoft Windows ICS 网络中，则应该被配置在一个 Microsoft Windows ICS 域名的分离组织单元中。

无线设备通信应该被加密和保存保护。加密不是一定要降低终端的操作情况。应该考虑加密 OSI 的第二层中而不是第三层来降低加密潜在因素。也应该考虑用于执行加密功能的硬件的使用。

对于网状网络来说，考虑在 OSI 的第二层中完成广播 key 对公共密钥的管理的使用。不对称加密应该被用于执行管理功能，并且对称加密应该被用于确保每个数据流和网络控制流量的安全。如果设备被用于无线移动则自适应路由协议应该被考虑。网络的集合时间应该尽可能地支持在失败或者能量损失情况下的快速网络修复。网状网络的使用能提供由路径选择容错和网络的提前故障转移。

无线区域网络

ISA10020 委员会制定标准、推荐的实践、技术报告和相关信息，该相关信息将会定义使用集中区域等级(例如，IEEE 802.15.4)在自动和控制环境中执行无线系统的过程。指导直接指向那些用于包括设计、执行、正在进行的维护、可伸缩性或者管理工业自动化和控制信息、以及用户的申请、系统综合者、从业人员和控制系统制造商和供应商的完成生命循环。

6.3.3 审计

审查是一项记录的独立的审核和检查，也是访问系统控制的适当性的动作，用于确认同意建立的政策和操作性过程，也用于推荐控制、政策或者过程中的必要的改变。落入到 NIST SP 800-53 审计 (AU)族中的安全控制提供用于产生审查记录、它们的内容、容量和保持需求的政策和过程。控制也提供安全防卫来反映例如审查失败或者审查日志能力已负荷。审查数据应该防止被修改并且被设计为具有无可替代的能力。

ICS 详细建议和指导

需要确认系统被有意图地执行。ICS 的定期审查应该被执行来证实以下事项：

系统证实测试中的安全控制(例如，制造接收测试和网站接收测试)仍然被安装并在产品系统中被正确操作。

不受安全影响的产品系统包括并提供自然信息和应该发生的弹性组成的范围。

改变项目的管理严格地按照审查程序和所有变化的许可。

每次定期审查的结果应该以规定的形式即预先定义的、适当的尺寸来显示安全执行和安全趋势。安全执行尺寸应该与安全执行趋势一起被发送到适当的参与者

传统地，IT 系统中的用于审查的最初基础已经被记录保存。在 ICS 环境中使用适当的工具需要从与 ICS、主要产品和设备的安全隐患相似的 IT 专业获取可扩展的知识。安装在 ICS 中的很多过程控制设备已经被安装多年，并且不具有提供本章节中阐述的审查记录的能力。因此，这些用于审查系统和网络活动的调制解调器工具的适应性依赖于 ICS 中组成部分的能力。

在 ICS 环境中管理网络的主要任务确认依赖性和可获取性来支持安全和有效操作。在相关产业中，合规性能够将复杂性添加到安全和授权管理中，注册和安装保存管理，所有能够增加安装和操作需求的功能被使用。在这种环境中的这些工具的价值能够通过重新证明所需的效果来估计，或者重置基于攻击、事故或者正在被考虑的错误。系统应该提供可依赖的、同步时间戳来支持审查工具。

监视传感器、日志、IDS、防病毒、打包管理、政策管理软件和其他安全措施应该在灵活的实时基础上被完成。第一线监控服务能够接受警钟、作出快速的初始决定并采取动作来改变适当的工具人员进行干扰。

系统检查工具应该与新的既存的 ICS 项目合作。这些检查工具是应该在被安装在操作 ICS 上之前被测试(例如，在类似的 ICS 上为下线)。这些工具提供证据和系统保存的完整性。此外，激活的日志管理工具可能标识进攻或者过程中的事件，并且提供定位和跟踪信息来帮助响应事件[33]。

应该存在用于跟踪用户的所有单一活动的方法，或者是人为的方式(例如，标示控制室)或者是自动的方式(例如，在程序和/或 OS 层中登录)。政策和过程被跟踪，日志如何存储(或者打印)，他们如何被保护，谁访问过日志以及他们如何/合适审查该日志应该记录。这些政策和过程应该随着 ICS 申请和平台进行变化。合法的系统典型地使用打印日志，打印日志通过管理、操作和安全性被审查。被 ICS 申请保存的日志可能被存储在各种定位中并且可能或者不可能被加密。

6.3.4 系统和交流保护

落入到 NIST SP 800-53 系统和交流保护(SC)族中的安全控制提供用于保护系统和数据交流组成部分的政策和过程。

6.3.4.1 加密

加密是数据(明文文本)秘密转换为一种隐藏数据的原始手段的方式从而防止数据被别人知道或者被使用。如果转换是相反的，则响应的相反过程被称之为解密，该解密是一种将存储的加密数据转换为原始状态的过程[74]。

ICS 详细建议和指导

在安装加密前，首先确定加密是否是用于特别 ICS 申请的适合解决途径，这是因为授权和保存通常是用于 ICS 申请的安全事项。其他秘密措施例如密码散列也应该被考虑。

由于加密、解密和认证每条信息所需的额外的时间和计算机资源，在 ICS 环境下的加密应用可能引起通讯延迟，对于 ICS，任何加密或任何其他安全技术的应用所导致的任何延迟都不应降低终端设备或系统的操作性能。为了降低加密延迟，应考虑在 OSI 层 2 加密，而不是在层 3。

