NSFOCUS

2013

工业控制系统及其安全性研究报告

执行摘要

随着工业信息化进程的快速推进，信息、网络以及物联网技术在智能电网、智能交通、工业生产系统等工业控制领域得到了广泛的应用，极大地提高了企业的综合效益。为实现系统间的协同和信息分享，工业控制系统也逐渐打破了以往的封闭性：采用标准、通用的通信协议及硬软件系统，甚至有些工业控制系统也能以某些方式连接到互联网等公共网络中。这使得工业控制系统也必将面临病毒、木马、黑客入侵、拒绝服务等传统的信息安全威胁，而且由于工业控制系统多被应用在电力、交通、石油化工、核工业等国家重要的行业中，其安全事故造成的社会影响和经济损失会更为严重。出于政治、军事、经济、信仰等诸多目的，敌对的国家、势力以及恐怖犯罪分子都可能把工业控制系统作为达成其目的的攻击目标。

工业控制系统脆弱的安全状况以及日益严重的攻击威胁，已经引起了国家的高度重视，甚至提升到‘国家安全战略’的高度，并在政策、标准、技术、方案等方面展开了积极应对。在明确重点领域工业控制系统信息安全管理要求的同时，国家主管部门在政策和科研层面上也在积极部署工业控制系统的安全保障工作。

近年来，以“伊朗布什尔核电站遭到‘震网病毒’攻击”为代表的一系列针对工业控制系统的信息安全事件表明：攻击者正普遍采用被称为高级持续性威胁（Advanced Persistent Threat，简称 APT）的新型攻击手段。攻击者不仅具有明确的攻击目标，而且在攻击时也多采用有组织的多攻击协同模式；显然，这种新型的攻击手段更难防御，对安全厂商及相关研究机构的安全服务能力提出了更高的挑战。但由于国内工业控制系统及其工作环境的相对封闭性，国内安全研究团队的研究对象多集中在互联网和传统的信息系统上。在工业控制系统安全方面自然不会有太多的研究成果和实践经验。另一方面，工业控制系统提供商则更关注工业控制系统的可用性和实时性，对系统的安全性也是很少涉及。

在这种背景下，我们及时成立了一个有多名资深技术专家所组成的研究团队来专门从事工业控制系统的安全研究。研究团队在初步了解工业控制系统知识的基础上，结合公司在安全攻防、协议安全性以及漏洞研究方面的技术优势，首先对‘工业控制系统所面临的安全威胁及对策’、‘工业控制系统的协议安全性’、‘工业控制系统相关的漏洞分析’等几个主题进行了较为深入的研究。

本技术报告内容即为研究团队的先期研究成果，期望报告的内容可以供工业控制系统的安全管理人员以及相关安全产品的规划及研发人员参考所用。帮助他们初步了解工业控制系

统及其存在的安全性问题，进而为后续开发适用于工业控制系统相关的安全产品及提供相应的安全解决方案奠定基础。

为便于读者阅读，下面对报告的内容组织逻辑进行简单介绍。

- 首先，对工业控制系统的基本概念和系统体系架构进行了概要介绍，并从多个角度探讨了工业控制系统与传统 IT 信息系统的差异性。这可以让不熟悉工业控制系统的读者能够对工业控制系统有一个初步了解，并有助于理解后续章节的内容。（第二章）
- 其次，从安全威胁、安全防护以及安全管理等多个角度讨论工业控制系统所面临的安全问题及安全威胁，并与传统 IT 信息系统所面临的安全问题与威胁做了较为详细的差异化对比分析。并重点选择具有较大差异性的工业控制系统专有通信协议的安全性、专有的安全漏洞情况进行详细地分析研究。所得到的研究成果有助于读者更深入地了解当前工业控制系统所面临的安全威胁。（第三章）
- 再次，为便于读者对工业控制系统所面临的安全威胁有一个直观的认识；我们还虚构了两个攻击案例，来描述从不同攻击途径对工业控制系统进行入侵攻击的过程（第四章）。
- 最后，在上述研究的基础上，对当前工业控制系统所面临的安全威胁及问题进行分析总结，并提出了针对性的安全建议（第五章）

目录

一. 前言 1

1.1 研究背景及意义 1
1.2 研究目标及内容 4

二. 工业控制系统概述 6

2.1 工业控制系统的体系架构 6
2.2 工业控制系统与传统 IT 信息系统的对比 11

三. 工业控制系统的安全性分析 13

3.1 工业控制系统与传统信息系统安全的对比分析 13
3.2 工业控制系统协议的安全性 17
3.2.1 工业控制系统协议相关的安全问题 23
3.2.2 针对工业控制系统协议的异常行为分类 33
3.2.3 工业控制系统协议的安全总结 36
3.3 工业控制系统漏洞的统计分析 37
3.3.1 按发布时间分布情况分析 37
3.3.2 按威胁类型分布情况分析 37
3.3.3 按厂商分布情况分析 39
3.3.4 按厂商所属地区情况分析 40
3.3.5 按受影响对象属性分类情况分析 41
3.3.6 按漏洞的攻击途径分类情况分析 42

四. 工业控制系统的攻击场景研究 44

4.1 案例 1：攻击者利用现场无线网络干扰生产的攻击场景 44
4.2 案例 2：攻击者利用办公网窃取机密生产资料的攻击场景 46

五. 工业控制系统的一些安全建议 50

5.1 工业控制系统面临的安全问题分析 50
5.2 工业控制系统的安全建议 51

六. 结束语 57

附录　缩略语中英文对照 58

参考文献 59

作者信息 62

表格索引

表格 1 工业控制系统与传统 IT 信息系统的差异化对比 13
表格 2 工业控制系统与传统 IT 系统的安全性对比 15
表格 3 与 MODBUS 协议相关的几个典型安全问题 25
表格 4 MODBUS 协议典型异常行为 25
表格 5 与 PROFIBUS 协议相关的几个典型安全问题 26
表格 6 针对 PROFIBUS 的若干可能攻击场景 26
表格 7 与 DNP3 协议相关的几个典型安全问题 27
表格 8 针对 DNP3 协议的安全建议 27
表格 9 DNP3 协议典型异常行为 28
表格 10 针对 DNP3 协议的典型攻击场景 29
表格 11 与 ICCP 协议相关的几个典型安全问题 29
表格 12 针对 ICCP 协议的安全建议 30
表格 13 ICCP 协议典型异常行为 31
表格 14 ICCP 协议典型攻击场景 31
表格 15 针对 MODBUS 协议的异常行为分类 34
表格 16 针对 DNP3 协议的异常行为分类 35
表格 17 安全测试、检查的替代手段（建议） 55

插图索引

图 1.1 ICS-CERT 统计工业控制系统安全事件 2
图 2.1 工业控制系统（ICS）部署图 7
图 2.2 SIMATIC S7 控制器 8
图 2.3 SCADA 的人机界面 10
图 3.1 考虑工业控制系统安全与传统 IT 信息系统安全时的原则性区别 14
图 3.2 工业控制系统市场分布情况 17
图 3.3 MODBUS 协议栈 20
图 3.4 FMS、DP 和 PA 21
图 3.5 Idle Scan 32
图 3.6 针对 6 种安全属性违反情况的图示 34
图 3.7 公开漏洞数量的年度统计分析图 37
图 3.8 公开漏洞按威胁类型分布的统计分析 39
图 3.9 公开漏洞所涉及的主要工业控制系统厂商 40
图 3.10 相关漏洞涉及的 ICS 厂商所属地区分析 41
图 3.11 漏洞所涉及对象按软硬件形态的分类分析 42
图 3.12 漏洞按攻击途径的分类分析 43
图 3.13 远程漏洞的主要分类 43
图 4.1 案例 1：攻击者利用现场无线网络干扰工厂生产的攻击场景 45
图 4.2 案例 2：攻击者利用办公网络窃取机密生产资料的攻击场景 48
图 5.1 绿盟科技应用安全开发生命周期（NSFocus ADSL） 52
图 5.2 基于六元组的异常检测模型 53

一. 前言

1.1 研究背景及意义

随着工业化与信息化进程的不断交叉融合，越来越多的信息技术应用到了工业领域。目前，工业控制系统已广泛应用于电力、水力、石化、医药、食品制造、交通运输、航空航天等工业领域，其中，超过 80%的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业。工业控制系统已经成为国家关键基础设施的重要组成部分，工业控制系统的安全关系到国家的战略安全。

与此同时，由于工业控制系统广泛采用通用软硬件和网络设施，以及与企业管理信息系统的集成，导致工业控制系统越来越开放，并且与企业内网，甚至是与互联网产生了数据交换。也就是说以前工业控制系统在物理环境上的相对封闭性以及工业控制系统软、硬件的专用性将会被打破，通过互联网或企业内网将有可能获取相关工业控制系统较为详细的信息，再加上运营工业控制系统的企业安全意识普遍较差，这样就给敌对政府、恐怖组织、商业间谍、内部不法人员、外部非法入侵者等创造了可乘之机。尤其是 2010 年伊朗布什尔核电站遭到“震网病毒”（Stuxnet）攻击后，一系列工业控制系统安全事件被陆续曝光，并呈现飞速增长趋势（如图 1.1 所示）[CJ]。在这些安全事件中，攻击者普遍采用被称为高级持续性威胁

Stuxnet是一种计算机蠕虫病毒，这种蠕虫病毒可以在连接互联网的电脑中传播扩散，同时感染移动存储设备，包括U盘、移动硬盘，甚至带有USB装置的手机、相机等。一旦通过存储设备进入内部计算机，就会在内网中快速传播，直到侵入安装了西门子WinCC/PCS 7 SCADA控制软件的主机，展开破坏性攻击。

赛门铁克公司的研究表明，在感染初期主要受影响的国家主要包括伊朗、印度尼西亚和印度[Symantec]。赛门铁克安全响应中心高级总监凯文霍声称，多数受感染的系统在伊朗（约60％）[Robert]。它可能是专门针对伊朗的“高价值基础设施”而设计的，例如布什尔核电厂或纳坦兹的核设施。据ISIS（Institute for Science and International Security）研究所估计，纳坦兹因此而发生故障的离心机可能多达1000台，占总数的10％。

Stuxnet 利用了四个 Windows 系统未公开的零日漏洞 [Microsoft]，并使用两个盗取的数字证书对软件进行数字签名。部分专家认为，在恶意软件的历史上，研发 Stuxnet 可能是投入规模最大的一次。它的许多功能都需要完整的项目团队实现，并且要对工业生产过程有深入的了解[Gregg]。赛门铁克估计，Stuxnet 开发团队至少包括五至三十个人，并且需要 6 个月的准备时间[Halliday]。多家新闻和研究机构认为，它可能是以色列或美国研制，以遏制伊朗核计划的一次尝试[Beaumont] [Reals]。[BWLZ]

（Advanced Persistent Threat，简称 APT）[BWLZ]的新型攻击手段，攻击者不仅具有明确的攻击目标，而且在攻击时也多采用有组织的多攻击协同模式。为达成 APT 攻击需要长时间的集中高端人才和技术，需要具备无孔不入的情报收集能力，往往掌握最新的 0-day 漏洞，拥有能够规避当时检测工具的传播和控制程序，以及利用所掌握资源快速展开连锁行动的组织力和行动力[BWLZ]。显然这样的攻击不是能够依靠单一技术实现防范和检测的，需要多层面安全措施的综合防御。显然，这对安全厂商及相关研究机构的安全服务能力提出了更高的挑战。

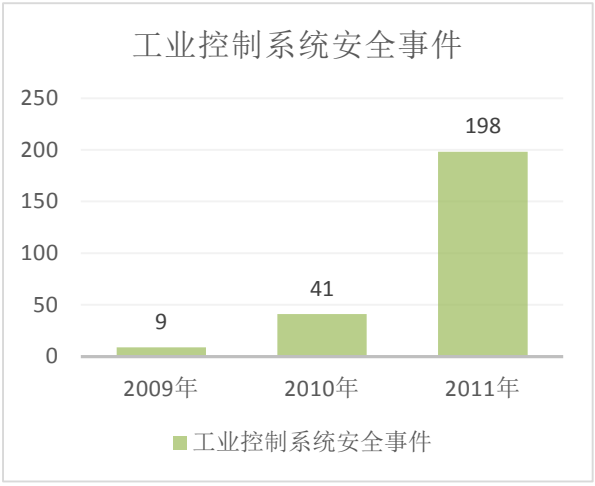

图 1.1　ICS-CERT 统计工业控制系统安全事件

备注：根据 ICS-CERT（US-CERT 下属的专门负责工业控制系统的应急响应小组）的统计，2011 年度共上报工业控制系统相关 ICS 事件 198 起，较 2009 和 2010 年均有较大上升（2009 和 2010 年分别为 9 起和 41 起），其安全事件集中于能源、水利、化工、政府机构以及核设施等领域，其中能源行业的安全事件在三年间共 52 起，占安全事件总数的 21%。

虽然针对 ICS 的安全事件与互联网上的攻击事件相比，数量少得多，但由于 ICS 对于国计民生的重要性，每一次事件都会带来巨大的影响和危害。

工业控制系统的重要性、脆弱的安全状况以及日益严重的攻击威胁，已引起了世界各国的高度重视，并在政策、标准、技术、方案等方面展开了积极应对。

从全球范围来看，信息技术较为发达的美国在工业控制系统安全保障领域走在世界的前列，美国作为信息化和工业自动化最发达的国家，拥有信息技术和工业自动化技术的主导权和话语权，在工业控制系统的信息安全管理体制、技术体系、以及相关资金投入上平都居世界领先水平。美国政府早在 2002 年起重视工业控制系统信息安全问题，十年来在工控安全领域进行了大量的工作，已经形成了完整的工控系统信息安全管理体制和技术体系[LHC]。

在工业控制系统信息安全研究方面，以石油化工、电力等能源行业为重点；在管理体制、技术体系和标准法规方面，美国国土安全部、能源部、国家实验室共同推动了美国工业控制系统信息安全工作的开展。

在工业控制系统管理体制方面，美国主要由国土安全部（DHS）和能源部（DOE）牵头，分别在工业控制系统信息安全领域制定专门的专项计划，开展工业控制系统信息安全工作。在美国能源部和国土安全部等部门支持下，爱达荷国家实验室 INL 于 2003 年开始建设，并在 2005 年正式投入运行了关键基础设施测试靶场（CITR），其中就包括了 SCADA/控制系统测试床和电力网测试床。这为工业控制系统安全保障工作的顺利开展奠定了良好的基础。美国国土安全部的国家网际安全处（NCSD）制订了控制系统安全计划（CSSP），其目标是消除所有关键基础设施和重要资源行业领域的工业控制系统安全风险；美国能源部电力调度与能源可靠性办公室（DOE-OE）制订了国家 SCADA 测试床计划（NSTB），该测试床提供各种工控系统的真实测试环境，帮助工业界和政府评估工业控制系统的脆弱性和测试工业控制系统软硬件的安全性[NSTB]。

在工业控制系统技术研究方面，美国建立了依托模拟仿真平台、综合采用现场检查测评与实验室测评相结合的测评方法。以模拟仿真平台为基础的验证服务和自主可控测评服务已成为当前工业控制系统信息安全的一种必然趋势。美国国土安全部下属的工业控制系统应急响应小组（ICS-CERT）同 US-CERT 协作，以工业控制系统安全为关注点，开展相关技术工作，包括响应和分析控制系统相关事故、执行漏洞和恶意代码分析、为事故响应和取证分析提供现场支持、以可行动情报形式提供态势感知、协调漏洞、防范措施的可靠披露、通过信息产品和告警共享和协调漏洞信息和威胁分析。

在在工业控制系统标准法规方面，美国形成了从国家法规标准到行业化标准规范的一整套标准规范。国家相关法规战略包括国土安全总统令 HSPD-7、《联邦信息安全管理法》（FISMA）、国家基础设施保护计划（NIPP）等。此外，美国国家标准与技术研究所（NIST）发布了一系列指南，包括《工业控制系统安全指南》（NIST SP 800-82）[NIST-1]、《联邦信息系统和组织的安全控制推荐》（NIST SP 800-53）等[NIST-2]。

而我国正处于工业化和信息化深度融合阶段，这就对工业控制系统安全防护策略和技术提出了更高的要求。但以前国内工业控制系统的安全问题由于种种原因并没有得到高度的重视，在这种背景下，国内信息安全产业和科研机构的核心工作，以前也主要集中在互联网环境下的安全问题，对工业控制系统领域的安全同样关注不够。

自从“震网”病毒事件爆发以及美国发布“国家网络空间安全战略”政策之后，工业控制系统安全才引起国家的高度重视，并把工业控制系统的安全提到了国家安全战略的地步。工业和信息化部发布了《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451号），强调加强工业信息安全的重要性、紧迫性，并明确了重点领域工业控制系统信息安全的管理要求[GXB451]。随后，国务院又发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号），意见要求建立国家信息安全保障体系，提升网络与信息安全保障水平，确保重点领域信息安全，并且明确提出要“保障工业控制系统安全”。同时，国家发展和改革委等部门也开始从政策和科研层面上积极部署工业控制系统的安全保障工作，研究和制定相关规范及要求。在有利政策、用户需求及工业控制系统安全事件的驱动下，国内安全界对工业控制安全方面的研究工作也已开始展开，并已有部分研究文档问世[BWLZ]、[LHC]、[XB]、[CJ]、[ZFG]、[HYX]、[ZS]、[TW]、[ZSP]、[GB26333]。

显然，基于工业控制系统安全的高度战略意义以及国内工业控制界与信息安全界对工业控制领域安全技术研究不足的现实，及时开展工业控制系统的安全问题分析，并结合公司在安全攻防及漏洞挖掘方面的技术优势，重点开展工业控制系统的协议安全性分析、相关漏洞的分析以及攻击场景的分析研究具有重要的现实意义。为公司后面提供具备对工业控制系统安全防护能力的行业版安全产品与有效的解决方案奠定基础。

1.2 研究目标及内容

本报告是一篇关于工业控制系统基本知识及其安全性分析的综述性技术报告。期望报告的内容可以供工业控制系统的安全管理人员以及相关安全产品的规划及研发人员参考所用。

为方便读者的阅读，下面对报告的内容组织逻辑进行简单介绍。

- 首先，我们对工业控制系统的基本概念和系统体系架构进行了概要介绍，并从多个角度探讨了工业控制系统与传统 IT 信息系统的差异性。这可以让不熟悉工业控制系统的读者能够对工业控制系统有一个初步了解，并有助于理解后续章节的内容。（第二章）
- 其次，我们从安全威胁、安全防护以及安全管理等多个角度讨论工业控制系统所面临的安全问题及安全威胁，并与传统 IT 信息系统所面临的安全问题与威胁做了较为详细的差异化对比分析。并重点选择具有较大差异性的工业控制系统专有通信协议

的安全性、专有的安全漏洞情况进行详细地分析研究。所得到的研究成果有助于读者更深入地了解当前工业控制系统所面临的安全威胁。（第三章）

- 再次，为便于读者对工业控制系统所面临的安全威胁有一个直观的认识；我们还虚构了两个攻击案例，来描述从不同攻击途径对工业控制系统进行入侵攻击的过程（第四章）。
- 最后，在上述研究的基础上，对当前工业控制系统所面临的安全威胁及问题进行分析总结，并提出了针对性的安全建议（第五章）。

二. 工业控制系统概述

工业控制系统（ICS-Industrial control system）（也称工业自动化与控制系统）是由计算机设备与工业过程控制部件组成的自动控制系统，工业控制系统被广泛的应用于在电力、水处理、石油与天然气、楼宇自动化、化工、交通运输、制造业等行业，在震网病毒爆发后，工业控制系统作为国家关键基础设施（CIP）的重要组成部分逐渐成为了国家空间安全和信息安全的关注热点。国际自动化协会（ISA）与 IEC/TC65/WG 整合后发布 IEC 62443 《工业过程测量、控制和自动化 网络与系统信息安全》对工业控制系统给出了定义，即：“工业控制系统包括了制造和加工厂站和设施、建筑环境控制系统、地理位置上具有分散操作性质的公共事业设施（如电力、天然气）、石油生产以及管线等进行自动化或远程控制的系统.”

如图 2.1 所示，通常情况下工业控制系统的子系统或功能组件包括但不限于：

- 数据采集与监控系统（SCADA）、分布式过程控制系统（DCS）、可编程逻辑控制器（PLC）、远程测控单元（RTU）、网络电子传感/监视/控制/诊断系统等
- 相关信息系统，如图形化界面、过程历史库、制造执行系统（MES）以及厂站信息管理系统

2.1 工业控制系统的体系架构

工业控制系统通过工业控制网络结合计算机技术实现了计算机系统向工业自动化控制领域的延伸；作为一系列组成元素（组件）的总称，工业控制系统这一称呼涵盖了可对工业过程安全性、可靠性操作产生影响的一系列、硬件和软件。在计算机技术、工业控制与自动化技术、微电子技术共同的演进和融合的前提下，很多组件如 DCS 和 SCADA、PLC 和 RTU 在功能和使用场景上的界限已经逐渐模糊，为了能够清晰的理解其功能特点和安全属性，将着重介绍一些相对关键的工业控制组件：

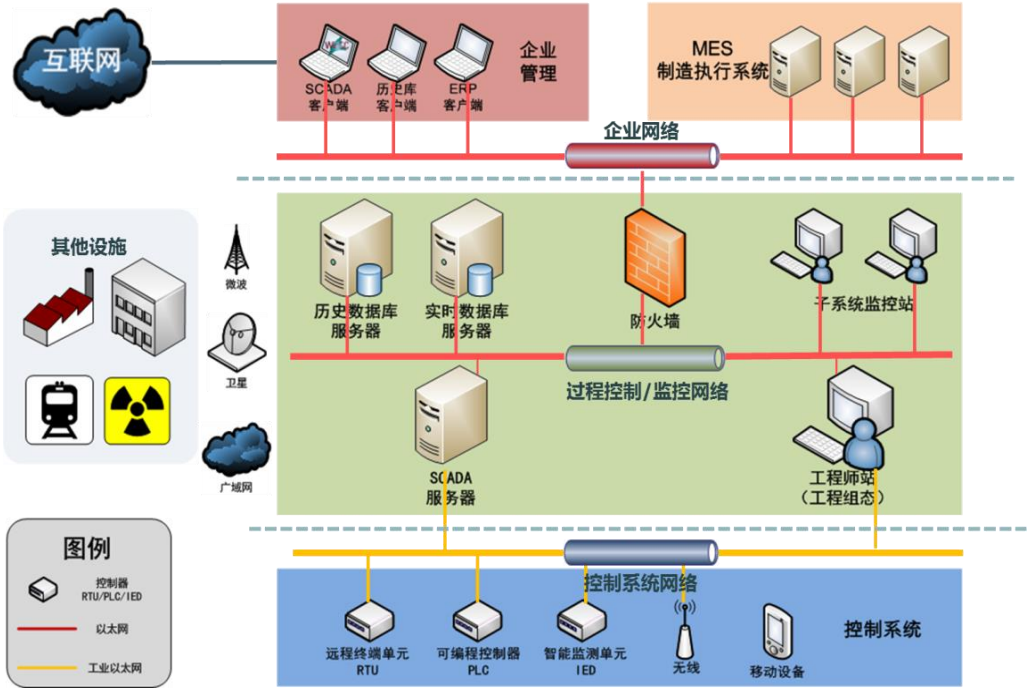

图 2.1 工业控制系统（ICS）部署图

- **控制器**：作为直接控制设备、获取设备状况的控制系统，控制器随着嵌入式计算技术的卓越性能和软逻辑控制器在工业控制领域的成熟应用。典型的控制器如 PLC（可编程逻辑控制器）、PAC（可编程自动化控制器）以及 RTU（远程控制单元）等，早期的生产过程自动化领域里，PLC 的应用较为广泛，利用远程 I/O 卡件与控制室实现通过单根电缆的通讯信息交换。80 年代初期，一些相对生产规模小一些的厂家利用它们在数据采集转换及通讯方面的优势，以 RTU 等组件结合 PLC 构建了当前的 SCADA 系统。以当前最为常见的控制器 PLC 和 RTU 为例：

  可编程逻辑控制器（Programmable Logic Controller ，简称 **PLC**）实质是一种专用于工业控制的计算机，其硬件结构基本上与微型计算机相同，具有电源、CPU、存储器等计算机组件（图 2.2 为西门子 SIMATIC S7 控制器的外型示意图）。PLC 由于其具备价格便宜、编程简单等特点，作为 SCADA 和 DCS 系统中的现场控制组件，被应用于几乎所有的工业过程控制领域。针对 PLC 的进行编程控制和诊断通常通过下位机软件（即常见的 WINCC、Unity Pro）来实现，下位机软件存在的安全漏洞将直接导致 PLC 产生安全风险，特定的可编程逻辑控制器（如西门子 6ES7-417 、6ES7-315-2）也面临诸如拒绝服务等风险 。

图 2.2 SIMATIC S7 控制器

远程终端单元（RTU——Remote Terminal Unit 的缩写），有的行业也称之为远程测控终端，是 SCADA 系统的基本组成单元，负责对现场信号、工业设备的监测和控制。和 PLC 相比，RTU 具有通讯距离较长、通讯接口多样、存储容量大、适应更加恶劣的温湿度环境等特点，通过经济、性能、环境等角度考虑，部分行业的客户选择利用 RTU 来进行数据采集、处理和传输（网络通信），以智能化变电站举例，为了实现电网调度自动化的现代化管理，RTU 作为远动终端部署在变电站侧，负责采集所在变电站电力运行状态的模拟量和状态量，监视并向调度中心传送这些模拟量和状态量，执行调度中心发往所在变电站的控制和调度命令。由于 RTU 更多吸收了通信技术的发展，其应用更多侧重在广域环境，如石油天然气长输管线和油气田领域。应该说 PLC 是为了传统工厂基础自动化的发展需求而出设计的，RTU 在分布式和远程能力上对 PLC 进行补充，更适用当前 ICS 系统的特点。

- **组态编程软件**：针对 PLC 进行组态编程以实现基本自动化功能的软件，又被称之为下位机软件（下位机的称呼是相对于上位机提出的，从概念上看，下位机处于被控制者和被服务者的位置，而上位机和下位机如何通讯，一般取决于下位机，可能采用 TCP/IP 通讯或者采用更为私有的通讯协议实现。）典型的下位机软件如 SIMATIC Step7，通过特定接口和线缆，如 RS232C 与 PLC 的 MPI 接口相连，可对 PLC 代码块进行配置/编译，替换软件核心文件即可实现 PLC 感染和隐藏（Rootkit 功能），从而改变工业生产控制系统的行为，如通过改变某些工艺参数，如混合工艺的原材料配比，最终改变工艺过程的温度、压力、流量、液位和时间值以及机械过程中马达的运动速度等。
- **数据采集与监视控制系统**（Supervisory Control And Data Acquisition ，**简写为 SCADA**），国内也称之为组态监控软件，通过 SCADA 可以实现广域环境的生产过

程和事物管理，其大部分控制工作依赖控制器等现场设备实现（如 PLC/RTU）。因此，SCADA 也被认为并不是完整的控制系统，而是位于控制设备之上侧重上位功能的应用软件。通常 SCADA 系统分为两个层面，即客户/服务器体系结构。服务器与硬件设备通信，进行数据处理何运算。而客户用于人机交互，如用文字、动画显示现场的状态，并可以对现场的开关、阀门进行操作。而上位机（HMI）与下位机（控制设备）结合的 SCADA 系统，作为操作员平台和中央监控系统，通过分布式的数据采集和控制系统，集中了 PLC 在现场测控和 DCS 组网通讯的优势，已经在各个领域中被广泛应用，如电力调度用于掌握运行状态和故障诊断。

- **人机界面**（Human Machine Interface，简称 HMI），SCADA 系统的核心组件，通过良好的人机界面反映全面的过程信息，从而达到实时的动态数据处理（如图 2.3 所示）。基于嵌入式技术的人机交互设备一般会包括绘图软件，可以让系统维护者修改系统在 HMI 中的呈现方式，并且通过组态和编程对生产过程与设备调度进行设计与配置，利用大量的通信接口和开放的程序结构连接到自动化环境，从而实现了对现场设备的监视与控制。典型的解决方案如西门子的 WinCC（包括 WINCC Flexible），均可实现对 HMI 设备、PLC 等控制器的组态功能。在震网病毒的案例里，攻击者即通过 WinCCConnect 账户的默认密码连接 Siemens Simatic Wincc，通过硬编码的 SQL 语句读取数据库数据，一方面查找感染系统的工业控制软件如 Step7、WinCC 的安装状态信息，从而精确定位工业网络目标，避免不必要的主机感染和暴露；一方面尝试从数据库中读取与工业控制网络设计相关的敏感信息，从而为后续可能发起的下一波攻击提供信息资源。

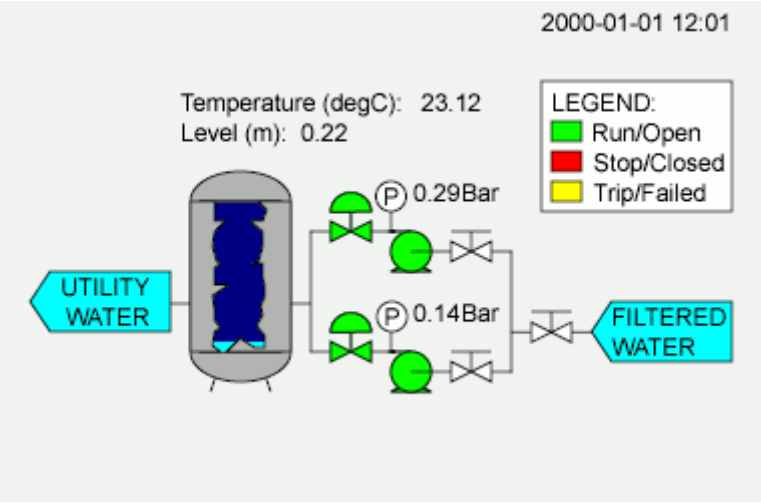

图 2.3 SCADA 的人机界面

- **分布式过程控制系统**（Distributed Control Systems，简称 DCS）：通常被应用于工业过程控制，如发电、炼油厂、污水处理、化工等，也被称为集散控制系统。DCS 系统通过调用 PLC 为分布式业务提供基本的操作控制（PLC 的功能实际相当于一个小型的计算机系统，通过配置该 PLC，可以向控制器中写入新的控制逻辑，从而完成不同的功能，最终实现工业设备的具体操作与工艺控制），适用于测控点数多、精度高且反应速度快的工业现场；和 SCADA 相比，DCS 和 PLC 通信通常使用更加高速可靠的局域网技术（工业以太网），而 SCADA 则通常侧重于远程长距离的监测和控制（如电力调度的远动控制）。目前从发展趋势上来看，SCADA 和 DCS，以及 PLC/RTU 在功能上进行着不断的相互渗透和整合，同时也分别由于其独特、不可取代的特性，共同作为工业控制系统在工业企业里同时扮演着不可替代的角色，如 SCADA 作为调度管理手段侧重于生产管理的上位监控，DCS 实现工业过程的复杂控制，而 PLC 在工业作业现场环境内实现单机及简单控制。

通过上面对工业控制系统体系架构和核心系统组件的介绍可知，工业控制系统是由工业控制组件通过通信网络互联的一个分布式控制系统，因此考虑工业控制系统安全时，除了重视其核心系统组件的安全属性外，也要了解并重视其网络环境的安全相关属性的影响，如网络开放程度、网络结构、协议安全性等。据此我们对工业控制系统所涉及到的相关网络也作了初步的调研，当前的工业控制系统在具体部署时通常要涉及如下的几个网络部分（如图 2.1 所示）：

- **企业资源网络：**

  主要涉及企业应用，如 ERP、CRM 和 OA 等与企业运营息息相关的系统，根据风险敏感程度和企业应用场景的不同，工业企业可能存在于外部的互联网通信边界，而一旦存在互联网通信，通常也具有较完备的典型安全边界防护措施，如防火墙等。一般情况下，工业控制系统的监控采集数据信息需要被企业内部的系统和人员访问，该访问过程需要企业资源网作为工业企业信息化应用体系最上层直达工业控制层，甚至现场总线层，其中由于实时性和协议私有性的局限，可能其访问过程未能实现基本的访问控制。除了典型的企业应用资源，部分工业企业还存在 MES（制造执行系统，）作为中间层负责生产制造执行过程的管理，是工业企业的核心系统。

- **过程控制和监控网络（简称为控制网络）：**

SCADA 服务器、历史数据库、实时数据库以及人机界面等关键工业控制组件主要部署在控制网络内部，通过 SCADA 服务器（MTU）与远程终端单元（RTU）组成远程传输链路，现场总线的控制和采集设备（PLC 或者 RTU），依照需求传送设备状态至监控系统。数据通常具有特定格式，操作员通过人机界面（HMI）了解系统状态，人机界面（HMI）以图形化显示的方式对实际系统的运行状态进行模拟，操作员通过待控制系统的示意图决定是否要调整 RTU（或 PLC）的控制。数据通常也会传送到历史数据服务器（一般是商用关系数据库），供趋势追踪和分析。

- **控制系统网络：**

作为自动化系统与现场设别相连的唯一网络，控制系统网络利用总线技术(如 PROFIBUS 等)将传感器/计数器等设备与 PLC 以及其他控制器相连，PLC 或者 RTU 可以自行处理一些简单的逻辑程序，不需要主系统的介入即能完成现场的大部分控制功能和数据采集功能，如控制流量和温度或者读取传感器数据，使得信息处理工作实现了现场化。控制系统网络由于通常处于作业现场，因此环境复杂，部分控制系统网络采用各种接入技术作为现有网络的延伸，如无线和微波，这也将引入一定的安全风险。

从厂商解决方案的角度，西门子（Siemens）、通用电气（GE）、施耐德电气（Schneider-Electric.）均针对各工业领域，如制造业、石油天然气、石化提出了成熟的解决方案，如西门子 SIMATIC PCS 7/WINCC/STEP 7/S7，通用电气 CIMPLICITY/iFIX/ PACSystems 等，而国内的亚控（Kingview）、三维力控在国内也就占有较高的市场份额。当前的工业控制系统由于开放性的需要，已经逐渐从专用转向为通用，厂商之间通过 ODBC、OLE 等标准接口，通过以太网、PROFIBUS 现场总线等开放网络，可以实现管理系统和控制系统的互连。

2.2 工业控制系统与传统 IT 信息系统的对比

随着工业信息化的快速发展，工业控制系统也在利用最新的计算机网络技术来提高系统间的集成、互联以及信息化管理水平。比如，逐步采用一些 PC 服务器、终端产品，操作系统和数据库等通用 IT 产品，逐步采用基于 TCP/IP 协议的工业以太环网和 OPC 通信协议，这将促使 TCP/IP 协议逐步成为工业控制系统的基础通信协议，而为保持工业控制系统的兼容性，专用的工业控制协议则将会逐步迁移到应用层。通用互联网技术的采用将为企业打破生产系

统的封闭性，实现管理与控制的一体化、提高企业信息化水平，实现生产、管理系统的高效集成奠定基础。但是通过上面章节关于工业控制系统的概述可知：工业控制系统与传统 IT 信息系统因其建设目标不同，使得它们在技术、管理与服务等很多方面依然有相当大的差异之处，一些典型的差异化见表格 1）。

表格 1 工业控制系统与传统 IT 信息系统的差异化对比

对比项	工业控制系统（ICS）	传统 IT 信息系统
建设目标	利用计算机、互联网、微电子以及电气等技术，使工厂的生产和制造过程更加自动化、效率化、精确化，并具有可控性及可视性。 强调的是工业自动化过程及相关设备的智能控制、监测与管理。	利用计算机、互联网技术实现数据处理与信息共享。
体系架构	ICS 系统主要由 PLC、RTU、DCS、SCADA 等工业控制设备及系统组成	有计算机系统通过互联网协议组成的计算机网络
操作系统	广泛使用嵌入式操作系统 VxWorks、uCLinux、WinCE 等，并有可能是根据需要进行功能裁减或定制。	通用操作系统（window、UNIX、linux 等），功能相对强大。
数据交换协议	专用通信协议或规约（OPC、Modbus、DNP3 等)直接使用或作为 TCP/IP 协议的应用层使用	TCP/IP 协议栈（应用层协议：HTTP、FTP、SMTP 等）
系统实时性	系统传输、处理信息的实时性要求高、不能停机和重启恢复。	系统的实时性要求不高，信息传输允许延迟，可以停机和重启恢复。
系统故障响应	不可预料的中断会造成经济损失或灾难，故障必须紧急响应处理	不可预料的中断可能会造成任务损失，系统故障的处理响应级别随 IT 系统要求而定
系统升级难度	专有系统兼容性差、软硬件升级较困难，一般很少进行系统升级，如需升级可能需要整个系统升级换代	采用通用系统、兼容性较好，软硬件升级较容易，且软件系统升级较频繁
与其他系统的连接关系	一般需要与互联网进行物理隔离	与互联网存在一定的连通性

三. 工业控制系统的安全性分析

3.1 工业控制系统与传统信息系统安全的对比分析

在传统的信息安全领域，通常将保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）称为安全的三种基本属性，简称 CIA。并且通常认为保密性的优先级最高，完整性次之，可用性最低。