另外，由于以下一条或多条原因，加密后的信息经常大于未加密的信息：

- ✧ 为了减少错误的额外的总和检验码
- ✧ 为了控制密码方式的协议
- ✧ 填充 (对于分组密码)
- ✧ 身份验证程序
- ✧ 其他所需的加密程序

密码方式还引起密钥管理问题. 声音安全策略需要定期的密钥改变。随着 ICS 的地理尺寸增大，这种程序变得更加困难, 大量的 SCADA 系统就是严酷的例子。因为网点访问可能会代价大而且缓慢，其在远程改变密钥的情况下是有用的。如果选择密码方式, 最有效的安全措施是使用通过 NIST/通信安全机构（CSE）加密模块验证程序（CMVP）[21] 认证的完全加密系统。在该程序中保持有一个标准，即保证大范围的专家仔细研究了加密程序的缺点，而不仅是被一个单独组织的几个工程师开发出来的。最低限度, 保证其具有如下特点:

- ✧ 用某种方法（例如计数器模式）来保证同样的信息每次不生成同样的值
- ✧ ICS 信息被保护起来，不受重复和伪造影响
- ✧ 密钥管理在密钥的整个生命周期中是安全的
- ✧ 该系统使用有效的随机数字生成器
- ✧ 整个系统已经被安全地实现

尽管如此，, 该技术只有在其是有效执行的信息安全策略所不可或缺的部分时才起作用。美国煤气协会 (AGA) 报告 12-1 [5]包括了这种安全策略的一个列子。当其应用于一个天然气 SCADA 系统，其需要策略有点能够适用于任何 ICS。

对于一个 ICS, 加密能够被开发成一个全面的、执行的安全策略的一部分。组织应当选择加密的保护基于风险评估、被保护的信息的认可的价值以及 ICS 操作限制。特别是, 一个加密的密钥应当足够长，从而通过分析来猜想或确定它需要更多努力、时间以及超过被保护财产的代价。

加密软件应当防止物理篡改和不受控制的电子连接。假设密码方式是适当的解决方法，如果被保护的单位数量大或者地理分散而导致改变密钥困难或昂贵，则组织应当选择具有远程密钥管理的加密保护[33]。

6.3.4.2 虚拟专用网络 (VPN)

加密通讯数据的一个方法是通过 VPN，VPN 是一个专用网络，其操作起来像是公共基础结构上的覆盖层，从而该专用网络能够在公共网络上运行。如今，最常见的实现 VPN 技术的类型是：

IPsec. IPsec 是一套由 IETF 定义的用来管理在公共网络层上的 IP 层的安全通信数据的标准。IPsec 包括在许多现在的操作系统中. 该标准的目的是保证不同厂商平台之间的互通性，然而，现实是多厂商实现互操作性的决心，取决于由终端用户组织进行的具体实施测试。IPsec 支持两种加密模式: 传输和安全加密链路。传输模式只加密每个数据包的数据部分（负载），留下未加密的报头。更加安全的安全加密链路模式给每一个数据包添加一个新的报头并且给原始的报头和负载加密。在接收端，IPsec-客户端设备解密每一个数据包。该协议一直在不断完善，以满足特定的要求，如扩展协议以解决个别用户身份验证和 NAT 设备的横向扩展。这些扩展通常是特定于供应商的，并可能导致主要是在主机与安全网关环境下的互操作性问题。 NIST SP800-77 对 IPsec VPN 提供了指导。

SSL. SSL 提供一种在两台机器之间加密每一个数据包内容的安全通道。该 IETF 对 SSL 版本 3 协议做了略微修改，并创造了一个叫做传输层安全（TLS）的新的协议。术语“SSL”和“TLS”经常可交换地使用, 并且文档一般使用 SSL 术语。SSL 最经常被认识为保护 HTTP 流量，该协议作为超文件传输安全协议(HTTPS)而执行. 但是，SSL 并不限于 HTTP 流量，其能够用来保护许多不同的用户层程序。基于 SSL 的 VPN 产品已获得接受，因为“无客户端的”VPN 产品市场。这些产品使用标准的 Web 浏览器作为客户端，其中有内置的 SSL 支持。“无客户端的”一词的意思是指在用户的系统上无需安装或配置第三方 VPN 客户端“软件。 NIST SP800-52 提供了 SSL 配置的指导。

SSH。 SSH 是一个命令接口和用于安全地进入远程计算机的协议。它广泛应用于网络管理员远程控制网络服务器和其它类型的服务器。最新版本，SSH2，是

IETF 推荐的一套标准。通常情况下，SSH 被开发为一个远程登录程序的安全的替代品。 SSH 是包含在大多数 UNIX 分类中，典型地是通过第三方数据包添加到其他平台。

ICS 特别建议和指导

VPN 是最常用在 ICS 的环境以提供从不受信任的网络至 ICS 控制网络的安全访问。不受信任的网络范围可以从互联网到企业局域网。若正确配置，则 VPN 可以极大地限制在控制系统电脑主机和控制器之间的访问和被访问，从而提高了安全性。通过消除中间网络的未经授权的非必要的流量，他们还可以潜在地提高控制网络的响应。用来保护控制系统的 VPN 设备应进行彻底的测试，来验证 VPN 技术与应用程序兼容，并且 VPN 设备的实施不会不可接受地影响网络流量特性[33]。