在工业控制系统领域则有较大的不同，由**错误!未找到引用源。**的分析可知，工业控制系统强调的是工业自动化过程及相关设备的智能控制、监测与管理。它们在系统架构、设备操作系统、数据交换协议等方面与普通 IT 信息系统存在较大差异，而且更为关注系统的实时性与业务连续性。也就是说，工业控制系统对系统设备的可用性、实时性、可控性等特性要求很高，因此在考虑工业控制系统安全时要优先保证系统的可用性；其次，因各组件之间存在固有的关联，因此完整性次之；而对于数据保密性来说，则由于工控系统中传输的数据通常是控制命令和采集的原始数据，需要放在特定的背景下分析才有意义，而且多是实时数据，因此对保密性的要求最低，如图 3.1 所示[NIST-1]。这就是在考虑工业控制系统安全时与考虑传统 IT 信息系统安全时的原则性区别。

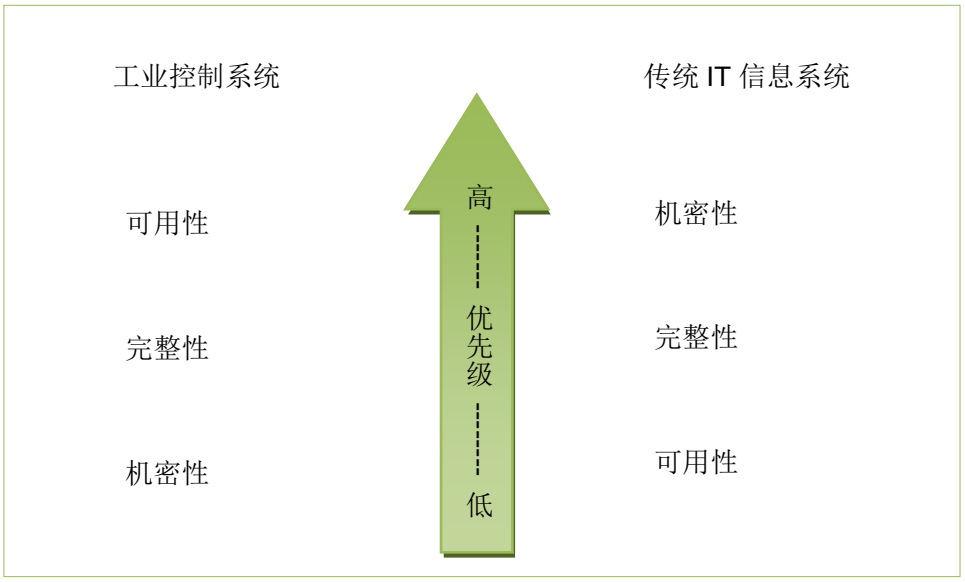

图 3.1　考虑工业控制系统安全与传统 IT 信息系统安全时的原则性区别

由于工业控制系统作为企业的核心生产运营系统，一般来说其工作环境具有严格的管理，外人很难进入，同时系统自身也多与企业的办公网络（普通 IT）系统之间存在一定的隔离措施，与互联网则一般处于物理隔离的状态，也就是说其环境相对封闭。在加上工业控制系统主要由 PLC、RTU、DCS、SCADA 等工业控制设备及系统组成，这些设备品种繁多，且其功能多基于不同于互联网通用操作系统的嵌入式操作系统（如 VxWorks、uCLinux、WinCE 等）开发，并采用专用的通信协议或规约（如 OPC、Modbus、DNP3 等）实现系统间通信。正是由于这些工业控制系统设备及通信规约的专有性以及系统的相对封闭性，使得一般的互联网黑客或黑客组织很难获得相应的工业控制系统攻防研究环境以及相关系统资料支持，从而通常黑客的攻防研究工作多集中在互联网或普通 IT 信息系统上，而很少关注工业控制系统，

自然相关的系统及通信规约的安全缺陷（或漏洞）也很少被发现。而同时工业控制系统提供商则在重点关注系统的可用性、实时性，对系统的安全问题、防护措施以及运维策略也缺乏系统的体系的考虑。但是随着 2010 年“震网”及后续一系列工控安全事件[CJ]的发生，表明出于某些国际组织、国家的政治、经济、军事等原因，工业控制系统已经面临这些组织所发起的新型高级可持续的攻击威胁。至此，工业控制系统的安全问题才被世界各国政府及企业组织所重视，开始展开这方面的研究工作。

上述这些原因，也使得工业控制系统与传统 IT 信息系统在所面临的安全威胁、安全问题及所需要考虑的安全防护措施等方面存在较大的不同——表格 2 从多个角度对这些差异进行了讨论分析。

表格 2 工业控制系统与传统 IT 系统的安全性对比

对比项		工业控制系统（ICS）	传统 IT 信息系统
安全威胁	威胁来源	● 以组织为主	● 个体 ● 群体 ● 组织
	攻击方法	● 攻击目的性强的高级持续性威胁（APT：StuxNet、Duqu 等） ● 采用有组织的多攻击协同模式	● 常用攻击方式：诸如拒绝服务、病毒、恶意代码、非授权实用、破坏数据安全三性（CIA）、假冒欺骗等 ● 近年来也有一些组织采用 APT 的攻击模式攻击一些重要信息系统
安全防护	系统安全	● 重点关注 ICS 系统及其设备专用操作系统的漏洞、配置缺陷等问题； ● 当前系统防护能力不足：系统补丁管理困难、安全机制升级困难，	● 关注通用操作系统的脆弱性、安全配置、病毒防护以及系统资源的非授权访问等。 ● 系统级防护能力较强（防病毒、补丁管理、配置核查、外设管控等系统级安全手段丰富）

	网络安全	● 需要重点关注专有通信协议及规约的安全性及其实时、安全的传输能力。 ● ICS 缺乏统一的数据通信协议标准，专有协议与规范种类繁多。 ● 专有通信协议、规约在设计时通常只强调通信的实时性及可用性，对安全性普遍考虑不足：比如缺少足够强度的认证、加密、授权等。 ● 通常需要与互联网进行物理隔离，	● 主要是关注 TCP/IP 协议簇的安全性传输、拒绝服务、应用层安全等，一般对数据传输的实时性要求不高。 ● 安全技术、产品、方案相对成熟，安全防护能力强 ● 一般不要求与互联网进行物理隔离
	数据安全	● 重点关注 ICS 设备状态、控制信息等在传输、处理及存储中的安全性	● 服务器中存储数据的安全存储及授权使用
安全管理	身份管理	● 系统用户的身份认证及授权管理相对简单 ● 部分控制设备硬件实现，难以进行密码周期性修改	● IT 用户的身份认证、授权机制比较成熟、完善； ● 用户身份管理系统软件实现，可方便地进行密码周期性修改
	补丁管理	ICS 系统补丁管理困难、漏洞难以及时处理 ● ICS 系统补丁兼容性差、发布周期长以及系统可用性与业务连续性的硬性要求，使得 ICS 系统管理员绝不会轻易安装非 ICS 设备制造商指定的升级补丁 ● 使用周期长、相对陈旧的系统，也可能因厂商不存在或厂商不再进行产品的安全升级支持，而造成系统漏洞无法及时打补丁	● 传统 IT 信息系统的漏洞和补丁管理系统或工具比较成熟，漏洞一般可以及时地得到处理。
	行为管理	● ICS 需要严格防止系统误操作与蓄意破坏； ● 但通常缺乏针对 ICS 的安全日志审计及配置变更管理。 ● 存在部分 ICS 系统不具备审计功能或者虽有日志审计功能但系统的性能要求决定了它不能开启审计功能	● 一般有比较完善的 IT 系统及网络行为审计机制
	应急响应	● 需要保障 ICS 系统业务连续性的应急响应计划，强调快速响应	● 应急响应计划可选

显然，工业控制系统及其安全性研究也可以算是信息安全研究的一个新领域，对此，我们将需要首先熟悉工业控制系统，其次重点研究 ICS 自身的脆弱性（漏洞）情况及系统间通信规约的安全性问题，并在此基础上基于模拟攻击场景进行攻防推演分析。只有在充分了解 ICS 的前提下，才能逐步完善系统的安全性保障措施。因此，本文后续章节的内容将重点是讨论工业控制系统的通信协议（规约）安全性研究、ICS 相关漏洞的整理分析以及部分典型攻击场景模拟分析。

3.2 工业控制系统协议的安全性

工业控制系统（ICS）广泛应用于电力、油气、市政、水利、铁路、化工、制造业等行业的数据采集与监视控制。针对 ICS 的安全问题进行研究，要求我们对 ICS 的网络操作具有基本的了解，而这种了解又要求我们对其使用的通信协议具有基本的分析和研究。

有很多特定的协议（下文将这些协议统称为工控协议）可用于 ICS，但是特定的行业通常仅使用其中的一种或几种特定的协议。ICS 系统发展之初，使用的协议基本上都是基于串行链路的现场（总线）协议。随着以太网技术的出现、发展和互联网技术的日益进步，早期基于串行链路的现场（总线）协议基本上都出现了基于以太网（或者互联网）的演化版本。

1. 协议的行业应用情况

目前，我国 ICS 的市场规模[GK]约为 100 亿元，但是由于各个行业对 ICS 的要求不同，因此发展也不完全相同。其中，在电力行业中，ICS 应用最为广泛，约占整个 ICS 市场的半壁江山，如图 3.2 所示。

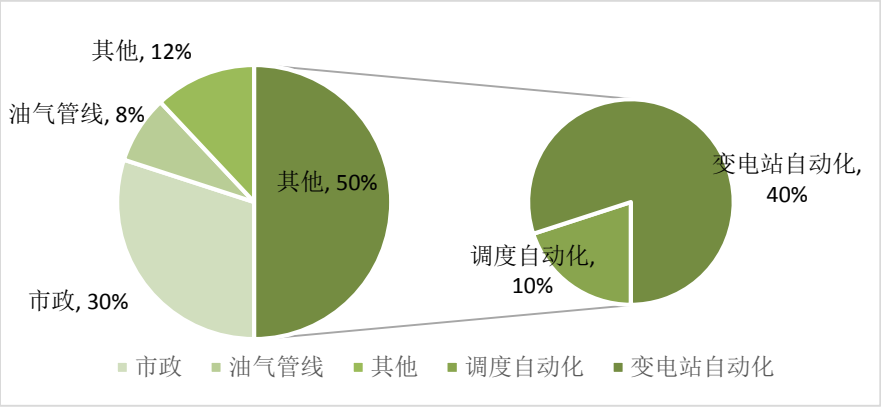

图 3.2 工业控制系统市场分布情况

电力系统中，变电站自动化约占到 ICS 市场的 40%，是 ICS 最大的应用领域，同时技术发展也最为成熟。目前，变电站的综合自动化已经在我国得到大规模应用。其中，以远程终

端单元、微机保护装置为核心，将变电所的控制、信号、测量、计费等回路纳入计算机系统，从而取代传统的控制保护屏，降低变电站的占地面积和设备投资，提高二次系统的可靠性。电力调度自动化约占到 ICS 市场的 10%，在提高电网运行的可靠性、安全性与经济效益等方面有着不可替代的作用。作为能量管理系统（EMS）的一个最主要的子系统，为 EMS 系统提供大量的实时数据，在减轻调度员的负担，实现电力调度自动化与现代化，提高调度的效率和水平等方面有重要的作用。

市政行业约占到 ICS 市场的 30%，包括：供水、供电、供暖、供气、水处理、交通等多个具体行业。这些行业进入门槛低，价格竞争激烈，利润水平低。目前，市政行业 ICS 整体市场增长缓慢，但是由于各行业的环保要求逐步提高，水处理领域的增长相对较快。油气管线领域约占 ICS 市场的 8%，市场集中度相对较高，但市场增长不稳定。该行业项目数量虽然不多，但是项目金额较大，客户购买力较强。其它行业约占 ICS 市场的 12%，包括水利、铁路、化工、制造业等多个具体行业。目前，这些行业在我国还属于 ICS 的新兴市场，相对来说虽然目前增长不快但有巨大的增长潜力。

通过对上述主要行业中使用的 ICS 系统及其采用的工控协议的广泛和深入的调研，几种典型的工控协议及其行业使用情况如下表 3-1 所示。

表格 3-1 工控协议在 ICS 中的使用情况

行业	细分	协议
电力	变电站自动化	Modbus、Profibus、DNP3、IEC 60870-5-101/104、ICCP（IEC 60870-6，TASE.2）、IEC 61850
	调度自动化	
油气	油气管线、油气井	Modbus、Profibus、DNP3
市政	供水、供电、供暖、供气、水处理、交通	
其他	水利、铁路、化工、制造业	

具体来说，ICS 进入电力行业较早，发展时间最长，采用的协议也最多，主要包括：Modbus[MBUS]、DNP3[DNP]、IEC 60870-5-101/104[IEC60870-5]、ICCP（即 IEC 60870-6 或者 TASE.2）[IEC60870-6]和 IEC 61850[IEC61850]等。其它行业的 ICS 发展相对滞后，使用情况比较类似且相对电力行业的 ICS 要简单很多，采用的协议主要是 Modbus、Profibus[PBUS]、DNP3 三种。

2. 典型协议简介

工控协议可分为使用串行链路通信的现场（总线）协议和使用以太网通信的以太网协议（包括 TCP/IP 协议之上的某些应用层协议）。

例如，基于串行链路的 MODBUS RTU、MODBUS ASCII、MODBUS PLUS 和基于以太网的 MODBUS TCP；基于串行链路的 PROFIBUS FMS、PROFIBUS DP、PROFIBUS PA 和基于以太网的 PROFINET CBA、PROFINET IO；基于串行链路的的 DNP3 和基于以太网的 DNP3/UDP、DNP/TCP；基于串行链路的 IEC 60870-5-101 和基于以太网的 IEC 60870-5-104（国际上，一般将 IEC 60870-5-104 看作 IEC 60870-5-101 的以太网演化版本，虽然两者在报文格式上存在巨大的差异，但是可用于完成相同的任务。目前，国内还有另一种直接在以太网上实现的 IEC 60870-5-101 协议，该协议使用 IEC 60870-5-101 的报文格式，但是使用以太网作为传输介质）。除了上述几种传统的通用协议，电力行业 ICS 广泛使用的协议还有 ICCP（IEC 60870-6，TASE.2）和 IEC 61850 等协议。

下面，我们对几个主要行业广泛使用的 6 种典型工控协议作一个简单的介绍。包括：Modbus、PROFIBUS、DNP3、IEC 60870-5-101/104、ICCP（即 IEC 60870-6 或者 TASE.2）和 IEC 61850。

a) MODBUS

1979 年，PLC 的发明者美国 Modicon 公司（现为法国施耐德电气公司的一个品牌）发明了全球第一个可真正用于工业控制的现场（总线）协议 MODBUS。随着工业的发展和互联网技术的日益进步，MODBUS 协议也不断得到更新和扩展。目前，出现了多种 MODBUS 协议变种，例如：使用串行链路的现场（总线）协议 MODBUS RTU、MODBUS ASCII、MODBUS PLUS，以及使用以太网的以太网协议 MODBUS TCP 等。MODBUS 标准定义了 OSI 模型第 1/2/7 层的协议，如图 3.3 所示。

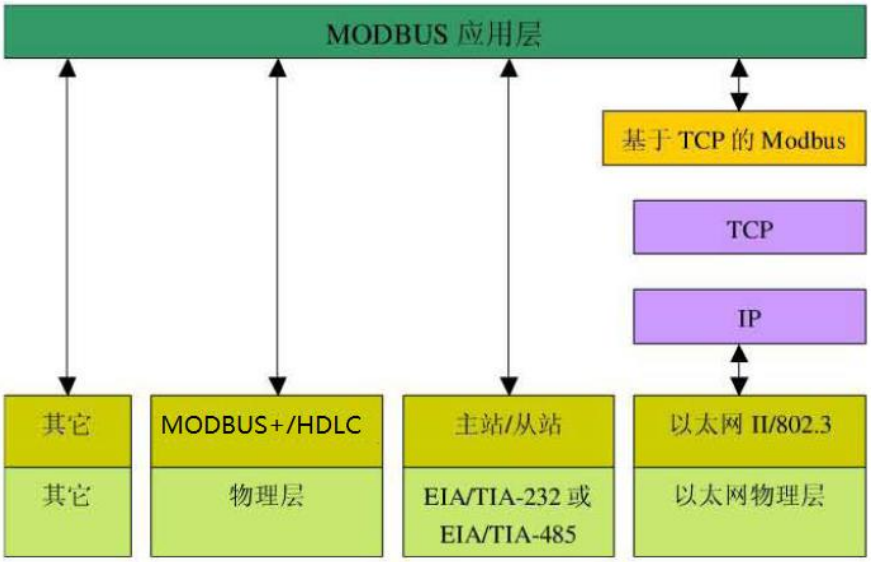

图 3. 3 MODBUS 协议栈

MODBUS 协议采用主-从结构，提供连接到不同类型总线或者网络的设备之间的客户机-服务器通信。客户机（主站）使用不同的功能码请求服务器（从站）执行不同的操作，服务器执行功能码定义的操作并向客户机发送响应，或者在操作中检测到差错时发送异常响应。

b) PROFIBUS

1987 年，德国联邦科技部集中西门子等十几家公司以及多个研究机构，按照 OSI 参考模型制订现场总线的德国国家标准 PROFIBUS。1991 年 4 月，PROFIBUS 在 DIN19245 中发表，并正式成为德国国家标准。开始时，PROFIBUS 中只有 PROFIBUS-FMS 协议；1993 年，引入了 PROFIBUS-DP 协议；1994 年，又引入了 PROFIBUS-PA 协议，从而使得 PROFIBUS 更加完善。而 PROFINET 是现场总线标准 PROFIBUS 在以太网上的新一代标准。

Profibus 以 OSI 作为参考模型，包括 PROFIBUS-FMS、PROFIBUS-DP 和 PROFIBUS-PA 三种协议。其中 PROFIBUS-FMS 协议最早出现，PROFIBUS-PA 协议出现最晚，而目前广为使用的是 PROFIBUS-DP 协议，这三种协议的关系如图 3.4 所示。

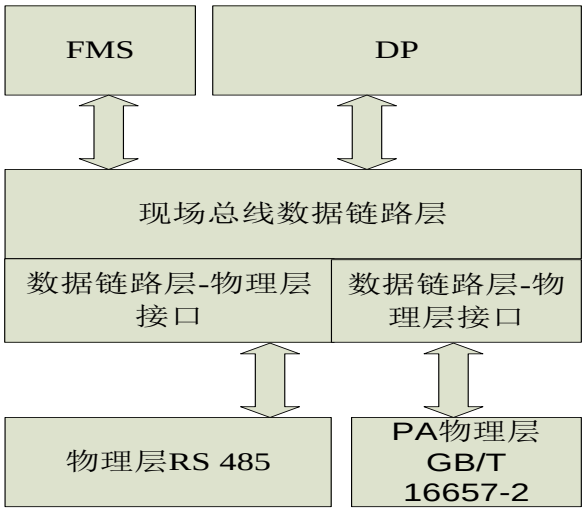

图 3.4 FMS、DP 和 PA

其中，PROFIBUS-FMS 对第一层、第二层和第七层（应用层）均加以定义。PROFIBUS-DP 使用了第一层（物理层），第二层（数据链路层）和应用用户接口，第三层到第七层未予描述。应用用户接口规定了用户系统以及不同设备可调用的应用功能，并详细说明了各种不同 PROFIBUS-DP 设备的设备行为，还提供了 RS 485 传输技术和光纤传输技术。直接数据链路映射（DDLM）提供应用用户接口到第二层服务的映射。该结构确保了快速和高效的数据传输。PROFIBUS-PA 采用了扩展的 PROFIBUS-DP 协议，使用耦合器能很方便地将 PROFIBUS-PA 设备集成到 PROFIBUS-DP 网络中，而根据 IEC 61158-2（GB/T 16657-2）标准，这种通过总线给现场设备供电的传输技术可确保其本质的安全性。

c) DNP3

在 IEC 60870-5 协议规范还未标准化之前（当时仍处于紧张开发过程中），智能网格建设中不同供应商的产品之间的互操作需求已经非常强烈。1993 年，通用电气-哈里斯加拿大子公司（前身为加拿大 Westronic 公司）以部分完成的 IEC 60870-5 协议规范作为基础开发了一种开放且可快速实现的协议，该协议专用于满足北美需求，这就是 DNP3 协议的来源。DNP3 对数据链路层、伪传输层和应用层进行了描述，使用串行链路进行数据通信。

DNP3 的链路规约数据单元（LPDU）采用的可变长帧格式 FT3 定义为：一个固定长度的报文头，后面跟着可选的数据块（每个数据块还附有一个 l6 位的 CRC 校验码）。DNP3 的伪传输层专门设计用于请求站和响应站间传输超出链路规约数据单元长度限制的信息。在 DNP3 中，只有被指定的主站能够发送应用层的请求报文，而从站则只能发送应用层的响应报文（包括主动响应报文）。

相对于 IEC 60870-5-104 对 IEC 60870-5-101 的修改，TCP/IP 上的 DNP3 并没有对串行链路上的 DNP3 作任何实质上的修改，而是将整个链路规约数据单元（LPDU）作为 TCP/IP 之上的应用层数据进行传输（也可能是基于 UDP）。

d) IEC 60870-5-101/104

EC 60870-5-101 是远动设备及系统传输规约中基本远动任务配套标准，适用于具有编码比特串行数据传输的远动设备和系统。而 IEC 60870-5-104 则是采用标准传输规约集的 IEC 60870-5-101 网络访问，即 IEC 60870-5-104 是 IEC 60870-5-101 在 TCP/IP 上的实现。

DNP3 和 IEC 60870-5-101/104 都遵从 IEC 60870-5 的数据链路帧格式（IEC 60870-5-1）和链路传输过程（IEC 60870-5-2），两者之间存在很多相似之处。此处，仅简单介绍一下两者间存在的差异（两者应用层完全不同，此处不涉及应用层），如下表所示：

表 DNP3 和 IEC 60870-5-101/104 的差异

差异	DNP3	IEC 60870-5-101/104
传输方式	平衡方式	平衡方式和非平衡方式
字符格式	8 位数据位、1 位起始位和 1 位停止位	8 位数据位、1 位起始位和 1 位停止位、1 位奇偶校验
帧格式	使用 FT 3，只有变长帧	使用 FT 1.2，有变帧长帧、固定帧长帧和单字节帧
链路层控制字段		将部分应用层命令定义为链路层控制功能，使得部分命令报文不包括应用层数据
链路地址字段	单一地址格式，地址长度固定为 16 位，包含源地址和目的地址	支持 IEC 60870-5-2 中定义的大部分地址格式，但是只包含从站链路层地址，且地址长度可选
伪传输层	在数据链路层和应用层之间加入伪传输层，允许将应用层数据分段组装在多个链路帧中传输	

e) ICCP

远方控制应用服务元素 2（Tele-control Application Service Element 2，TASE.2）又名控制中心间通信协议（Inter Control-center Communication Protocol，ICCP），可利用标准的底层网络通信协议，在多个控制中心间通过广域或局域网实现实时数据及其它信息的相互传输。

TASE.2 的产生和发展经历了两个阶段。从 1993 年开始，IEC TC57 WG07 选择当时已经广泛应用的挪威 ELCOM90 协议（同期还有美国西部电网的 WSCC 等）为基础，制定了国际标准 TASE.1，该标准以 ISO9072 ROSE 为基础。由于 TASE.1 与 ISO/ITU-T 的兼容性差，因此受到美国和德国的坚决反对；于是美国电科院（EPRI）牵头开发了 ICCP，并于 1996 年将其纳入 IEC 体系（IEC 60870-6），称为 TASE.2。该标准以 ISO 9506 MMS（Manufacturing Message Specification）为基础[MMS]。初期，TASE.2 与 TASE.1 并列为国际标准，但互不兼容，形成了欧洲与美国两个系列相争的局面。但由于 MMS 已经广泛应用于各行各业，故 TASE.2 较 TASE.1 适应性更强。随着欧洲发电联盟（UCPTE）宣布采用 TASE.2，持续数年的争论也随之结束，TASE.2 成为全球统一的通信协议。

f) IEC 61850

变电站自动化技术发展很快，国内外厂商相继推出了多种变电站自动化系统产品。为使不同厂商的产品具有互操作性（Interoperation），1995 年国际电工委员会第 57 技术委员会（IEC TC57）成立了 3 个工作组 10/11/12（WG 10/11/12）负责制定 IEC 61850 标准。工作组成员分别来自欧洲、北美和亚洲国家，他们有电力调度、继电保护、电厂、操作运行及电力企业的技术背景，其中有些成员参加过北美及欧洲一些标准的制定工作。3 个工作组有明确的分工：第 10 工作组负责变电站数据通信协议的整体描述和总体功能要求；第 11 工作组负责站级数据通信总线的定义；第 12 工作组负责过程级数据通信协议的定义。

IEC 61850 按照变电站自动化系统所要完成的控制、监视和继电保护三大功能从逻辑上将系统分为 3 层，即变电站层、间隔层和过程层，并定义了 3 层间的 10 种逻辑接口。

3.2.1 工业控制系统协议相关的安全问题

为了增强工控系统的整体安全性，有必要改善工业控制系统协议的安全特征。对协议进行基本的分析将有助于暴露协议中存在的安全问题，进而能够指导安全机制的开发，并最终合并到协议描述中。当前的工控协议基本都有已经完成的国际标准，且有行业和专业组织管

理。向这些已经建立的标准中合并变化不仅过程耗时，而且基本上都会遭受因管理组织不愿改变成文标准而引起延迟。在合并任何新的安全特征到标准之前，理解安全问题将使得将变更合并进标准需要的复审次数更少。另外，理解协议相关的安全问题还将有助于 IDS/IPS 规则的开发。为每一个潜在的利用开发攻击签名是可能的，且工控网络管理员将发现这些签名对于监控其网络的安全是非常有用的。

分析任何协议时，区分安全问题的种类是非常有用的：一类是协议自身的设计和描述引起的，另一类是协议的不正确实现引起的。发现协议设计和描述中的安全问题较协议实现中的安全问题可能要容易的多，也可能要难得多，但修复源于不正确的协议实现的安全问题相对要容易一些。虽然两种类型的安全问题都需要解决以改善网络的整体安全性，但本节仅关注协议自身设计和描述引起的安全问题，关于协议实现所引起的安全问题可参考 3.3 节。

绝大多数工控协议在设计之初，仅关注于效率以支持经济需求、关注于实时性以支持精确需求、关注于可靠性以支持操作需求，并且通常在专用计算机和私有的操作系统上实现。不幸的是，绝大多数工控协议会为了这些需求而放弃一些并不是绝对必需的特征或功能。更不幸的是，诸如认证、授权和加密等需要附加开销的安全特征和功能也包括在内。再进一步让事情复杂的是，目前很多工控协议已经演化或扩展为在通用计算机和通用操作系统上实现，并运行在以太网（甚至互联网）之上以满足商业发展需要，潜在地将这些有漏洞的协议暴露给攻击者。本文将与工控协议相关的安全问题分为两类：一类是工控协议自身特点所造成的固有安全问题;另一类是演化到基于通用计算机、通用操作系统和TCP/IP后继承的安全问题。

1. 固有的问题

目前广泛使用的工控协议在设计之初，大多定位使用于与其它计算机网络隔离的工业控制网络，因此安全不是一个重要的功能需求，并且目前也没有任何合并安全特征到这些协议的尝试。除了缺乏必要的安全防护机制外，工控协议的另一个特点是针对其的攻击主要集中在应用层数据。

下面，我们对这几种典型的工控协议中出现的安全问题进行分析，提供一些针对可能威胁的反制措施，并简单列举一些应该引起 IDS/IPS 开发人员高度关注的异常行为。限于篇幅，本文仅就 MODBUS、PROFIBUS、DNP3、ICCP 这 4 种协议进行详细分析。

a) MODBUS

MODBUS 中存在的主要安全问题的根源在于缺乏认证、授权和加密等安全防护机制。与 MODBUS 协议相关的几个典型的安全问题如

表格 3 所示：

表格 3 与 MODBUS 协议相关的几个典型安全问题

根源	安全问题举例
缺乏认证	仅需要使用一个合法的 Modbus 地址和合法的功能码即可以建立一个 Modbus 会话
缺乏授权	没有基于脚色的访问控制机制，任意用户可以执行任意的功能
缺乏加密	地址和命令明文传输，可以很容易地捕获和解析

MODBUS 相对其它工控协议来说最为简单，因此针对 MODBUS 协议的安全建议除了增加必要的认证、授权和加密功能外，也可以考虑使用白环境。

针对 MODBUS 应用层数据分析结果显示：功能码滥用是导致 MODBUS 网络异常的一个主要因素。需要引起 IDS/IPS 开发人员高度关注的 MODBUS 消息如表格 4 所示：

表格 4 MODBUS 协议典型异常行为

序号	异常行为描述
1	强制从站进入只听模式（08-04）
2	重启通讯会话（08-01）
3	重置诊断信息（例如计数器或诊断寄存器等）（08-0A）
4	请求从站标志信息（43-14）
5	请求从站附加信息（17）
6	不合法的报文长度（2 个字节表示长度），潜在拒绝服务攻击
7	非 Modbus 协议运行在 TCP 的 502 端口
8	从设备忙异常代码延迟（异常码 06），潜在拒绝服务攻击
9	确认异常代码延迟（异常码 05），潜在拒绝服务攻击
10	不正确的报文长度（最大 253），潜在拒绝服务攻击
11	配置扫描（例如定义的点列及其值）（30 秒内 5 个异常码 02）
12	可用功能码扫描（60 秒内 3 个异常码 01）
13	修改分隔符（08-03）
14	周期较短（实际阈值待定）的无意义命令，暴力拒绝服务
15	广播性质的报文或一个主站向多个从站的请求
16	包含在异常协议数据单元中的信息

b) PROFIBUS

与 MODBUS 协议一样，PROFIBUS 协议起初也被设计用于与其它计算机网络网络隔离的工业控制网络，未提供基本的安全防护机制。与 PROFIBUS 协议相关的几个典型的安全问题如表格 5 所示：

表格 5 与 PROFIBUS 协议相关的几个典型安全问题

根源	安全问题举例
缺乏认证	仅需要使用一个合法的 PROFIBUS 地址和合法的功能码即可以建立一个 PROFIBUS 会话
缺乏授权	没有基于脚色的访问控制机制，任意用户可以执行任意的功能
缺乏加密	地址和命令明文传输，可以很容易地捕获和解析
协议复杂性	采用面向对象的思想设计协议提供的服务

针对 PROFIBUS 协议的首要安全建议是引入 PROFISAFE 安全设备。PROFIsafe 将安全设备和标准设备的数据流完全整合在以 PROFIBUS 为平台的总线系统中，使标准设备和安全设备能同时共用一条通信链路。

在 PROFIBUS 网上，所有结点连接到公用的通信介质上，每个源结点可以直接发送消息到其目的结点。由于所有的结点直接连接到介质，因此攻击者并不能修改或删除从一个结点发送到另一个结点的消息，但时能够非常容易地读取到网络上传输的消息，也可以冒充其它的结点。

在 PROFIBUS 网上有 master 和 slave 两种不同类型的结点，每个 slave 仅能受一个 master 的控制。PROFIBUS 网络上的 master 结点形成一个根据其站地址升序排列的的逻辑环。每个 master 结点维护一个 master 站列表（LMS），并追踪其在环中的前站和后站。站地址与其后站地址的差异称为 GAP。每个 master 维护一个 GAP 更新定时器，并在每次定时器到期时查询邻居 master 以更新自己的 LMS。当一个 master 结点收到令牌时，检测以确认发送令牌的站是其在 LMS 中的前站。如果不是其前站，则令牌被丢掉。如果发送令牌的结点坚持重新发送令牌，那么结点会认为网络拓扑发生了变化，并将发送令牌的站设置为其前站。针对 PROFIBUS 的若干可能攻击场景如表格 6 所示：

表格 6 针对 PROFIBUS 的若干可能攻击场景

序号	攻击场景
1	伪装为 master 结点加入网络，并将其 slave 设置为初始配置
2	通过保持对所有 slave 的控制，造成拒绝服务

3	通过时钟同步功能向网络中的某些结点发送错误的时钟同步值，扰乱正常的网络操作
4	通过向令牌帧引入错误可违背协议的访问控制机制
5	通过向数据帧引入错误可破坏数据完整性
6	强制定时器超时可使得设备进入自动睡眠模式，从而关闭设备的接收器。如果设备是 slave，那么该设备会被标识为一个不可操作的设备。如果错误被引入 master 的接受器，那么将造成其不停地重传令牌
7	通过修改 GAP 更新定时器的值可以潜在地阻止结点更新其 LMS
8	通过降低 GAP 更新定时器到一个非常低的值，造成结点在基本所有时间都忙于执行更新而不是发送消息，从而阻塞低优先级的消息传输
9	攻击者通过伪造站地址欺骗另一个结点接受攻击者作为其前站，从而破坏令牌循环

c) DNP3

DNP3 与 MODBUS 比较类似，缺乏认证、授权和加密等安全防护机制。除此之外，协议的相对复杂性也是 DNP3 中存在的主要安全问题根源。与 DNP3 相关的几个典型的安全问题如表格 7 所示：

表格 7 与 DNP3 协议相关的几个典型安全问题

根源	安全问题举例
缺乏认证	使用定义良好功能码和数据类型可以非常容易地建立一个会话
缺乏授权	没有基于脚色的访问控制机制，任意用户可以执行任意的功能
缺乏加密	地址和命令明文传输，可以很容易地捕获和解析
协议复杂性	相对于 MODBUS 的请求相应模式，DNP3 增加了主动上送模式

针对 DNP3 协议的首要安全建议是采用更安全的 DNP3 替换目前存在安全问题的 DNP3。如果条件受限，不能完全替换存在安全问题的 DNP3，其它可以考虑的措施包括：添加必要的安全防护措施，使用任何 TCP/IP 安全最佳实践来保护 DNP3 数据，或者使用标准的纵深防御最佳实践，如表格 8 所示：

表格 8 针对 DNP3 协议的安全建议

措施	举例
替换 DNP3	使用 Security DNP3
必要的安全防护措施	隔离 DNP3 网络，增加验证和授权
TCP/IP 安全最佳实践	使用传输层安全（Transport Layer Security，TLS）保护 DNP3 数据

采用纵深防御	防火墙、IDS 和 IPS

针对 DNP3 应用层数据分析结果显示：与 MODBUS 协议类似，功能码滥用也是 DNP3 协议异常的一个主要因素。需要引起 IDS/IPS 开发人员高度关注的 DNP3 消息如表格 9 所示：

表格 9 DNP3 协议典型异常行为

序号	异常行为描述
1	关闭主动上送（21）
2	在 DNP3 端口（TCP 和 UDP20000）上运行非 DNP3 通信
3	长时间多重主动上送（响应风暴）
4	授权客户冷重启（13）
5	未授权客户冷重启（13）
6	停止应用（18）
7	热重启（14）
8	授权客户的广播请求（根据 DigitalBond 中 IPS/IDS 规则）
9	未授权客户的广播请求（根据 DigitalBond 中 IPS/IDS 规则）
10	配置扫描（例如定义的点列及其值）（30 秒内检测到至少 5 个指示字的第 9 或 10 位设置为 1）
11	可用功能码扫描（60 秒内 3 个指示字的第 8 位设置为 1）
12	更改时间（功能码 02，对象类型 50）
13	校验和错误
14	认证失败
15	数据流控制标志（DFC）欺骗
16	重新初始化数据对象（15）
17	重新初始化应用（16）
18	冰冻并清除可能重要的状态信息（9）
19	无通告冰冻并清除可能重要的状态信息（10）
20	未授权的操作（4）、直接操作（5）、无通告直接操作（6）
21	源自或到达非显式认证的 DNP3 设备的 DNP3 通信
22	配置崩溃（指示字的第 13 位设置）
23	应用数据层 FIR/FIN 标记报文重组攻击
24	应用数据层传输序号报文重组攻击
25	伪传输层 FIR/FIN 标记报文重组攻击
26	伪传输层传输序号报文重组攻击
27	服务不可用或未实现（数据链路层功能码 14 或 15）

28	重置用户进程（数据链路层功能码 1）
29	伪造数据链路层广播地址（0XFFFF）并向所有的从站发送错误请求

现实中针对 DNP3 的攻击包括使用中间人攻击捕获特定系统的地址，并使用捕获的地址对该系统进行操纵，具体的攻击场景如表格 10 所示：

表格 10 针对 DNP3 协议的典型攻击场景

序号	攻击场景
1	关闭主动上送
2	向主站发送伪造的主动上送消息，欺骗操作员做出不合适的操作
3	通过向整个 DNP3 网络注入广播数据来制造风暴行为以达到拒绝服务
4	操纵时间同步数据，导致同步失败并引起随后的通信错误
5	操纵或清除确认消息以迫使系统进入连续的重传状态
6	发起未授权的停止、重新启动或者其它能引起崩溃的功能

d) ICCP

与上述三种协议类似，ICCP 缺乏认证和加密机制。与上述三种协议不同的是，ICCP 通常用于不同的控制中心之间的对等通信，而其它三种协议典型地用于 PLC / RTU 和 HMI / MTU / SCADA 主机之间的服务器-客户端通信；ICCP 虽然使用双边表提供了基本的访问控制机制，但是显式定义的可信关系可能会危害到 ICCP 结点之间的安全；ICCP 是一种广域网协议，这使得其很容易被接触并遭受包括拒绝服务在内的多种攻击。与 ICCP 相关的几个典型的安全问题如表格 11 所示：

表格 11 与 ICCP 协议相关的几个典型安全问题

根源	安全问题举例
缺乏验证	可以很容易地建立会话
缺乏加密	报文明文传输，可以很容易地捕获和解析
显式地定义可信关系	通过利用双边表能够直接地损坏 ICCP 服务器和客户端的安全
可访问	广域网协议使得其高度可访问并其极容易遭受很多种攻击

ICS-CERT 报告过多个 ICCP 的漏洞，且互联网上曾出现过针对 ICCP 的利用代码。因此，非常有必要对 ICCP 网络执行适当的渗透测试并对服务器和客户端打补丁。除此之外，针对 ICCP 协议的首要安全建议是采用更安全的 ICCP 替换目前存在安全问题的 ICCP。如果条件受限，不能完全替换存在安全问题的 ICCP，其它可以考虑的措施包括：添加必要的安全防护措施，谨慎定义双边表，使用任何 TCP/IP 安全最佳实践来保护 DNP3 数据，或者使用标准的纵深防御最佳实践，如表格 12 所示：

表格 12 针对 ICCP 协议的安全建议

措施	举例
确认与修复	ICS-CERT 报告过多个 ICCP 的漏洞，且互联网上曾出现过针对 ICCP 的利用代码，因此非常有必要对 ICCP 网络执行适当的渗透测试并对服务器和客户端打补丁
替换 ICCP	使用 Security ICCP
必要的安全防护措施	使用专用且隔离的 ICCP 网络，增加验证
谨慎定于双边表	双边表是控制中心间的主要的保证和许可措施，通过 ICCP 发起的恶意命令能够直接改变或影响控制中心的操作
TCP/IP 安全最佳实践	使用传输层安全（Transport Layer Security，TLS）保护 ICCP 数据
采用纵深防御	防火墙、IDS 和 IPS

针对 ICCP 应用层数据分析结果显示，需要引起 IDS/IPS 开发人员高度关注的 ICCP 消息如表格 13 所示（其中：最后 1 条针对增加了必要安全防护措施的情况）：

表格 13 ICCP 协议典型异常行为

序号	异常行为描述
1	功能“read”可用于泄露受保护的信息
2	功能“write”可用于操纵客户和服务器操作
3	在 ICCP 端口（TCP102）上运行非 ICCP 通信
4	任何源自或者到达非验证的 ICCP 设备的 ICCP 通信

现实中通过监视 ICCP 链路，检测到的具体攻击场景如表格 14 所示：

表格 14 ICCP 协议典型攻击场景

序号	攻击场景
1	侵入者通过被忽视的访问点（例如拨号、合作方或提供者的网络）获取对控制中心网络的未授权访问
2	心怀怨恨的雇员访问和传输未授权的信息、更改安全配置以及其它可能损害控制中心物理安全的恶意操作
3	源自重复信息请求（spamming）的拒绝服务攻击，消耗服务器的可用资源以阻止合法的 ICCP 操作
4	ICCP 服务器或者其它设备感染恶意软件从而泄露敏感信息，例如盗窃可用于破坏目的的命令功能码、改变用于交易的能源计量以崩溃财务运营以及其它各种恶意目的
5	截获或者修改 ICCP 消息

2. 继承的问题

目前，基本所有广泛使用的工控协议都已经演化或扩展为在通用计算机和通用操作系统上实现，并运行于 TCP/IP 之上以满足商业发展需要。TCP/IP 协议自身存在的安全问题不可避免地会影响到运行于其上的应用层工控协议。本文从操作系统层、网际层和传输层三个层次介绍 TCP/IP 之上的工控协议继承的安全问题。

a) 操作系统层

- VxWorks 认证 API 弱哈希算法

随着通用计算机和通用操作系统在工控系统中的广泛使用，攻击者可以使用与实时操作系统开发人员相同的调试工具。他们可以读符号表，查看每一条汇编，甚至可能都不需要编程知识。例如：风河系统（Wind River Systems）的 VxWorks 实时操作系统的认证 API 使用默认的弱强度哈希算法，攻击者可通过暴力碰撞计算出与实际密码具有相同哈希值的字串。

b) 网际层

- 遭受 UDP 端口诊断服务器攻击

VxWorks 的调试服务运行于 UDP 17185（0X4321），默认打开。攻击者不需要任何认证就可以隐秘地执行以下攻击：远程倾倒内存，远程补丁内存、远程调用函数、远程任务管理。

- 遭受 Smurf 攻击

Smurf 攻击是以最初发动这种攻击的程序名“Smurf”来命名的。这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf 攻击通过将向某个网络广播地址发送的 ICMP 请求数据包的回复地址设置成第三方的受害者，导致该网络的所有主机都对此 ICMP 请求做出答复，从而淹没受害主机并导致网络阻塞，最终导致第三方崩溃。在工控系统的背景下，遭受 Smurf 攻击的对象可以是 RTU，也可能是 SCADA 主机。

- 遭受被动网络探测攻击

攻击者可以通过网卡混杂模式被动地捕获广播网络的所有数据包。在工控系统的背景下，攻击者可以获取网络的拓扑、RTU 设备功能、SCADA 主机运行的服务以及其他数据。

- 遭受 Idle Scan 攻击

Idle Scan 又叫 Zombie Scan 或者 Dumb Scan，是一种 TCP 端口扫描方法，可以用于确认目标主机的特定端口是否是打开的。该方法通过使用一个称为 Zombie 的主机，避免与目标主机发生直接的交互。基本原理如图 3.5 所示：

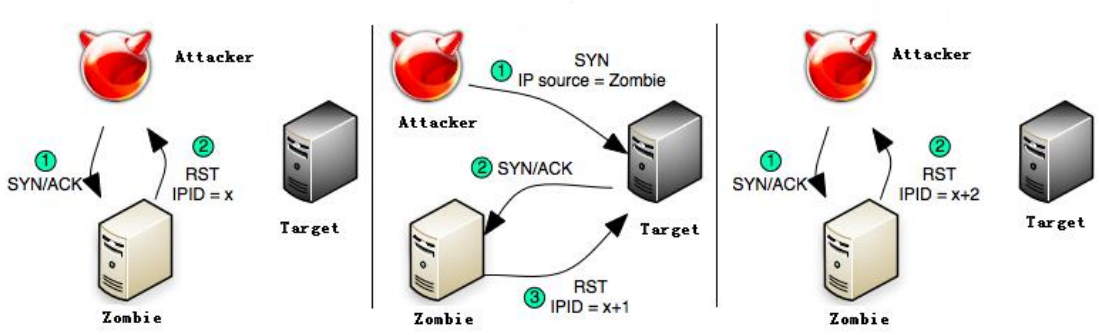

图 3.5 Idle Scan

首先攻击者向 Zombie 主机发送一个 SYN/ACK 报文，Zombie 返回一个 RST 报文（IPID 为 x）；第二步攻击者向目标主机的特定端口发送一个 SYN 报文，但是将源地址伪造为 Zombie 主机，如果目标主机上该端口是打开的，则会向 Zombie 主机回复 SYN/ACK 报文，与第一步

相同，由于 Zombie 并没有发送 SYN 报文，因此 Zombie 返回一个 RST 报文（IPID 为 x+1）；第三步攻击者再次向 Zombie 主机发送 SYN/ACK 报文，如果 Zombie 返回一个 RST 报文（IPID 为 x+2），则表示目标主机上特定的端口打开。如果目标主机上特定的端口未打开或被防火墙屏蔽，则第二步目标主机不会向 Zombie 发送 SYN/ACK 报文，Zombie 也不会返回一个 RST 报文（IPID 为 x+1），因此第三步攻击者得到的 RST 报文（IPID 仍为 x+1）。在工控系统的背景下，可以使用 Idle Scan 确认 SCADA 主机上特定的端口是否打开。

- 遭受 ARP 欺骗/放毒攻击

ARP 主要用于在局域网上转换 IP 地址为 MAC 地址。ARP 欺骗/放毒通过修改网络上缓存的 IP/MAC 对实现。通过发送虚假的 ARP 报文到网络，攻击者可以混淆网络设备（例如交换机）。在工控系统的背景下，可以通过 ARP 欺骗/放毒，接收发往其它结点的数据完成嗅探，或者将发往其它结点的数据转向到不可达结点从而造成拒绝服务。

- 中间人攻击

攻击者可以通过恶意软件的基线响应重放、流氓侵入者设备等多种方式，或者通过在 ARP 欺骗/放毒混淆网络设备的基础上实现中间人攻击。

- 遭受链/环攻击

在链攻击中，很多结点之间形成一个连接链，攻击者有可能隐藏起来源和身份。在环攻击下，连接链变成了一个环，攻击者的来源和身份更难以追踪。在工控系统的背景下，要谨防攻击者发动链/环攻击。

c) 传输层

- 遭受 SYN Flooding 攻击

SYN Flooding 攻击通过发送大量的 TCP 半开连接请求，耗尽目标的资源。在工控系统的背景下，可能造成目标的拒绝服务。

3.2.2 针对工业控制系统协议的异常行为分类

1. 分类方法论（基于威胁方式的分类）

要全面地认识一个系统可能存在的安全问题，除了要理解上述的基本属性，也应该考虑其他一些用于描述信息安全不同特性的属性。例如：Sun 公司一份关于 Solaris 上加固企业计算的技术报告[SUN]中，对通过窃听技术截获网络数据，通过中间人攻击修改网络数据，通过拒

绝服务中断网络流，通过欺骗伪造认证（原文使用 authority，实际上应该是 authentication）进行了分析，这四种攻击分别违反了保密性、完整性、可用性和认证四种安全属性。

前文中，我们对几种典型的工控协议中存在的若干安全问题进行了研究，指出了与这些安全问题相关的可疑异常行为。本节，我们根据各种可疑异常行为对六种安全属性的违反情况，对其进行分类，如图 3.6 所示。这六种安全属性是：保密性、完整性、可用性、认证（authentication）、授权（authorization）和不可抵赖性（non-repudiation）。

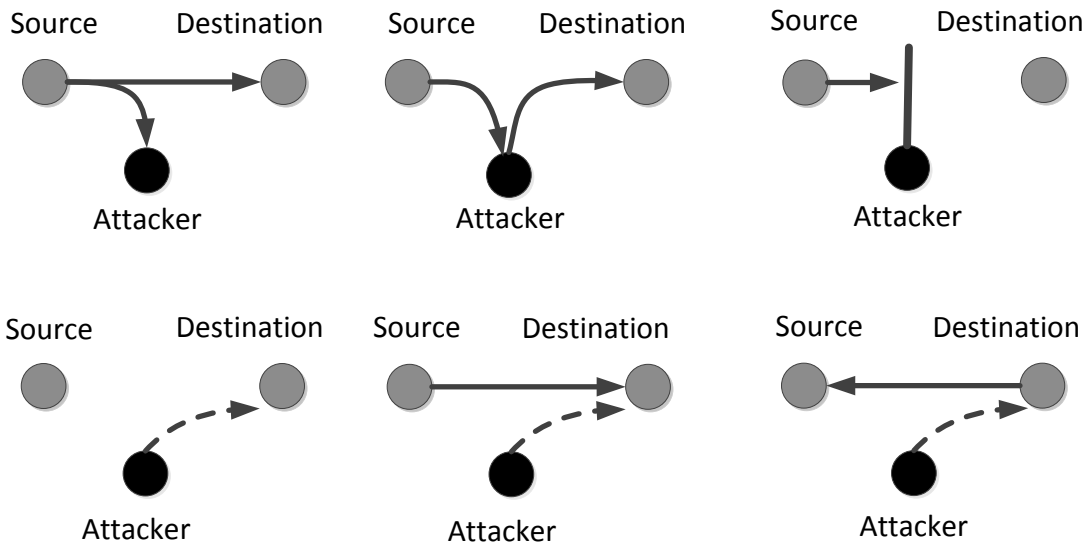

图 3.6 针对 6 种安全属性违反情况的图示

以工控系统为例，认证的重要性在于，保证收到的消息来自合法的用户，允许未认证用户向设备发送控制命令会造成巨大的危害；授权的重要性在于，保证不同的特权操作需要由拥有不同权限的认证用户来完成，可降低误操作与内部攻击的概率；不可抵赖性的重要性主要体现在事后审计上。对于工控系统，总的来说：不可抵赖性的重要性最低，授权、认证、机密性、完整性、可用性依次增强。

2. 异常行为分类举例一：针对 Modbus 的分类

根据前文介绍的异常行为分类方法论，本节根据对上述 6 种安全属性的违反情况，对 MODBUS 协议中可能出现的异常行为（表格 15）进行分类，如下表所示。其中，对应位置的“√”表示可能违反指定的安全属性。

表格 15 针对 MODBUS 协议的异常行为分类

序号	保密性	完整性	可用性	认证	授权	不可抵赖性
1			√	√	√	√
2			√	√	√	√

3			√	√	√	√
4	√			√	√	√
5	√			√	√	√
6		√	√			
7				√		
8			√	√		
9			√	√		
10		√	√			
11	√			√	√	√
12				√	√	√
13			√	√	√	√
14			√	√		
15				√	√	
16				√		

3. 异常行为分类举例二：针对 DNP3 的分类

根据前文介绍的异常行为分类方法论，本节根据对上述 6 种安全属性的违反情况，对 DNP3 协议中可能出现的异常行为（表格 16）进行分类，如下表所示。其中，对应位置的“√”表示可能违反指定的安全属性。

表格 16 针对 DNP3 协议的异常行为分类

序号	保密性	完整性	可用性	认证	授权	不可抵赖性
1			√	√	√	√
2				√		
3				√		
4			√		√	√
5			√	√	√	√
6			√	√	√	√
7			√	√	√	√
8					√	
9				√	√	
10	√			√	√	√
11				√	√	√
12			√	√	√	√

13				√		
14					√	√
15			√	√		
16			√	√	√	√
17			√	√	√	√
18		√		√	√	√
19		√		√	√	√
20				√	√	
21				√		
22	√	√	√	√		
23		√	√	√		
24		√	√	√		
25		√	√	√		
26		√	√	√		
27			√	√		
28			√	√	√	√
29				√		

3.2.3 工业控制系统协议的安全总结

为了增强工控系统的整体安全性，有必要改善工控协议的安全特征。对协议进行基本的分析将有助于暴露协议中存在的安全问题。协议中的安全问题可分为两类：一类是协议自身的设计和描述引起的，另一类是协议的不正确实现引起的。

本节对几种广泛使用的工控协议自身设计和描述引起的安全问题进行了分析和研究，发现与之相关的安全问题可分为两类：一类是工控协议自身特点所造成的固有安全问题；另一类是演化到基于通用计算机、通用操作系统和 TCP/IP 后继承的安全问题。工控协议自身特点所造成的固有安全问题主要源于认证、授权、不可抵赖等安全属性的缺失，而继承的安全问题主要包括从操作系统层、网际层和传输层三个层次继承的安全问题。

3.3 工业控制系统漏洞的统计分析

截止到 2012 年 11 月底，绿盟科技安全漏洞库中共收录到 216 个与工业控制系统相关的漏洞，对这些漏洞我们主要按发布时间、威胁类型、厂商分布、厂商所属地区、受影响的对象分类以及漏洞的攻击途径等几个角度进行了统计分析，其结果如下：

3.3.1 按发布时间分布情况分析

图 3-7 给出了从 2007 年到 2012 年 11 月之间所发布的工业控制系统相关公开漏洞按年度进行统计分析的结果。从图中可以很明显地看出：在 2011 年之前，公开披露的工业控制系统相关漏洞数量相当少。但在 2011 年出现了井喷现象，并持续到 2012 年。这显然和 2010 年的 Stuxnet 蠕虫引起人们对工业控制系统安全问题的广泛关注有关。我们预计至少在未来一段时间内，工业控制系统仍然将是漏洞研究者们感兴趣的话题。

图 3.7 公开漏洞数量的年度统计分析图

3.3.2 按威胁类型分布情况分析

按照漏洞可能造成的危害，我们将其分为越权执行、越权写入、越权读取、拒绝服务四大类威胁：

1、越权执行，指的是缓冲区溢出、命令执行、SQL 注入等可以直接对系统造成较大程度控制的漏洞。

2、越权写入，指的是能以某种方式在系统上写入文件、修改用户密码和系统配置等，但无法直接执行代码的漏洞。

3、越权读取，指的是能读取指定或任意文件、内存信息等的漏洞。

4、拒绝服务，指的是可导致进程崩溃、死锁等，使软件无法正常工作的漏洞。

根据我们对工业控制相关漏洞按威胁类型的分析结果（图 3.8 所示）可知，危害最严重的越权执行类漏洞数量也是最多。

而通过对这类漏洞的详细分析发现，这类漏洞又以缓冲区溢出类漏洞最多，占该类漏洞的一半以上。从整体上看，近年来缓冲区溢出类漏洞无论是绝对数量还是相对比例都呈下降趋势，而在工业控制系统领域却出现较多缓冲区溢出类漏洞的现象，我们认为其主要原因可能是因为以前研究者对此类漏洞关注较少，所以很多软件中累积了大量此类漏洞，而当研究者们开始对这些软件进行检查时，积累多年的漏洞就暴露了出来。

另外，很多软件为了实现通过浏览器控制管理的功能，自己实现了 WEB 服务器。我们发现这些自己实现的 WEB 服务器几乎都存在安全漏洞。特别是目录遍历问题，极其普遍。

WEB 服务器属于较容易出漏洞的软件，Apache、IIS 等主流 WEB 服务器软件历史上都出过很多严重安全问题，软件开发者和漏洞研究者们配合，修改了很多年，到今天才做到相对比较安全。而由于工业控制系统软件的开发者通常不具备 WEB 服务器的安全开发经验，所以自行实现的 WEB 服务器很难做到安全。我们建议开发者最好参考一些比较成熟的开源轻量级 WEB 服务器的代码，而不要完全自己从头开发。

另外，身份验证、权限管理等相关漏洞也相对较多。

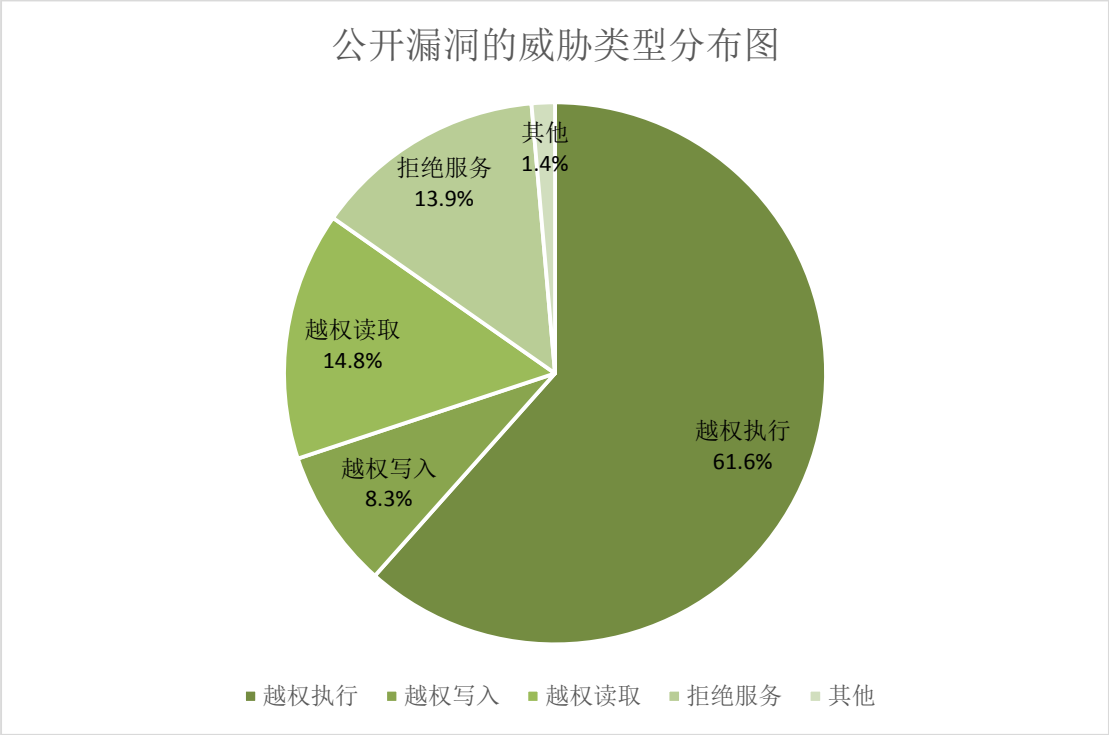

图 3.8 公开漏洞按威胁类型分布的统计分析

3.3.3 按厂商分布情况分析

图 3.9 通过对漏洞的统计分析，给出了公开漏洞所涉及的主要工业控制系统厂商及各厂商系统所发现漏洞占漏洞库中所有漏洞的比例。但需要说明的是：各厂商产品的漏洞数量不仅与产品自身的安全性有关，而且也和厂商的产品数量、产品的复杂度、受研究者关注程度等多种因素有关。因此，我们并不能简单地认为公开漏洞数量越多的厂商产品越不安全。

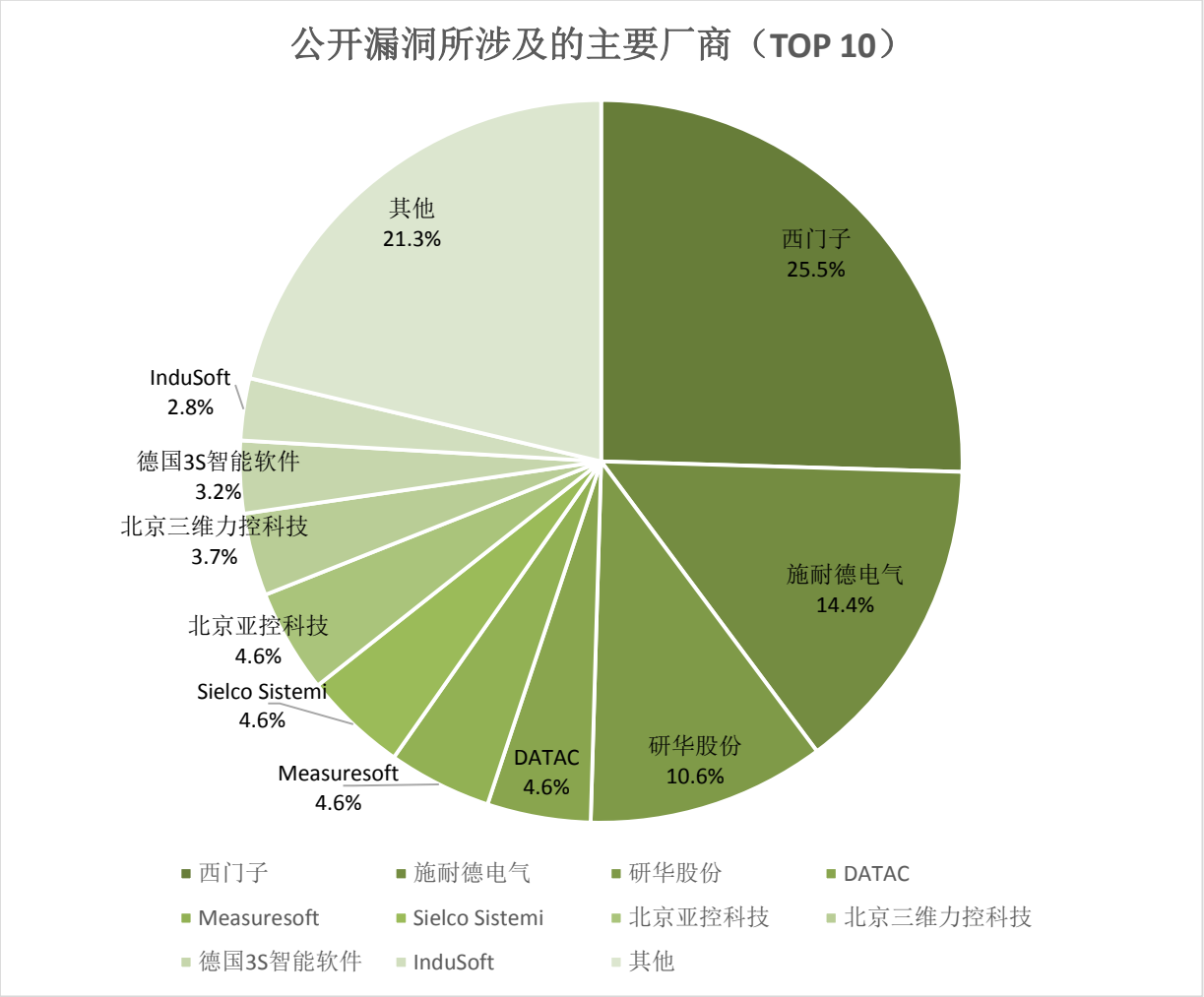

图 3.9 公开漏洞所涉及的主要工业控制系统厂商

3.3.4 按厂商所属地区情况分析

在公开的工业控制系统漏洞中，中国（含港、澳、台地区）的厂商约占五分之一（如图 3.10 所示），但结合市场份额和产品数量等因素综合来看，这个比例其实并不算少。事实上，由于语言等原因，很多国内工业控制软件（这里主要指大陆地区厂商的 ICS 软件）并未被国际上的安全研究者所分析，否则这个比例可能更大。

为了解中国大陆地区工业控制系统软件安全的真实情况，我们对 6 家大陆地区主要工业控制软件提供商的产品进行了为期 1 个月的尝试性分析，在其中 5 家厂商的产品中已发现了多个严重安全漏洞。

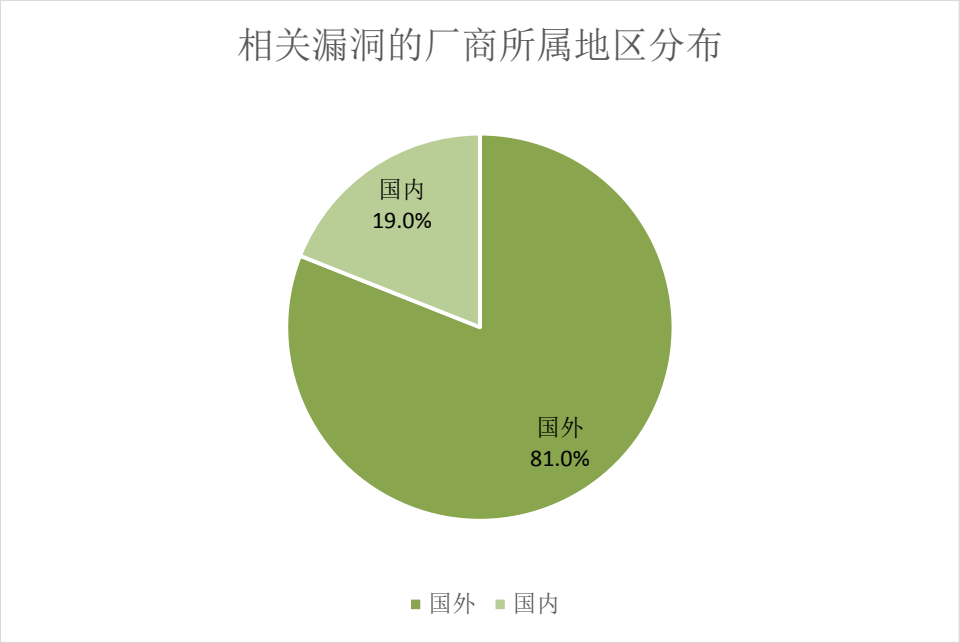

图 3.10 相关漏洞涉及的 ICS 厂商所属地区分析

3.3.5 按受影响对象属性分类情况分析

图 3.11 是对漏洞按受影响对象的软、硬件形态进行统计分类的结果。得到软件中的漏洞占多数的分析结果并不意外，因为从逻辑复杂度来说，相关软件通常都比硬件更复杂，因而更容易出问题。而且对研究者来说，获得软件作为研究对象相对容易（大部分厂商都提供软件的测试版本下载），而获得硬件的成本则高得多。所以公开的硬件类漏洞数量一般远少于软件类漏洞的数量。

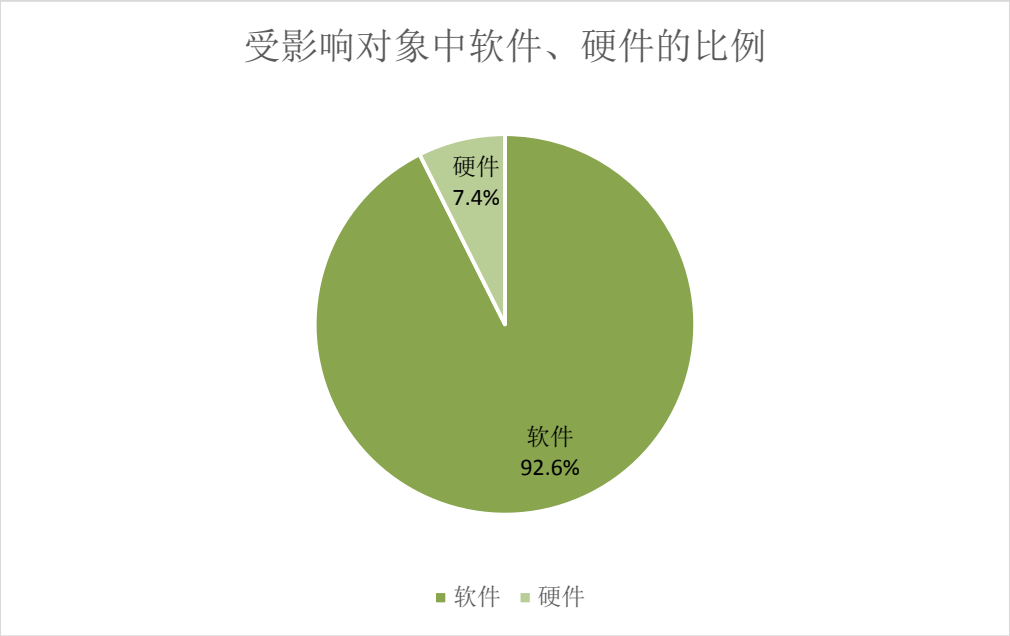

图 3.11 漏洞所涉及对象按软硬件形态的分类分析

3.3.6 按漏洞的攻击途径分类情况分析

通常漏洞按攻击途径划分为以下几类：远程服务器漏洞、远程客户端漏洞以及本地漏洞，其中：

- 远程服务器漏洞主要是指位于提供网络服务的进程中的漏洞。攻击者可以通过网络在另一台电脑上直接进行攻击，而无需用户进行任何操作。
- 远程客户端漏洞则几乎都是 ActiveX 控件的问题。这类漏洞需要诱使用户访问某个恶意网页才会被触发。
- 本地漏洞指的是必须登录到安装软件的计算机上才能利用的漏洞。该类漏洞因利用条件苛刻，威胁也最小。

根据工业控制系统相关的漏洞按攻击途径的分类统计分析结果（如图 3.12、图 3.13 所示）可知：远程漏洞占绝大多数，本地漏洞很少。而在远程漏洞中，服务器漏洞又占绝大多数。

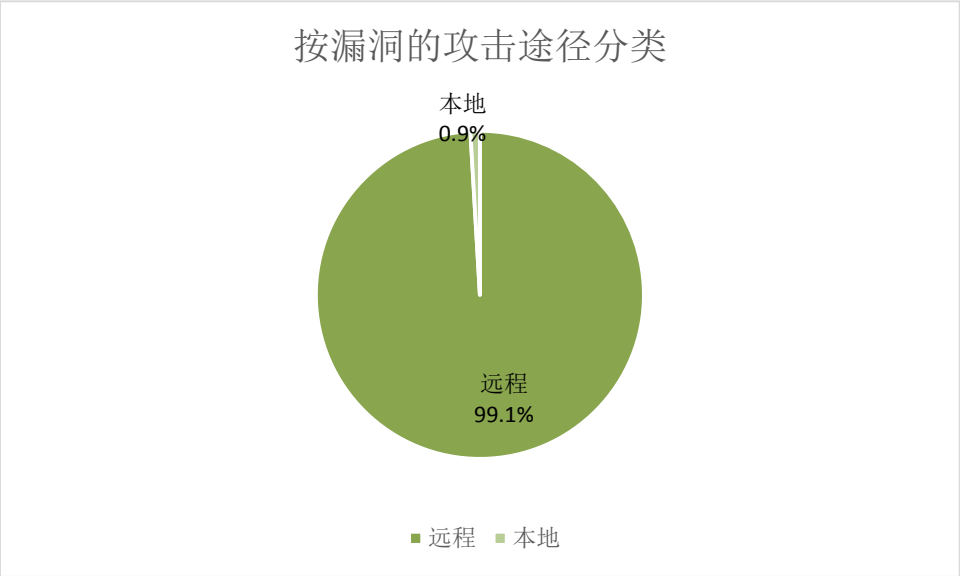

图 3.12 漏洞按攻击途径的分类分析

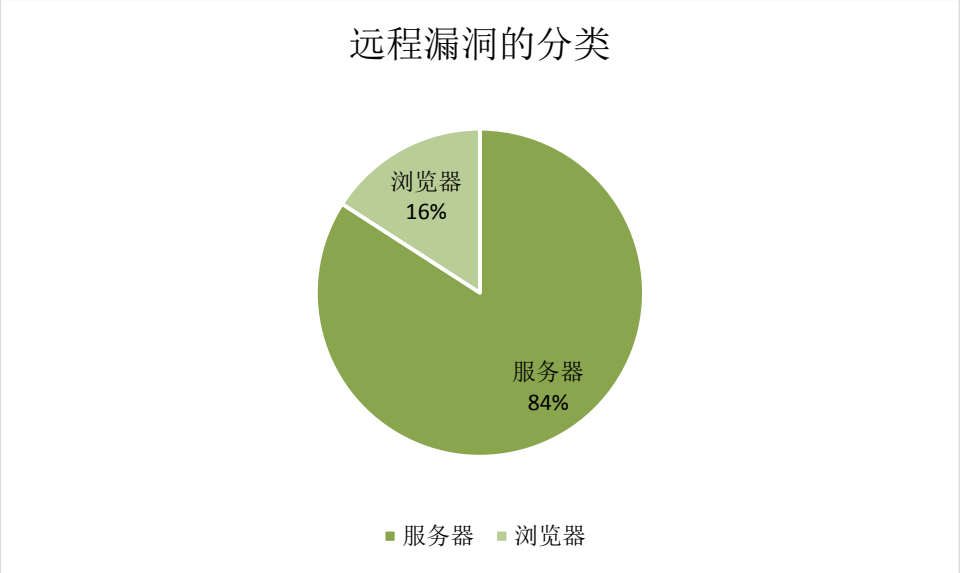

图 3.13 远程漏洞的主要分类

四. 工业控制系统的攻击场景研究

上述章节重点分析了工业控制系统所存在的脆弱性问题——协议的安全缺陷及相关漏洞的情况，本章将基于一个虚构的工业控制系统环境（如图 4.1、图 4.2 所示），针对攻击者可能利用现场无线网络或企业办公网进行渗透攻击，威胁工业控制网络的两种情况，分别介绍一个虚构的攻击场景案例。

本章描述攻击场景案例（虚构）的目的仅是为了使读者对工业控制系统所面临的可能安全威胁有一个直观的了解，提高大家的安全防护意识，尽早考虑其工业控制系统所面临的具体安全风险及应对措施，做到防患于未然。

4.1 案例 1：攻击者利用现场无线网络干扰生产的攻击场景

- **案例起因**

工厂 A 和工厂 B 正在争夺一笔巨额海外订单。这笔订单对双方都非常重要，可能直接影响今后在业界的地位。

工厂 B 的老板悄悄找来了分管技术的副厂长，让他在厂里选两个技术最好的人，设法入侵工厂 A 的自动化生产系统，使其无力争夺当前这笔订单。IT 部门的小王和自动化部门的小刘被选中了。

- **案例描述**

图 4.1 给出了虚拟攻击者利用工业控制系统的现场无线网络从工厂 A 的外部逐步渗透，最终侵入到工艺处理区网络，达到干扰公司 A 的生产控制过程，进而影响其产品质量的攻击场景示意图。案例的虚拟入侵过程具体描述如下：

第一步：侵入无线运料小车网络

小王从小刘处了解到，工厂 A 也在使用无线运料小车，运料小车通过 802.11b 协议连接到工艺处理区的网络。小王对无线网络比较熟悉，他认为这可能是比较容易的突破口。

通过实地察看，小王发现工厂 A 的安全保卫工作比较严密，外人并不容易混进去。而距离围墙最近的厂房也有二十多米。小王带着笔记本电脑在围墙外尝试扫描无线网络，勉强看到一些信号，但连接很不稳定。并且在围墙外也很容易被人发现。

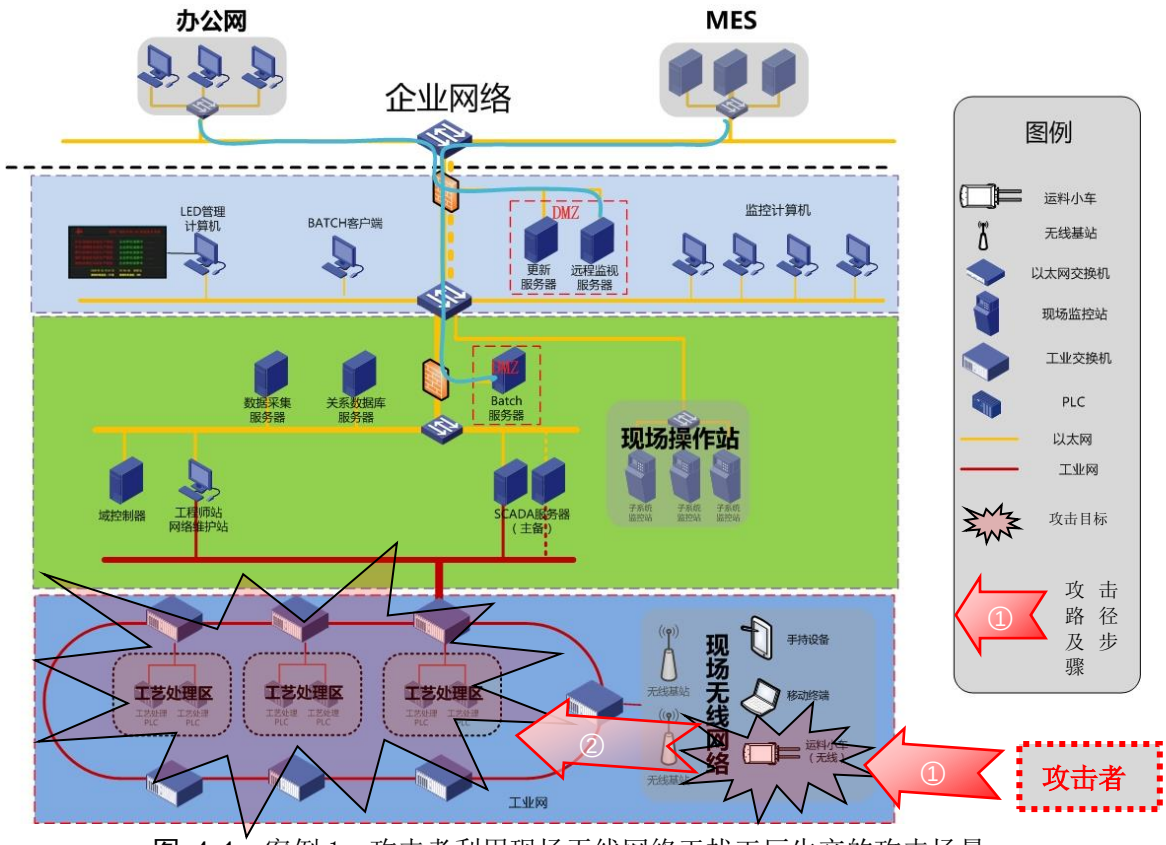

图 4.1 案例 1：攻击者利用现场无线网络干扰工厂生产的攻击场景

于是小王带着一只 16dBi 增益的定向天线，一只大功率无线网卡，和小刘在工厂 A 附近的一栋居民楼租了间房。这间房和最近的厂房距离大约 200 米。

小王在窗口架设好天线，指向厂房。连接好所有设备后，他运行了一个无线网络信息收集工具。小王惊奇地发现，运料小车和无线接入点之间的通信甚至没有启用 WEP 加密——事实上，即使启用了 WEP 这种并不安全的加密方式，也可以很快破解得到密码。

小王很轻松地将笔记本通过无线网络接入了运料小车所在的网络，然后运行网络扫描程序，开始收集信息。

第二步：侵入工艺处理区网络，干扰生产控制设备

小刘告诉他，接入运料小车所在的工艺处理区网络后，不光可以直接访问网络中所有其它运料小车和生产设备的 PLC，还有可能访问到 SCADA 服务器和工程师工作站等。

根据小刘提供的信息，小王对扫描结果进行分析，在其中寻找工业控制相关协议的默认端口，很容易就识别出了几十台运料小车对应的几十个 IP 地址。因为这些运料小车都开启了 TCP/502 端口，也就是 MODBUS 协议使用的端口。

小王通过无线网络抓取了一些运料小车的控制数据，交给小刘分析，希望通过这种方法了解运料小车的控制协议，但小刘表示这比较困难。小王注意到运料小车的 IP 上除 MODBUS 的 TCP/502 端口外，还开启了 HTTP 服务。他用浏览器访问小车的 HTTP 服务，发现这是运料小车的管理界面，在这个界面上可以找到厂商、型号等信息。

小刘告诉小王，工业控制系统一般都是集成化的，从运料小车上看到的厂商信息，可能就是工厂 A 的整套工业控制系统提供商。于是小刘以工厂 B 技术人员的身份，很容易从这家提供商处索取到了相关文档和试用软件等资料。

利用这些资料，再结合对网络的扫描结果，小王和小刘不但很快摸清了这套工业控制网络的结构，还知道了如何控制运料小车——他们甚至不需要分析控制协议，直接用从厂家索取的软件就行了。

小王提出，可以通过控制运料小车，使其改变装料、卸料等时间，让工厂 A 无法生产出合格的产品。但小刘提醒他说，小车的异常动作可能很容易被发现，从而引起怀疑和追查。

小刘看了小王的扫描结果，参考之前从工厂 A 的控制系统提供商处索取的资料，发现工艺处理区的网络里还有一些 IP 地址对应的是生产设备的温度控制器。于是他提出，可以一方面接管对温度控制器的控制，发送伪造的控制命令，使工艺温度略微提高一些，导致产品质量下降；同时给 SCADA 服务器发送伪造的传感器数据，使 SCADA 服务器认为设备温度仍然是正常的。这样，即使工厂 A 发现了产品存在问题，也很难找到原因。

小王研究了一会儿，认为这个方案在技术上可行。

攻击持续数日后，果然传出了工厂 A 产品质量出现问题，并找不到原因的消息。还听说他们找来工业控制系统提供商的技术人员帮忙。于是小王停止了攻击，和小刘悄悄离开了那栋居民楼。

- **案例结果**

最终，那笔海外订单被工厂 B 获得了，而工厂 A 的生产线也恢复了正常。他们一直不知道为什么会在那个关键时刻出现问题。曾怀疑是内部有人捣鬼，但察看了监控录像，并没有发现任何异常。

4.2 案例 2：攻击者利用办公网窃取机密生产资料的攻击场景

- **案例起因**

工厂 B 得到那笔关键的订单后，一跃成为当地的明星企业。经过几年发展，不光拓展了生产规模，还建立起一支初具规模的科研团队，开发出好几种新产品，销路很不错。

专门受雇入侵网络的攻击小组 X 最近接到一笔生意，让他们窃取工厂 B 新产品的生产工艺、图纸、配方等资料。

- **案例描述**

图 4.2 描述了攻击小组 X（案例 2 中虚构的攻击者）通过工厂 B 的托管在 IDC 的服务器逐步攻击渗透，最终侵入工厂 B 的工业控制网络，并从 Batch 服务器中成功盗取重要生产数据的攻击场景。入侵过程具体描述如下：

第一步：X 首先设法入侵了工厂 B 对外的网站（托管在 IDC 的服务器）

网站看来是外包开发的，代码已经好多年没有升级维护了，所以入侵一点都不困难。但很快他们发现网站服务器并不在工厂本身的网络中，而是托管在 IDC 机房。但 X 也发现这台服务器同时是工厂 B 的邮件服务器。他们读了服务器上保存的邮件，了解了不少工厂 B 的情况，甚至还看到一些技术文档，但其中并没有想要的完整工艺资料。

第二步：渗透入侵办公网，控制科研人员办公计算机

在看了很多人的邮箱后，X 在一个科研人员的收件箱里发现一封尚未接收的邮件，里面有一个软件。X 修改了这封邮件，给软件捆绑上了木马。第二天，X 发现这封邮件已经被接收了。同时，木马的控制端也收到了一个连接。X 通过控制端察看了被控的电脑，果然是一个科研人员的办公电脑。

X 在这台电脑中找到一些技术资料。交给雇主后，雇主并不满意，称资料非常不完整，并且不是工厂 B 现在那些新产品的资料。于是 X 继续对网络进行渗透，很快又控制了研发部门的几台电脑，但仍没有找到雇主想要的资料。

X 继续进行渗透。半个月后，已经控制了办公网中二十多台电脑。X 仔细地检查每一台被控电脑，寻找有价值的数据，但都没有找到想要的工艺资料。

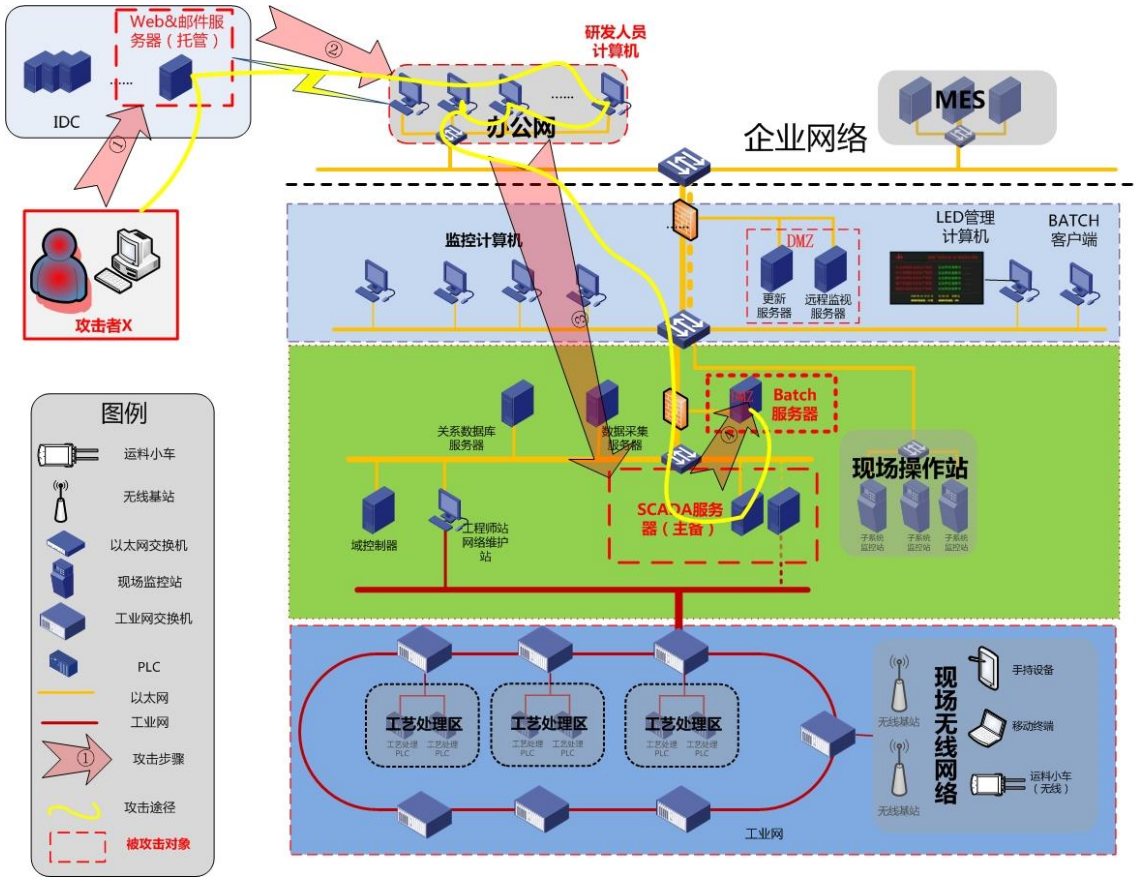

图 4.2 案例 2：攻击者利用办公网络窃取机密生产资料的攻击场景

第三步：从办公网渗透侵入工业控制网络，控制 SCADA 服务器

雇主告诉 X，生产系统中负责执行生产任务的 Batch 服务器里一定会有完整的工艺资料，MES（制造执行系统）相关服务器中也可能有。同时雇主也告诉 X，MES 服务器和办公网之间可能是直接连接的，建议他们优先考虑入侵 MES。

但 X 在网络中甚至没找到 MES，怀疑可能这些电脑本身的安全措施比较严格，扫描等常用网络探测措施都无法发现。而 Batch 服务器因为和办公网之间有防火墙隔离，无法直接访问到。

在监视一台电脑的桌面时，X 看到了一个运行着的 SCADA 监控界面。X 非常兴奋，因为之前一直认为办公网和工业控制网络是彻底隔离的，没想到有人为了方便随时查看系统的状态，让办公网也可以连接 SCADA 服务器。

X 查看这台电脑的当前连接，知道了 SCADA 服务器的 IP 地址。再通过分析电脑上安装的 SCADA 软件，很容易得到了该厂使用的软件名称和版本信息。在网上搜索了软件的相关信息后，X 发现他们所使用的软件版本较旧，存在好几个严重漏洞。

X 设法找到了同一版本软件，在自己的系统上搭建测试环境，开始编写针对这些漏洞的攻击程序。因为这些漏洞的利用难度都不大，所以只用了一天，程序就写好了。

利用攻击程序，X 顺利地控制了 SCADA 服务器。有了 SCADA 服务器作为跳板，现在 X 可以在工业控制这部分网络中横行无忌了。他们高兴地发现，这里很多电脑甚至连操作系统补丁都没有及时更新，存在大量漏洞。很快，X 找到了用来执行生产任务的 Batch 服务器。

第四步：侵入 Batch 服务器，盗取机密生产数据

X 发现 Batch 服务器所运行的控制软件也同样存在很多漏洞。所以，X 并没有费多大力气，也成功入侵了 Batch 服务器。在服务器的生产数据库里，获得了完整的工艺数据。

X 把窃取的资料交给雇主，雇主很满意。

- **案例结果**

不久后，工厂 B 在市场上发现了和自己的新产品类似的仿制品，检验后发现成分组成和各方面性能几乎都完全一样。这些仿制品的生产商是工厂 A。

五. 工业控制系统的一些安全建议

5.1 工业控制系统面临的安全问题分析

虽然因工业控制系统工作环境相对封闭、多采用专用通信协议且很难获得系统分析样本而很少遭到入侵攻击；但并不能说工业控制系统的用户就可以高枕无忧。本文前面章节的研究结果表明，目前工业控制系统普遍存在一些严重的安全问题，主要表现为：

- **严重漏洞难以及时处理，系统安全风险巨大**

当前主流的工业控制系统普遍存在安全漏洞，且多为能够造成远程攻击、越权执行的严重威胁类漏洞；而且近两年漏洞的数量呈快速增长的趋势。工业控制系统通信协议种类繁多、系统软件难以及时升级、设备使用周期长以及系统补丁兼容性差、发布周期长等现实问题，又造成工业控制系统的补丁管理困难，难以及时处理威胁严重的漏洞。

- **工业控制系统协议缺乏足够的安全性考虑，易被攻击者利用**

专有的工业控制通信协议或规约在设计时通常只强调通信的实时性及可用性，对安全性普遍考虑不足：比如缺少足够强度的认证、加密、授权等。尤其是工业控制系统中的无线通信协议，更容易遭受第三者的窃听及欺骗性攻击（比如第 4.1 节的虚拟案例 1 中利用现场无线网络攻击的攻击场景所描述的攻击方式）。

- **缺乏违规操作、越权访问行为审计能力**

操作管理人员的技术水平和安全意识差别较大，容易发生越权访问、违规操作，给生产系统埋下极大的安全隐患。实事上，国内 ICS 相对封闭的环境，也使得来自系统内部人员在应用系统层面的误操作、违规操作或故意的破坏性操作成为工业控制系统所面临的主要安全风险。因此，对生产网络的访问行为、特定控制协议内容和数据库数据的真实性、完整性进行监控、管理与审计是非常必要的。

但现实环境中通常缺乏针对 ICS 的安全日志审计及配置变更管理。这是因为部分 ICS 系统可能不具备审计功能或者虽有日志审计功能但系统的性能要求决定了它不能开启审计功能所造成的结果。同时目前的安全审计产品因缺乏对工业控制系统通信协议的解析能力而不能直接用于 ICS 系统中，需要专门的定制。由于工业控制系统通信协议缺

乏统一的标准，使得这种定制工作代价巨大且不能通用也是造成 ICS 中违规操作行为审计缺乏的原因之一。

- **没有足够的安全政策、管理制度，人员安全意识缺乏**

由于工业控制系统不像互联网或与传统企业 IT 网络那样备受黑客的关注，在 2010 年“震网”事件发生之前很少有黑客攻击工业控制网络的事件发生（如图 1.1 所示）；工业控制系统在设计时也多考虑系统的可用性，普遍对安全性问题的考虑不足，更不用提制订完善的工业控制系统安全政策、管理制度以及对人员的安全意识培养了。‘和平日久’造成人员的安全意识淡薄。

而随着 ICS 系统在国计民生中的重要性日益重要以及 IT 通用协议和系统在工控系统的逐渐应用，人员安全意识薄弱将是造成工业控制系统安全风险的一个重要因素，特别是社会工程学相关的定向钓鱼攻击可能是重要岗位人员沦为外部威胁入侵的跳板（比如 RSA 丢失 SecurID 认证令牌的事件中利用一封鱼叉式网络钓鱼的电子邮件侵入 RSA 公司内部网络的案例[netsecurity1] ）。

- **面对新型的 APT 攻击，缺乏有效的应对措施**

APT（高级可持续性威胁）的攻击目标更为明确，攻击时会利用最新的 0-day 漏洞，强调攻击技术的精心组合与攻击者之间的协同；而且是为不达目的不罢休的持久性攻击。近年来以震网为代表的针对工业控制系统的攻击事件都呈现了这些攻击技术特征[Symantec]，本文第四章的攻击场景中的攻击过程也说明了企业会面临竞争对手出于市场竞争目的而不择手段的攻击。

但是针对这种 APT 攻击，现有的安全防护手段均显得有些无力[BWLZ]。这也许需要整合各种安全技术，通过形成完善的安全防御体系（防御手段的组织化、体系化）才可能有效，然而工业控制系统对安全关注严重不足的现实，使其在面临 APT 攻击时将会遭到不可估量的安全损失。

5.2 工业控制系统的安全建议

工业控制系统安全的重要性及其普遍安全防护措施不足的现实，使得加强工业控制系统的安全性来说无疑是一项相对艰巨的任务。因为当面临攻击者的持续关注时，任何疏漏都可

能导致灾难。对此，我们在参考信息安全业内的最佳实践的基础上，结合工业控制系统自身的安全问题，提出了一些安全建议，期望能够有效地降低工业控制系统所面临的攻击威胁：

1. 加强对工业控制系统的脆弱性（系统漏洞及配置缺陷）的合作研究，提供针对性地解决方案和安全保护措施：

a) 源头控制：运营组织和关键提供商建立工业控制系统开发的全生命周期安全管理。在系统的需求分析、架构设计、开发实现、内部测试、第三方测试和人员知识传递等研发生命周期的典型阶段，融入安全设计、安全编码以及安全测试等相关安全技术，尽可能系统地识别和消除各个阶段可能出现的来自于人员知识和技能、开发环境、业务逻辑引入系统缺陷的安全风险（如图 5.1 所示）。

图 5.1 绿盟科技应用安全开发生命周期（NSFocus ADSL）

b) 分析检测及防护：工业控制系统行业应积极展开与安全研究组织或机构的合作，加强对重要工业控制系统所使用软硬件的静态和动态代码脆弱性分析、系统漏洞分析研究；开发工业控制系统行业专用的漏洞扫描、补丁管理及系统配置核查工具。

c) 漏洞库管理：国家主管机构主导建立权威的 ICS 专业漏洞库以及完善的漏洞安全补丁发布机制。

2. 尽可能采用安全的通信协议及规范，并提供协议异常性检测能力

a) 源头控制：在不影响系统实时性、可用性的前提下，工业控制系统应尽可能采用具有认证、加密、授权机制的安全性较高的通信协议来保证其控制命令和生产数据的安全传输。尤其是无线通信协议要重点考虑其安全性；因为不安全的无线通信协议非常容易遭致远程攻击（如第四章的虚拟案例一所述）。

b) 检测防护：基于对 ICS 通信协议与规约的深度解码分析，通过网络协议异常性特征识别与监测 ICS 各系统和网络间可能存在的威胁，并提供针对性的防护措施，从而提升了企业对于系统运行过程的威胁感知与安全防护能力

c) 标准制订：国家主管机构应促进工业控制系统行业与安全研究机构、厂商的合作，并主导制订相关的通信协议的安全标准。以提供推荐性行业标准。

3. 建立针对 ICS 的违规操作、越权访问等行为的有效监管

a) 异常行为检测：对 ICS 系统的各种操作行为进行分析，并基于<主体，地点，时间，访问方式，操作，客体>的行为描述六元组模型（如图 5.2 所示）构建系统操作行为或网络运行相关的白环境。基于白环境可以很方便地开发针对 ICS 异常行为的检测类产品（比如 IPS）。

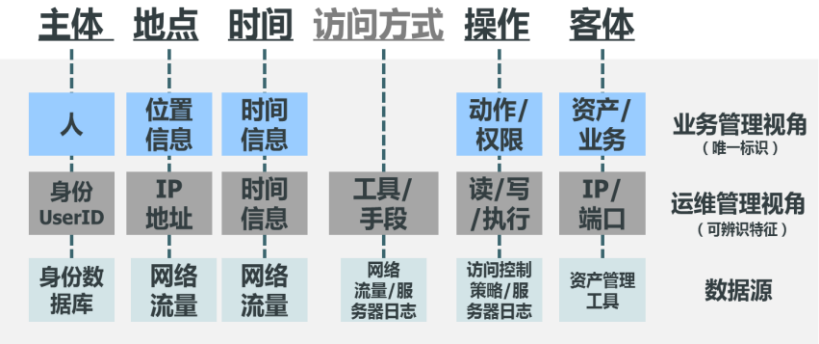

图 5.2 基于六元组的异常检测模型

b) 安全审计：基于对 ICS 通信协议与规约的深度解码分析，实现对 ICS 系统的安全日志记录及审计功能。应考虑对控制过程实现基于网络流量的安全审计，审计过程应力争做到对控制指令的识别和可控，如 Modbus、DNP3 等经典工控协议的解析能力分析，实现工业控制协议会话的过程记录和审计；并提供安全事件之后的事后追查能力。

4. 建立完善的 ICS 安全保障体系，加强安全运维与管理。

a) ICS 安全保障体系建设

在保证工业控制系统的正常运行的前提下，充分调动技术、管理等安全手段，对帐号与口令安全、恶意代码管理、安全更新（补丁管理）、业务连续性管理等关键控制领域实施制度化/流程化、可落地的、具有多层次纵深防御能力的安全保障体系建设。

其建设依据将参考以下国内外工业控制系统安全相关政策及实践，使企业能够充分识别运行管理过程的信息安全控制点，构建符合国家、行业监管、资本市场要求以及安全最佳实践的安全保障体系。具体参考的相关政策和安全实践包括但不限于：

- 《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451 号）
- GB/T 26333-2010 《工业控制网络安全风险评估规范》
- IEC 62443/ISA 99《工业过程测量、控制和自动化 网络与系统信息安全》
- NIST SP800-82 《工业控制系统 (ICS) 安全指南》
- NIST SP800-53 《联邦信息系统和组织的安全控制推荐》
- 北美电气可靠性协会关键性基础设施防护标准（NERC CIP 标准）等。

b) 安全运维与管理

- 边界控制：严格管理所有可能的 ICS 系统访问入口，包括将 SCADA 相关系统与互联网及其他办公网络物理隔离，严格控制移动介质和无线网络的接入，必要时采用设备准入控制机制。
- 系统上线安全评估及周期性安全评估：工业控制系统的入网与上线是整个系统安全生命周期的重要阶段，也是系统所有者和操作者掌握其安全风险水平的最佳时机。因此，在系统上线时要尽可能对系统的安全状况进行较为详细的评估：系统及应用漏洞扫描、WEB 应用测试与扫描、ICS 系统安全基线配置核查以及无线现场网络的安全评估等。然后根据评估结果在保障 ICS 系统可用性的前提下，尽可能对发现的安全问题进行处理。需要注意的是：常见的评估工具和测试手段将有可能会造成系统的中断（如产生偶然的拒绝服务攻击），因此对工业控制统的评估和测试和传统的 IT 风险评估相比应更加谨慎，在评估的过程中可采用一些能够确保对工业控制系统的影响降到最低的替代性评估手段（如表 5.1）。

对象	常见手段（IT 环境）	工业控制系统建议手段
主机和网络	主机地址扫描（如 NMAP）	手工配置检查 物理线缆跟踪/检索 数据包被动监听（嗅探和入侵检测） 控制扫描范围
服务	端口扫描（如 NMAP）	本地端口检查（Netstat）

		测试环境扫描
漏洞	漏洞扫描（如 Nessus）	本地服务检查（如 Banner）结合 CVE 漏洞库信息对比 测试环境扫描

表格 17 安全测试、检查的替代手段（建议）

- 系统防护：系统防护措施的更新速度是其有效性最重要的度量指标，只有及时更新通用或专用系统的安全补丁和相关配置，升级各种防护和检测设备的规则，才能起到有效的防护效果。
- 需要保障 ICS 系统业务连续性的应急响应计划，强调对安全事件的快速响应能力。

c) 此外，还需要加强人员的安全意识培训和工作流程管理制度的落实等。

5. 加强针对 ICS 的新型攻击技术（例如 APT）的防范研究

目前 ICS 领域影响最大的就是‘震网病毒’为代表的高级可持续性威胁（APT）类攻击。这类 APT 攻击并不是一个独立的、具体的攻击技术，而是一种攻击行为模式的体现。达成 APT 攻击需要无孔不入的情报收集能力；它们往往掌握有最新的 0day 漏洞、拥有能够规避当时检测工具的传播和控制程序，以及能够利用所掌握的资源快速展开连锁行动的组织力和行动力。显然，这样的攻击不是能够依靠单一的技术实现防范和检测的，针对性的防护需要多个层面安全防护措施的综合开展：

a) 做好 ICS 系统的基础性安全防护工作。从防范主体的角度来看，应当做到“安全防御无死角”。面对长期的侦测和试探，任何安全短板都可能成为攻击者的快速通道。也许只有做好各方面的防范，通过多种安全产品（机制）协同工作的体系化防御措施才能够抵御 APT 这些高级的持久性攻击[LHP]。

b) 加强“深入分析”技术的探索。APT 攻击并不意味着没有痕迹，只是隐蔽性较强而难以发现。通过收集 APT 攻击事件相关的技术情报（攻击的特征、原理、危害、样本及分析报告等），并利用多维度的海量数据挖掘和关联分析技术，实现跨时域、跨设备和跨区域的踪迹分析，来大幅增加发现攻击行为的概率。也就是说，只有具备及时识别、发现 APT 攻击的能力之后，才能有效地提供针对性的 APT 安全防护能力。

c) 加强国际合作，协同研究与防范。由于 APT 攻击具有低成本、高破坏和隐蔽性的特点，它对 CII 或工业控制系统攻击所造成的破坏和社会影响，很有可能不逊于核武器的攻击后果。如果不对其加以限制，只会使破坏程度不断升级。所以，成立国际联合组织、建立国际性的抑制体系可以减少国家间的过激行为，同时也可监控和打击网络犯罪及恐怖主义行为。

上述描述的安全建议从多维度考虑对工业控制系统可能面对的风险进行防护，并尽可能降低相关系统的安全风险级别。但需要意识到由于外部威胁环境和系统技术演变将可能引入新的风险点。系统、人员、商业目标以及内、外部威胁等安全相关因素的任何一个发生改变时，都应建议企业对当前安全防护体系的正确性和有效性重新进行评估，以确定其能否有效应对新的风险。因此 ICS 的安全保障措施也将是一个持续的改善过程，通过这一过程可使工业控制系统获得最大程度的保护。

六. 结束语

工业控制系统被广泛应用在电力、交通、石油化工等国家重要行业中，甚至很多系统已成为国家重要信息基础设施的一部分（比如电力行业的工业控制系统），它们的安危甚至能够严重影响到国计民生，因此，为保证系统的安全，工业控制系统在以往多是相对独立的工作环境，系统的软硬件及通信协议也基本上是不同于互联网的专有系统或协议。

近年来，工业信息化及物联网技术的高速发展，以往相对封闭的工业控制系统也逐渐采用通用的通信协议、硬软件系统，甚至有些工业控制系统也能够以某些方式连接到互联网等公共网络。传统信息网络所面临的病毒、木马、入侵攻击、拒绝服务等安全威胁也正在向工业控制系统扩散。特别是从“震网”病毒事件爆发及美国发布“国家网络空间安全战略”之后，工业控制系统的安全问题得到了各国的重视，并提到了国家安全战略的地步。但是因国内工业控制系统的相对封闭性，工业控制系统一直不是网络攻防研究关注的重点，国内的安全研究团队对工业控制系统了解不多，自然关于工业控制系统安全方面，也不会有太多的成果积累与实践经验；同时，工业控制系统厂商更加关注系统的可用性和实时性问题，也是很少考虑工业控制系统的安全性问题。

针对工业控制系统安全的重要性及相关研究相对不足的现实情况，我们及时开展工业控制系统安全性研究工作。在初步介绍工业控制系统的基础上，首先对工业控制系统与传统 IT 信息系统进行了差异化对比分析，初步讨论工业控制系统的安全性。其次，结合我们在安全攻防、协议安全性及漏洞研究方面的技术优势，重点开展工业控制系统的协议安全性分析、相关漏洞的统计分析以及几个典型攻击场景的分析研究；明确了工业控制系统当前面临的主要安全问题。最后，我们参考信息安全业内的最佳实践，针对工业控制系统的安全问题，提出了一些安全性建议，期望据此能够有效地降低工业控制系统所面临的攻击威胁。

本文的研究工作可供工业控制系统的安全管理人员以及相关安全产品的规划、研发及服务人员参考，可帮助他们初步了解工业控制系统的原理及其存在的安全性问题，进而为后续开发适用于工业控制系统相关的安全产品或提供相应的安全解决方案奠定基础。

附录　缩略语中英文对照

APT，Advanced Persistent Threat，高级持续性威胁

CII， Critical Information Infrastructure，关键信息基础设施

Configuration，组态

DCS，Distributed Control Systems，集散控制系统

DNP，Distributed Network Protocol，IEC 制订的一种工业控制通信协议

FCS，Fieldbus Control System，现场总线控制系统

Fieldbus，现场总线

HMI，Human Machine Interface，人机界面，通常指 SCADA 系统人机界面

ICS，Industrial Control Systems，工业控制系统

IEC，International Electrical Commission，国际电工委员会的简称

IED，Intelligent Electronic Device，智能电子设备

MES，Manufacturing Execution System，制造执行系统

MTU，Master Terminal Unit，主控终端

OLE，Object Linking and Embedding，对象链接与嵌入技术

OPC，OLE for Process Control, 用于过程控制的 OLE

PAC，Programmable Automation Controller，可编程自动化控制器

PLC，Programmable Logic Controller，可编程逻辑控制器

RTU，Remote Terminal Unit，远程终端

SCADA，Supervisory Control And Data Acquisition，数据采集与监视控制系统

Supervisory Workstation，监视站

参考文献

1. [Beaumont] Beaumont, Peter. Stuxnet worm heralds new era of global cyberwar. London: Guardian.co.uk. 30 September 2010
2. [BWLZ] 鲍旭华、王卫东、李鸿培、赵粮，2011 年安全回顾与展望，绿盟科技技术内刊，Vol.16，2012 年 4 月
3. [CJ] 曹嘉，ICS 工业控制系统安全事件分析，技术报告，绿盟科技内部报告，2012 年 10 月
4. [DNP] IEEE Power & Energy Society，IEEE Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3),IEEE Std 1815™-2010
5. [ENISA] Protecting Industrial Control Systems：European Network and Information Security Agency，ENISA，Dec.,2011
6. [Eric] Eric D.Knapp， Industrial Network Security：Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems,2011.
7. [GB26333] 工业控制网络安全风险评估规范，GB26333-2010-T
8. [GK] 中国工控网，SCADA 系统市场分析，www.gongkong.com
9. [Gregg] Gregg Keizer. Is Stuxnet the 'best' malware ever? Infoworld Retrieved 16 September 2010
10. [GXB451] 关于加强工业控制系统信息安全管理的通知，工信部协[2011]451 号
11. [Halliday] Halliday, Josh. Stuxnet worm is the 'work of a national government agency'. London: The Guardian. Retrieved 27 September 2010
12. [HYL] 胡毅、于东、刘明烈，工业控制网络的研究现状及发展趋势，计算机科学 Vol.37,NO.1,Jan. 2010
13. [HYX] 侯云晓，工业控制系统开源工具介绍，绿盟科技内部技术报告，2012
14. [IEC60870-5] IEC60870-5，PART {1，2，101，104}.
15. [IEC60870-6] IEC60870-6，PART {502，702，802}.
16. [IEC61850] IEC61850，PART {6，7-1，7-2，7-3，7-4，8-1，9-1，9-2}.
17. [ISA-2007] Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. ANSI/ISA–99.00.01–2007.

18. [LHC] 李文法、忽朝俭、曹嘉，工业控制系统安全概述，绿盟科技技术内刊，Vol.18,2012 年 9 月
19. [LHP] 李鸿培，下一代安全技术方向的思考，技术报告，绿盟科技内部报告，2012.4
20. [MBUS] Modbus IDA, MODBUS Application Protocol Specification v1.1a, North Grafton, Massachusetts. www.modbus.org/specs.php.
21. [Microsoft] Conficker Worm: Help Protect Windows from Conficker. Microsoft 10 April 2009, Retrieved 6 December 2010
22. [MMS] ISO-9506，PART{1，2}
23. [NIST-1] Guide to Industrial Control Systems (ICS) Security：NIST，SP800－82.,June,2011.
24. [NIST-2] Guide for Assessing the Security Controls in Federal Information Systems and Organizations：NIST，SP800－53A.
25. [NSTB] NSTB Assessments Summary Report：Common Industrial Control System Cyber Security Weaknesses.May.2010
26. [PBUS] Profibus International,“PROFIBUS Technology and Applications - System Description”, http://www.profibus.com
27. [RD04] Ron Derynck，SCADA system security threats, vulnerabilities and solutions，Verano，2004
28. [Reals] Reals, Tucker (24 September 2010). Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes? CBS News
29. [Robert] Robert McMillan. Iran was prime target of SCADA worm. Computerworld Retrieved 17 September 2010
30. [SR] Suhas Rautmare，SCADA System Security Challenges and Recommendations
31. [SUN] SUN Microsystems,Secure Enterprise Computing with the Solaris™ 8 Operating Environment, A Technical White Paper
32. [Symantec] W32.Stuxnet. Symantec 17 September 2010, Retrieved 2 March 2011
33. [TW] 唐文，工业基础设施信息安全，技术报告，西门中国研究院，2011 年
34. [USDE] 21 steps to improve cyber security of SCADA networks, The President’s critical infrastructure protection board, office of energy assurance, US department of Energy
35. [Wiki] https://en.wikipedia.org/wiki/Advanced_Persistent_Threat

36. [XB] 谢斌，烟草工业控制系统安全分析与防护思路，绿盟科技技术内刊，Vol.16，2012 年 4 月

37. [ZFG] 周发桂，信息安全基线在电力行业的应用，绿盟科技技术内刊，V0l.15，2011 年 12 月

38. [ZS] 张帅，ICS 工业控制系统安全风险分析，技术报告，金山网络企业安全事业部

39. [ZSP] 赵世平，工业控制系统中的现场总线安全性，安天实验室，2011 年 12 月

作者信息

李鸿培

Email：lihongpei@nsfocus.com

Blog: http://www.i170.com/user/falcon

博士、高级工程师，绿盟科技研究院战略师。研究方向主要涉及网络安全、可信网络体系架构、安全信息智能处理技术及工业控制系统安全研究等。

于旸

Email：yuyang@nsfocus.com

绿盟科技研究院安全研究员，应急响应小组专家成员。在漏洞研究及应急响应工具方面有很多重要研究成果：曾发现多个Cisco、Microsoft等安全漏洞，并开发了诸如可信shell、内核检查、系统调用异常检测等工具。

忽朝俭

Email：huchaojian@nsfocus.com

博士，绿盟科技研究院研究员。研究方向主要涉及网络安全、软件安全与程序分析、安全协议分析、漏洞研究以及工业控制系统安全等。

曹嘉

Email：caojia@nsfocus.com

绿盟科技行业技术部咨询服务顾问。长期参与咨询服务相关业务，对云计算、工业控制安全等领域有着深入研究，参与并且主持了与绿盟科技与工业控制系统相关的主要安全咨询项目，项目覆盖电力、石化、烟草等重点行业。

侯云晓

Email: houyunxiao@nsfocus.com

绿盟科技行业技术部咨询服务顾问。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS