NSFOCUS

2015 NSFOCUS ICS Security Framework Whitepaper

2015 绿盟科技工控安保框架

白皮书

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易。

股票简称：绿盟科技　股票代码：300369

关于作者

王晓鹏

Email: wangxiaopeng@nsfocus.com

绿盟科技工控安全项目总监，长期从事工控安全研究，具有多年的工控安全项目经验，参与多项国家工控安全标准的制定；工控安全产业联盟理事、国家工控安全工程实验室技术专家委员。

侯云晓

绿盟科技高级咨询顾问，长期从事工控安全研究，参与并主持工业控制系统相关的安全服务解决方案开发，参与多项针对大型工控设施的安全评估和咨询服务。

冯冲

Email: fengchong@nsfocus.com

绿盟科技烟草行业资深安全顾问，主持和参与多项烟草行业的信息安全规划和建设项目。

王涛

Email: wangtao2@intra.nsfocus.com

绿盟科技能源行业安全顾问，主持和参与多项能源行业的信息安全规划和建设项目。

目录

内容提要

根据 2014 年 ICS-CERT 发布的数据，工业控制系统硬件制造行业发生的网络渗透事件高达 65 例，占总比的 27%。

其 2014 的年度报告显示，在所有的攻击事件中，55% 的被调查事件显示，高级持续性威胁被用于攻击工业控制系统的安全漏洞。

另有部分安全风险来自黑客活动、网络罪犯以及机构的内部威胁。

从 2010 年震网病毒事件到 2015 年乌克兰电力攻击事件，绿盟科技持续跟踪分析这些工控系统安全事件中，并陆续发布多份工控安全研究报告，

同时持续与合作伙伴一起进行深入实践。在多年沉淀和经验积累后，绿盟科技总结出工业控制系统的攻击路线图，并在此基础上给出工控系统总体安全保障框架，该框架基于绿盟科技对工控系统安全需求的理解，结合国内工控安全的规范要求及国外相关标准内容，提出从技术、管理和运行三个维度来保障工控系统安全，这些维度包含网络边界防护、安全纵深防护、安全运行管理和安全管理制度要求等几个方面，涉及从上线前的安全检测、安全能力部署、安全运行三个阶段，覆盖工业控制系统运行周期的安全保障。

本次白皮书还着重分析了电力行业、石油石化行业、烟草行业工控安全面临的主要威胁，并给出了解决思路及保障框架，为保障业务顺利进行提供了建设性意见，强烈推荐该行业从业人员了解并探讨。

绿盟科技历次工控安全报告

序列	报告主题	研究内容
第 1 报告	工控安全问题	漏洞及威胁
第 2 报告	工控安全性分析	协议、漏洞及攻击场景
第 3 报告	工控安全威胁	APT 及变电站、自来水厂业务环境
第 4 报告	工控安全发展态势	政策、行业、厂商及生态环境
本次报告	工控安保框架	技术演进、电力、石油石化及烟草生产系统

如果您需要了解更多信息，请联系：

扫描二维码，在线看报告

01 工业控制系统安全新态势

1.1 工业信息化的新态势

1.1.1 工业 4.0

在 2011 年德国举办的工业设备展览会“汉诺威工业博览会 2011”上“工业 4.0”的概念被首次提出，在两年后的“汉诺威工业博览会 2013”上发布了最终报告，开始实施“工业 4.0”的国家战略。德国作为制造业大国，希望在未来制造业的各个环节中通过应用互联网技术，将数字信息与现实社会之间的联系可视化，将生产工艺与管理流程全面融合。由此实现智能工厂，并生产出智能产品。

与此同时美国也提出了“工业互联网”的概念，其将关注点放在设备互联、数据分析、以及数据基础上对业务的洞察，希望利用互联网使传统的工业互联互通，并着力关注云计算和大数据技术在此过程中的运用。

可以看到，虽然德国的工业 4.0 与美国的工业物联网的实施路径、逻辑思路、发展重点都有所区别，但究其根本他们的目标是一致的，就是实现智能制造，实现互联网技术和工业的融合。

我国政府在制定“中国制造 2025”的过程中，也紧盯新一轮产业发展的潮流，并结合我国国情选择了更易实现的工业 4.0 路径，与德国开展多领域的广泛、丰富的合作，大力发展工业现代化，力求将我国的工业 2.0、3.0 一起并联的到工业 4.0。

随着国际国内工业互联网、工业 4.0、中国制造 2025 战略的提出，工业生产的数字化已然成为一种不可阻挡的未来趋势，高度融合 IT 技术的工业自动化应用将会得到迅速而广泛的使用，对于工业控制系统的信息安全的关注也将达到前所未有的高度和广度。

1.1.2 能源互联网

能源是现代社会赖以生存和发展的基础，随着社会的快速发展，建立在传统石化能源基础上的能源发展方式已经难以为继，从当前和长远看，要实现能源的可持续发展，研究和解决世界能源发展问题，各国都在积极研究新型能源技术，以及对于可再生能源的有效利用方式，“能源互联网”概念由此应运而生。

目前对能源互联网的普遍认识是综合运用先进的电力电子技术、信息技术和智能管理技术，将大量由分布式能量采集装置、分布式能量储存装置和各种类型负载构成的新型电力网络、石油网络、天然气网络等能源节点互联起来，以实现能量双向流动的能量对等交换与共享网络。

在 能源互联网中将运用先进的传感器、控制和软件应用程序，将能源生产端、能源传输端、能源消费端的数以亿计的设备、机器、系统连接起来，形成能源互联网的“物联基础”。大数据分析、机器学习和预测等技术将成为能源互联网实现生命体特征的重要技术支撑，能源互联网通过整合运行数据、天气数据、气象数据、电网数据、电力市场数据等多种类型的海量数据，进行大数据分析、负荷预测、发电预测、机器学习，打通并优化能源生产和能源消费端的运作效率，需求和供应将可以进行随时的动态调整。

能源互联网目前还在规划和尝试建设阶段，未来能源互联网必将成为社会生活的重要组成部分，为社会的发展提供有力的推动。由于其对移动互联网等 IT 技术的应用，以及其数据的巨大价值，其必将成为安全攻击的重要目标，因此需要在规划和建设的初期就对其可能面临的安全风险进行分析，并同步规划应对的安全防范措施。

1.1.3 “互联网 +”时代的工控安全

我国政府在今年年初提出了“互联网＋”行动计划，推动生产制造模式的变革，产业的组织创新以及产业结构升级。随着该计划的推进网络和信息技术将渗透到各个传统的行业，使得传统行业的基础设施能够进行远程的智能化控制和操作。通过传统行业与互联网技术的结合就形成了物联网、工业互联网、信息物理系统、智慧城市等新兴领域，究其核心就是网络互连。

在网络互连的大背景下，工业控制系统的互连已经成为不可避免的趋势。通过网络互连一方面可以提高生产力和创新能力，减少工业能源及资源消耗，助力产业模式转型升级；但另一方面也会因为网络互联而诱发一系列网络安全问题。

工业控制系统设计之初是为了完成各种实时控制功能，并没有考虑到安全防护方面的问题，通过网络互联将他们暴露在互联网上，无疑将给他们所控制的关键基础设施、重要系统等都带来巨大的安全风险和隐患。从近几年网络攻击的发展趋势来看，目前工业控制系统遭受的网络攻击已经成为各国政府所面临的最严重的国家安全挑战之一。

1.2 工业控制系统安全的新态势

工业控制系统广泛用于冶金、电力、石油石化、核能等工业生产领域，以及航空、铁路、公路、地铁等公共服务领域，是国家关键生产设施和基础设施运行的“中枢”。从工业控制系统自身来看，随着计算机和网络技术的发展，尤其是信息化与工业化深度融合，工业控制系统越来越多地采用通用协议、通用硬件和通用软件，通过互联网等公共网络连接的业务系统也越来越普遍，这使得针对工业控制系统的攻击行为大幅度增长，也使得工业控制系统的脆弱性正在逐渐显现，面临的信息安全问题日益突出。2010 年的“震网”病毒、2012 年的超级病毒“火焰”、2014 年的 Havex 病毒等等专门针对工业控制系统的病毒爆发给用户带来了巨大损失，同时直接或间接地威胁到国家安全。2015 年发生的乌克兰电力遭受攻击事件看到，在不需要利用复杂攻击手段、不需要完整还原业务系统运行过程的情况下，就可以达到对工控系统的运行影响。从实际的攻击过程看，攻击的成本在降低，而攻击所带来的影响在进一步加重。

美国修订 ICS 安全指南

2015 年 6 月 8 日，美国国家标准与技术研究院发布第二版工业控制系统（ICS）安全指南，该指南包括如何调整传统 IT 安全控制系统以适应工业控制系统独特的性能、可靠性和安全性要求; 同时对威胁与漏洞、风险管理、实施方案、安全体系架构等部分进行了更新。

ICS 安全指南自 2006 年首次发布以来下载量已达到 300 万次，ICS 安全指南提供了如何减少计算机漏洞控制工业系统遭受恶意攻击，设备故障，错误，不充分的恶意软件防护和其他威胁等方面的建议。

大多数 ICS 最初都是专用的，采用独立的软硬件集合与其他部分隔开，并与外部威胁隔离。如今，大量的通用软件应用，互联网设备和其他非专用 IT 产品已经被广泛地集成到大多数 ICS 系统中。这种集成带来了许多好处，但是同时也增加了这些 ICS 系统的脆弱性。

由于独特的性能，可靠性和安全性的要求，保护 ICS 往往需要适应和扩展到 NIST 开发的安全标准和指导方针中以保护传统 IT 系统。本次修订的一个显著内容是一个新的 ICS 覆盖提供定制的指导，如何适应与应用安全控制及加强控制，特别出版物 SP800-53 包含了一个安全控制目录，可定制以满足特殊需求，某组织的使命，操作环境，或特定技术的使用。

1.2.1 国际安全形式的变化

世界各国高度重视工业控制系统的信息安全，美国、欧盟、日本等发达国家纷纷加大力度研发涉及工业生产运行的相关设备和网络的安全防护技术：

2013 年 2 月

美国总统发布了总统行政命令 13636 号，制定了“NIPP 2013 美国国家基础设施保护预案”，旨在建立国家基础设施的安全，维护网络环境，管理网络安全风险。

2013 年

欧盟发布了 COM (2013) 48—— 关于 NIS （Network and Information Security 网络与信息安全）指令的提案，该提案在 2009/140/EC 指令的基础上为网络运营商建立了安全要求。欧盟 2009/140/EC 指令是“公共网络运营商和服务商对安全风险和安全措施的管理”，以保障网络和服务的安全性。

2015 年

IEC 将建立网络安全评估，也就是检测与认证计划。这是针对产品生产商、供应商 / 系统集成商、运营商 / 资产拥有者的一套基于 IEC 62443 标准的网络安全评估体系； 是对产品、流程和人员的网络安全认证。对工控系统网络安全的检测与认证，能为资产拥有人提供保障，证明他们的产品符合 IEC 国际标准，符合基本的安全要求；同时也意味着产品的认证报告将被全球 60 多个国家认可。

2014 年 3 月

卡塔尔国发布了国家 ICS 安全标准。
国际标准 IEC62443 系列：这是国际电工标准委员会 IEC 制定的一套关于“工业通信网络和控制系统供应链的网络安全风险”的标准。

日本工控系统攻防实景模拟基地

根据日本情报处理推进机构 (IPA) 的数据显示，在 2014 财年，针对日本发电厂和其他核心基础设施的网络攻击多达 1257 起，较上年猛增 200%。陡然增长的数字表明，日本正在成为最容易遭受攻击的目标。

日本经济产业省下属的日本控制系统安全中心（CSSC）于 2013 年 5 月在日本宫城县多贺城市建立了“东北多贺城总部”，以日本控制系统安全中心（CSSC）为核心，由日立、东芝在内的 18 个团体共同发起，总共投入 20 多亿日元，具备 7 种类型的控制装置和系统。该总部内，模拟建设了各类火力发电站、化工厂、汽车制造等工厂基础设施中所使用的工业机器人、楼宇空调和照明系统。同时，单独开设“红队房间”，让技术人员模拟进行网络攻击，使生产设备错误操作或者中止。用以培训技术人员维护工场、发电站等工业控制系统安全的技能。这个场所是日本首个实景网络攻击的模拟攻防场所，培训人员通过体验网络攻击，了解系统的弱点，从而掌握防御技能。

攻击软件采用了美国国防部使用的网络攻防演习系统，能够进行 300 多种各类攻击的实战演练。日本还计划在未来研究中每年为此投入 5 亿日元。

1.2.2 国家政策的指引

自从工信部 451 号文发布之后，国内各行各业都对工控系统安全的认识达到了一个新的高度，电力、石化、制造、烟草等多个行业，陆续制定了相应的指导性文件，来指导相应行业的工控安全检查与整改活动。国家标准相关的组织 TC260、TC124 等标准组也已经启动了相应标准的研究制定工作。具体情况如下：

政策法规

- 工信部 451 号文《关于加强工业控制系统信息安全管理的通知》
- 国家发改委 14 号令《电力监控系统安全防护规定》
- 国能安全 36 号文《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》
- 国家烟草局《烟草工业企业生产区与管理区网络互联安全规范》等

国家标准

2014 年 12 月 2 日，全国工业过程测量控制和自动化标准化技术委员会 (sac/tc124) 发布了工业控制系统推荐性国家标准 GB/t30976.1 ～ .2-2014《工业控制系统信息安全》（2 个部分），主要包括：

- GB/t30976.1-2014—工业控制系统信息安全第 1 部分：评估规范；指导针对工控系统进行安全评估。
- GB/t30976.22014—工业控制系统信息安全第 2 部分：验收指南；指导对工控系统进行上线前的安全检测。

标准草案

在安标委的指导下，正在草拟的工控安全相关标准主要包括：

- 《信息安全技术工业控制系统安全管理基本要求》
- 《安全可控信息系统（电力系统）安全指标体系》
- 《信息安全技术工业控制系统信息安全检查指南》
- 《信息安全技术工业控制系统安全防护技术要求和测试评价方法》
- 《信息安全技术工业控制系统信息安全分级规范》
- 《信息安全技术工业控制系统测控终端安全要求》

在公安部的指导下，正在草拟的工控安全相关标准主要包括：

- 《工业控制系统信息安全等级保护设计技术指南》
- 《工业控制系统信息安全等级保护基本要求》
- 《工业控制系统信息安全等级保护测评指南》

与此同时，2014 年 12 月 1 日 “工业控制系统信息安全技术国家工程实验室”在京正式揭牌成立。该实验室是在中央将网络安全和信息化上升到国家战略的背景下建立的，由中国电子信息产业集团第六研究所承担建设任务，针对我国工业控制系统面临的日益严重的信息安全攻击威胁等问题，围绕涉及国计民生的重点工业和军事领域，建设我国自主的工业控制系统信息安全技术研发与工程化平台，开展关键技术和产品的研发和产业化。

通过实验室开展工控信息安全关键技术研发、标准规范制定和课题研究，建立工控信息安全领域发展趋势和重大问题研究机制，加强产、学、研、用在优势资源上的协同与集成，促进技术创新与产业孵化，致力改变我国高端工控系统及核心部件由国外进口的现状，实现工业控制系统“可发现、可防范、可替代”，建立我国自主的工控安全防护体系，提升工控安全核心竞争力。

1.2.3 工业控制系统安全需求的变化

图 1 对 2015 年发生的工控安全事件中，入侵工业控制系统所使用的关键技术进行了统计，网络钓鱼仍然是被经常使用的攻击方法，因为它是相对易于执行和有效的。通过弱身份验证技术所发生的入侵仍处于一个比较高的比例，网络扫描和 SQL 注入的尝试也保持较高的比例。作为资产所有者应确保他们的网络防御措施能够解决这些流行的入侵技术。

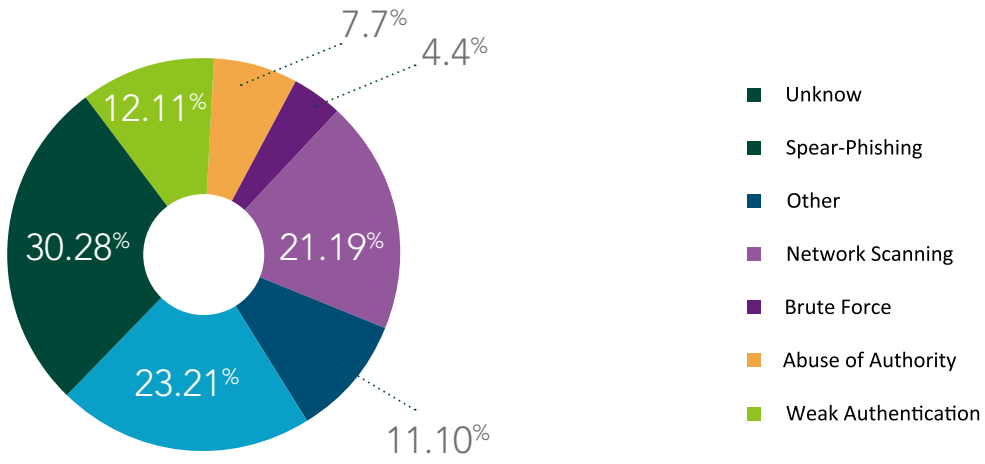
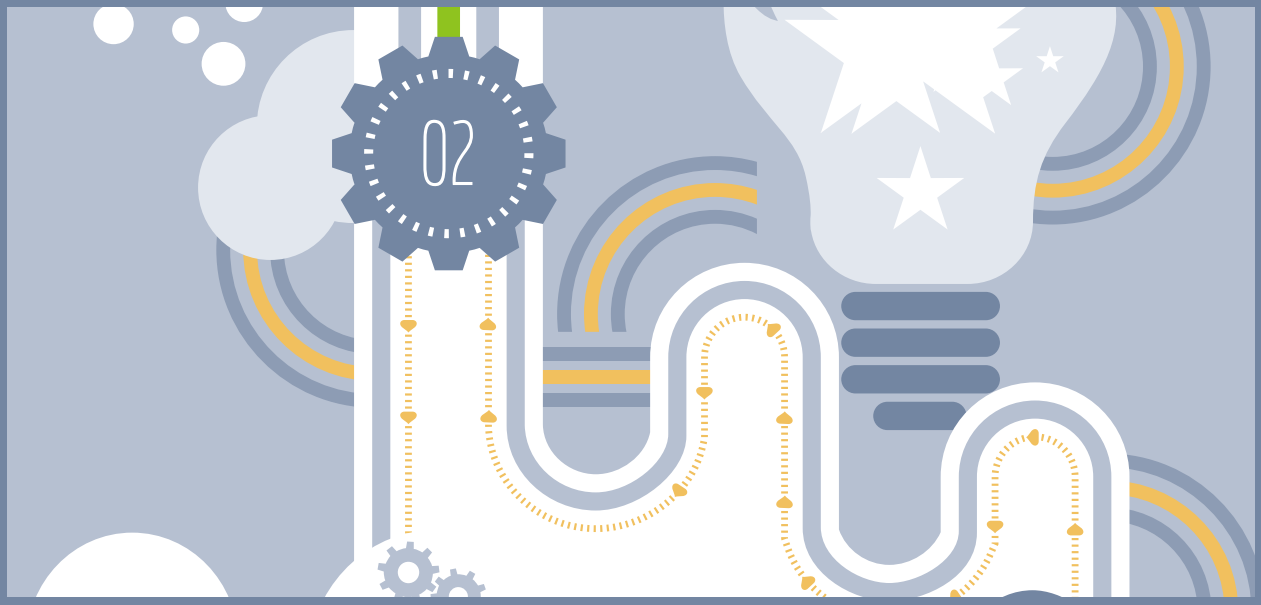


图 1 FY-2015 Mid-Year: Attempted Infection Vector.[①]

① 引用自：ICS-CERT 的 2015 财年半年报

02 工业控制系统安全技术演进路线图



工业自动化控制系统正逐渐从封闭、孤立的系统转化为开放互联的系统，工业自动化生产开始在所有网络层次上横向与垂直集成；将工业自动化控制网络与 IT 网络相连，以及为实现远程维护与 Internet 连接；越来越多地采用开放标准以及基于 PC 的系统。工业自动化生产领域在享受开放、互联技术带来的技术进步、生产率提高与竞争实力大大增强的利益的同时，也面临着越来越严重的安全威胁。

2.1 攻击技术路线

结合 ICS-CERT 往年安全事件的统计数据分析的结果可知，近年来，工业控制系统相关的安全事件正在呈快速增长的趋势，且这些事件多分布在能源、关键制造业、市政、交通等涉及国计民生的关键基础行业。这与关键基础行业对于现实社会的重要性及其工控系统的自动化、信息化程度较高有着紧密的关系。

由于大部分工业控制系统安全事件的相关报道和曝光程度相对较低，根据公开的信息整理了部分近年来的工业控制系统安全事件列表如下，由此可以看出 ICS 攻击技术路线大致演变过程：

时间	事件简介
2000 年	澳大利亚昆士兰新建的马卢奇污水处理厂出现故障，无线连接信号丢失，污水泵工作异常，报警器也没有报警。本以为是新系统的磨合问题，后来发现是该厂前工程师 Vitek Boden 因不满工作续约被拒而蓄意报复所为。
2003 年	美国俄亥俄州 Davis-Besse 核电站和其它电力设备受到 SQL Slammer 蠕虫病毒攻击，网络数据传输量剧增，导致该核电站计算机处理速度变缓、安全参数显示系统和过程控制计算机连续数小时无法工作。
2006 年	美国阿拉巴马州的 Browns Ferry 核电站 3 号机组受到网络攻击，反应堆再循环泵和冷凝除矿控制器工作失灵，导致 3 号机组被迫关闭。
2007 年	攻击者入侵加拿大一个水利 SCADA 控制系统，破坏了取水调度的控制计算机
2008 年	攻击者入侵波兰某城市地铁系统，通过电视遥控器改变轨道扳道器，致四节车厢脱轨。
2010 年	西门子首次监测到专门攻击该公司工业控制系统的 Stuxnet 病毒，也称为震网病毒。
2010 年	伊朗政府宣布布什尔核电站员工电脑感染 Stuxnet 病毒，严重威胁核反应堆安全运营。
2011 年	黑客入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统的供水泵遭到破坏。
2011 年	微软警告称最新发现的“Duqu”病毒可从工业控制系统制造商收集情报数据。
2012 年	两座美国电厂遭 USB 病毒攻击，感染了每个工厂的工控系统，可被窃取数据。
2012 年	发现攻击多个中东国家的恶意程序 Flame 火焰病毒，它能收集各行业的敏感信息。
2013 年	美国著名黑客巴纳比·杰克在旧金山突然神秘死亡，巴纳比·杰克生前的“明星事件”回顾： 1. 利用他独创黑客技术令自动提款机狂吐钞票 2. 扫描方圆 100 米之内的所有胰岛素泵，识别它们的注册码，将这些注册码程序化，并将它们分配给全部 300 个单位的胰岛素，对于一型糖尿病患者来说，这是很容易致命的。 3. 9 米之外入侵植入式心脏起搏器等无线医疗装置，然后向其发出一系列 830V 高压电击，从而令“遥控杀人”成为现实。
2014 年	“蜻蜓组织”利用恶意程序 Havex（与震网类似），对欧、美地区的一千多家能源企业进行了攻击。
2015 年	……

表1 近年来发生的工控安全事件

通过对大量工业控制系统信息安全事件的分析，我们发现大多数的工业控制系统信息安全事件影响范围和危害程度较大，且在此类事件中显露出来的攻击思路和攻击视野在一段时间内会带来示范效应。结合传统 IT 系统的攻击演变过程，总结出工业控制系统的攻击路线图。

图 2 工业控制系统攻击路线图

- **攻击目标演变：**攻击目标明确，通常针对关键基础设施和重要机构。
- **攻击者水平：**攻击代码愈加专业化，个人很难开展，黑客组织（竞争对手、工业间谍、尤其是有某些国家幕后支持的黑客组织）已成为当前工控系统所面临的主要攻击发起者。
- **攻击时间演变：**攻击事件持续时间很长，甚至长达数年；
- **攻击态度演变：**攻击者逐步变为极具耐心，不断尝试，一步一步获取目标系统的权限，然后长期蛰伏、收集信息，如此反复。
- **攻击手段演变：**由破坏通信过程，引起上位机与下位机通信中断，到通过控制上位机恶意下装引起控制器运行逻辑问题，到通过综合应用 IT 和 OT 结合的攻击手段引起上位机和下午整体逻辑异常，到通过攻击供应链提前预制恶意软件达到对控制系统进行攻击的目的。
- **攻击范围扩大：**攻击者关注的范围，由市政、电力等基础设施扩大到油化、冶金、制造业、智能部件、物联网等范围。

2.2 工控安全技术的发展

目前在役的工业控制系统大多是上个世纪末期开始研制的，由于当时的工业控制系统大多采用专用实时操作系统、Arcnet、FDDI 等网络设备和令牌环、令牌总线等特殊的网络协议，整个系统相对封闭，受到入侵的可能性不大。同时由于设计人员普遍缺乏信息安全的意识，在系统架构方面基本上没有考虑信息安全设计。

工业控制系统虽然长期“带病运行”，直到 2010 年左右 Stuxnet 蠕虫为代表的 ICS 信息安全事件使人们开始重视工业控制系统安全，也正是从这一时期开始，工业控制系统安全逐步被重视，大多数安全组织特别是国家力量开始对工业控制系统的安全性进行研究，同时不少工业控制系统厂家都对原系统进行升级，但这些升级大多属于局部修改，未能全面考虑信息安全问题，导致了信息安全风险的逐步扩大。

工控系统安全技术的发展看，目前工控系统的安全防护主要以边界防护为主。早期通过 IT 防火墙或者网闸等产品，通过基于 IP 的策略来为工控系统提供安全防护，同时部分工控系统辅以入侵检测设备来对进入工控系统的流量进行审

计。从实际的应用的效果看，通过基于访问控制规则的防火墙技术可以在边界处有效的过滤对工控系统的访问流量，但是，通过 IT 防火墙缺乏对控制系统包的深度过滤，针对工控系统的攻击流量在加入到正常通信流量中时，往往缺乏有效的识别，一旦攻击流量进行工控系统基本是可以在系统中“肆意而为了”；现阶段工控网络的边界处部署的防护措施网闸是也一种常用的技术手段，网闸来实现生产控制系统与信息系统之间的隔离。通过网闸可以单向限制信息系统向工控系统的数据传输，可以实现通过通信的双向认证实现对工控系统的防护，经历了几代技术的发展，网闸实现了基于单比特数据响应和验证，由于数据格式内容的固定及数据传输输出字节数量的限制，可以保障传输数据的可靠性。

伴随着工业控制系统安全技术的发展，针对工业控制系统本身需求的工业防火墙出现了，比较早的引入国内的多芬诺工业防火墙是国内较早采用工业防火墙，国内厂商陆续推出了工业防火墙，传统防火墙以黑名单策略配置为主，生产控制系统操作中相关的指令操作生产系统中黑名单潜在导致生产操作中断的风险，工业防火墙大多采用白名单机制，通过对已知的操作过程进行定义过滤掉非法的操作和指令等。从现有的工业防火墙产品看不但支持商用防火墙的基础访问控制功能，更重要的是它提供针对工业协议的数据级深度过滤，实现了对 Modbus、OPC、S7 等主流工业协议和规约的细粒度检查、过滤，以针对工控协议的设备地址、寄存器类型、寄存器范围和读写属性等进行检查，可防范各种非法的操作和数据进入现场控制网络。针对传统隔离装置无法深度解析工业控制系统的规约和协议的协议，无法基于寄存器地址和控制过程进行精细处理的情况，工业网闸技术除了具备隔离隔离装置的技术特性外，还可以实现对工业控制现场的每个测点赋予“只读”或“读 / 写”两种不同的权限。当设为“只读”权限时，所有数据回置操作被禁止从而实现单向数据传输，达到保护现场设备安全的目的。

从行业上看，电力工控系统（电力监控系统）同一生产环境中的不同区域之间采用单项隔离装置来实现不同区域之间的隔离，在于其他生产环境之间联系的数据通道上仍然是采用了传统的 IT 防火墙进行隔离，通过策略限制 IP 通信和限制传输传输端口，同时依赖于数据通道的加密措施和相关前置机本身具有的数据处理和查询机制的安全保障来提升系统的安全性。石油和石化领域中部分生产企业已经使用了工控防火墙做生产系统与信息系统之间的隔离，部分企业采用了工业防火墙做同一生产区域的不同安全区域之间的安全隔离；部分钢铁和关键制造业中也采用了工控防火墙做相关区域的隔离，但是还没有形成一定的规模效应。烟草行业中存在多用应用形式，有 IT 防火墙、工业防火墙和网闸，但是都还没有形成大规模的应用。

从工业控制系统安全事件看，单纯的边界安全防护技术已经不能够解决工业控制系统所面临的安全问题，相关的防护技术已经向纵深防护的方向发展，从工业控制系统的安全生命周期的角度来考虑工业控制系统的安全。从漏洞的挖掘→漏洞检测→工控审计→工业蜜罐（蜜罐场）→未知威胁检测→态势感知→综合预警的方向发展，以及综合应用相关技术来提升工业控制系统所面临的安全威胁。从研究力量上看，原有的信息安全企业、研究机构和大学已经开展了针对研究，工控系统的企业、研究机构和大学也在逐步开展针对工业控制系统的安全研究，但是，从整个产业的发展看，整体工业控制系统安全的与工业控制技术在融合方面还有一段距离。

工业控制系统为了保障业务的稳定运行，也开发了大量的功能安全功能，功能安全的技术，通过多点失效保障与表决机制等，来保障执行一个关键操作，其中更多是防止误操作对工业控制系统的影响，而功能安全所具备的失效保障的措施，在应潜在的对外部攻击所导致的功能失效方式也起到一定的作用。但是，随着工业控制系统信息化的程度的加深，必然导致了工业控制系统受攻击面在增多，融合实际的操作规程要求、融合实际的功能安全属性、基于业务的流程与工艺的行为建模和分析，形成信息安全技术手段与业务有机的融合的技术，才能在工业控制系统信息安全领域实现真正的突破。

另一方面随着智能电网、中国智造、能源互联网、中国制造 2025 等新型业务形态的出现，一些新的业务运行的形势的出现，如智能发电、虚拟电站、智能风电、智能工厂、云工厂等出现，使业务系统之间的交叉和连接关系变得更加复杂。传统控制系统的边界已经开始变得不那清晰，原有的以边界防护为主手段的防护体系必将面临的重大挑战。融合工控安全技术、虚拟化安全技术、云安全技术、大数据等技术的防护体系会成为未来工控安全发展的一个重要方向。

2.3 总体安全保障框架

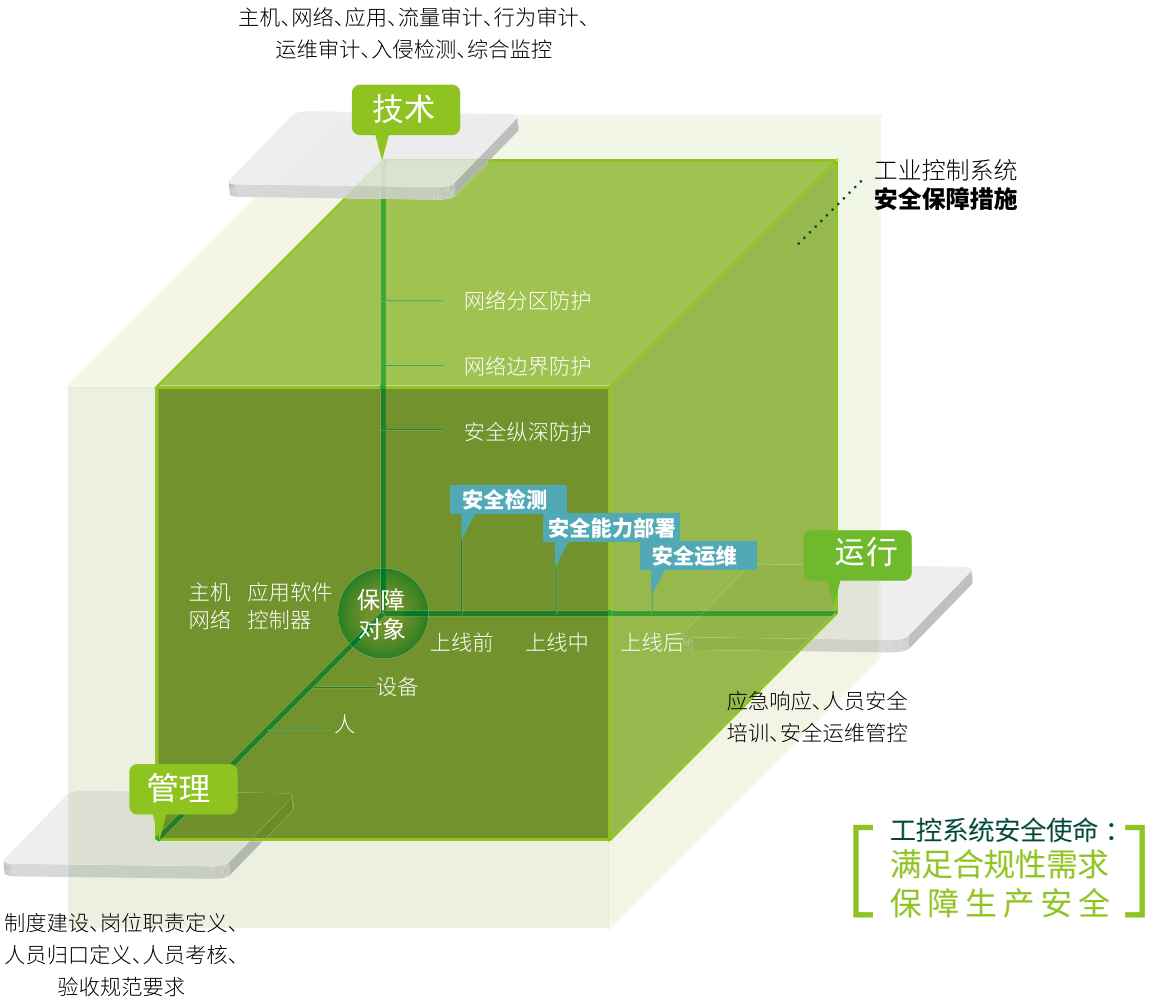


图 3 总体安全保障框架

基于绿盟科技对工控系统安全需求的理解，结合国内工控安全的规范要求及国外相关标准内容，绿盟科技提出从技术、管理和运行三个维度来保障来保障工业控制系统安全。三个保障维度中主要包含：网络边界防护、安全纵深防护、安全运行管理和安全管理制度要求等几个方面，融合了技术、管理和运行的要求来保障工业控制系统的安全。同时，我们结合工业控制系统运行阶段的特点，提出了针对工业控制系统的三个能力建设，包含从上线前的安全检测、安全能力部署、安全运行三个阶段，覆盖工业控制系统运行周期的安全保障。

2.4 电力行业工控安全解决思路 / 保障框架

从电力行业对工控安全需求看，电力企业在主要是以合规性建设为主，在 2004 年原电监会 5 号令颁布开始，大部分的电厂控制系统安全建设已经按照 5 号令的要求进行了整改，形成“安全分区、网络专用、横向隔离、纵向加密”的防护体系。从整体电力行业工控系统防护情况看，电网整体的防护水平要优于发电侧，而且从发电企业情况看，发电企业相对比较分散，造成在发电控制系统安全建设水平方面存在较大差异性。

本文中描述的内容，主要以在我国供电形式中占比最高的火电控制系统的安全需求为例，来说明发电企业在工控安全建设方面的思路。

2.4.1 火电控制系统逻辑架构

发电控制系统从业务功能范围来说，主要分为主控系统、辅控系统和网控系统。主控系统系统完成对锅炉、汽机的控制，辅控系统主要完成化水处理、除尘、输煤的处理。主控系统主要采用 DCS（分散式控制系统），辅控系统主要采用 PLC 进行控制，网控系统主要负责电厂电气运行情况的监控，通过远动装置接受电网的指令，通过 AGC 和 AVC 下发到发电机，来实现功率增减和励磁的调整，同时为升压站的运行提供控制。

从逻辑上来说，系统中主要承载几种类型的信息：控制信息（操作员站下达要求智能设备执行相关动作的指令），数据信息（遥测、遥信），配置信息（获取相关 I/O 卡键状体的信息），组态信息（系统中相关业务逻辑变更的信息）。主控主要通过 DPU 完成对相关被控设备的控制，辅控主要通过与 PLC 的通信实现整个控制流程的过程。具体如图 4 所示:

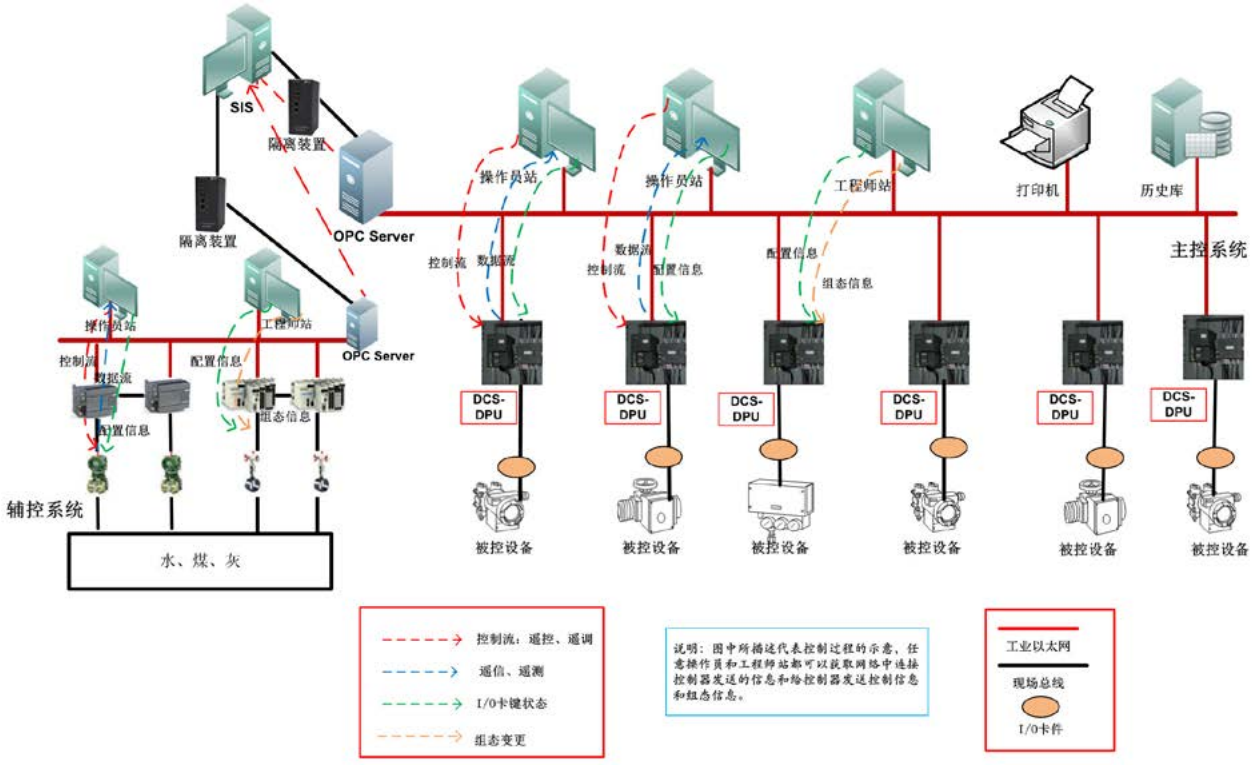


图 4 火电厂主控与辅控系统逻辑架构图

网控系统（NCS）主要实现对升压站的监控和实现与 DCS 采集信息的传输（主要实现 AGC 和 AVC）。网控系统主要分为站控层、间隔层和过程层。

- **站控层设备：**主机兼操作员工作站、一体化平台主机、远动通信设备、智能接口设备、故障录波及网络分析、网络交换机。（其中还有打印机、音响音响告警输出装置）
- **间隔层设备：**间隔层都是 I/0 测控装置。I/O 测控装置具有状态量采集、交流采样及测量、防误闭锁、同期检测、就地断路器紧急操作和单接线状态及数字显示等功能，对全站运行设备的信息进行采集、转换、处理和传送。I/O 测控装置还应配置有 “就地 / 远方” 切换开关。
- **过程层设备：**过程层设备包含智能终端、合并单元及智能一次设备接口等。可完成对断路器、隔离开关的信号采集、处理和控制，以及互感器采样值信息的采集和处理。

主要通过控制信息实现对一次设备的控制、信息采集和继电保护。如下图所示：

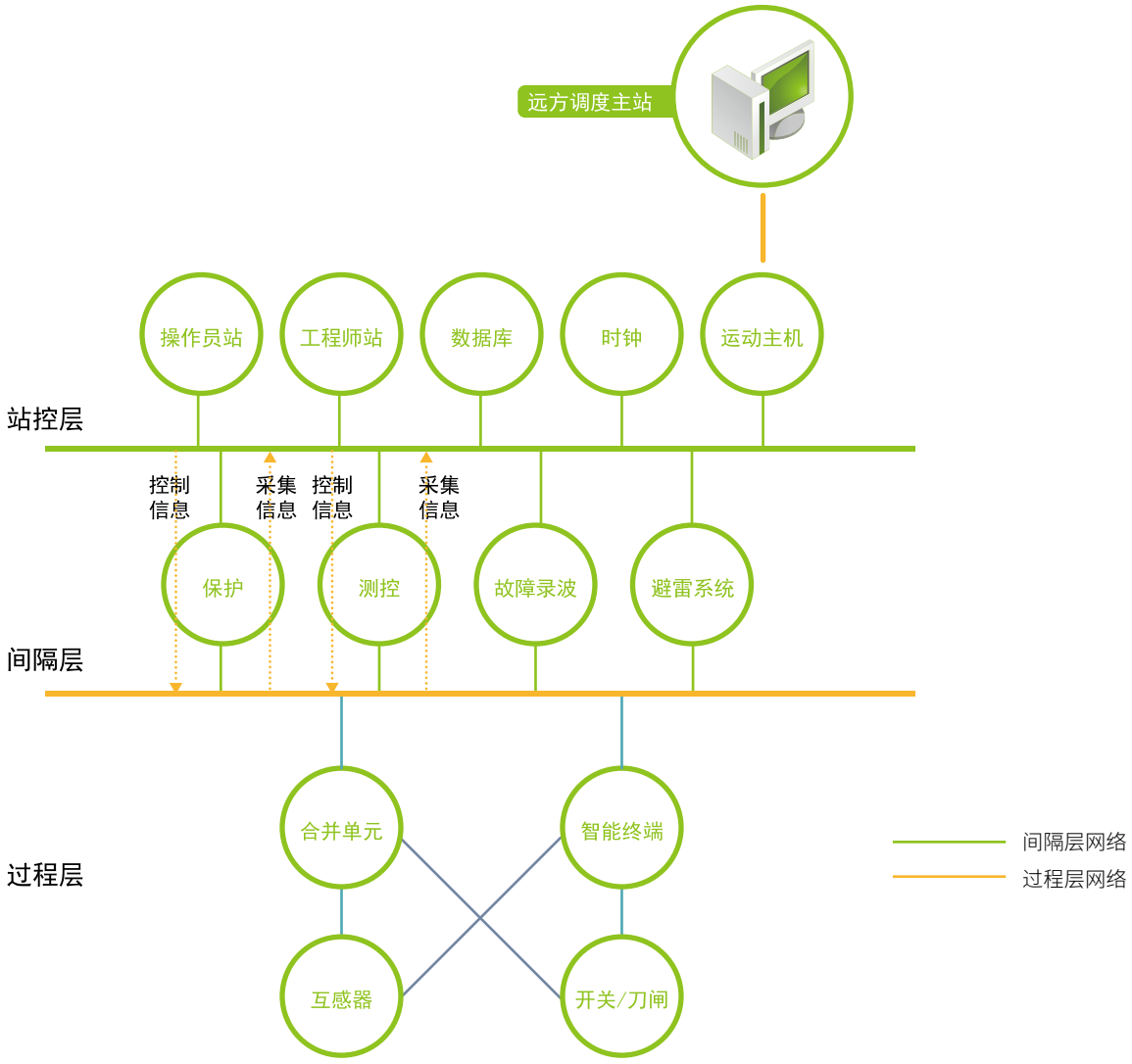


图 5 火电厂NCS逻辑架构图

2.4.2 主要控制系统之间的逻辑关系

DCS 和辅控系统之间可以通过网络或者硬接线连接，辅控向主控提供相关数参数。ＮＣＳ与主控之间实现双向的通信，ＮＣＳ可以通过向主控的ＡＧＶ和ＡＶＣ来控制发电机组的出力。ＮＣＳ向ＤＣＳ提供相关的数据，ＤＣＳ向ＮＣＳ提供相关的数据。相关控制系统的数据通过ＯＰＣ，通过隔离装置摆渡到镜像服务器，ＳＩＳ系统通过读取镜像服务器信息来进行相关生产流程优化处理和生产系统的环境的运行情况展示。

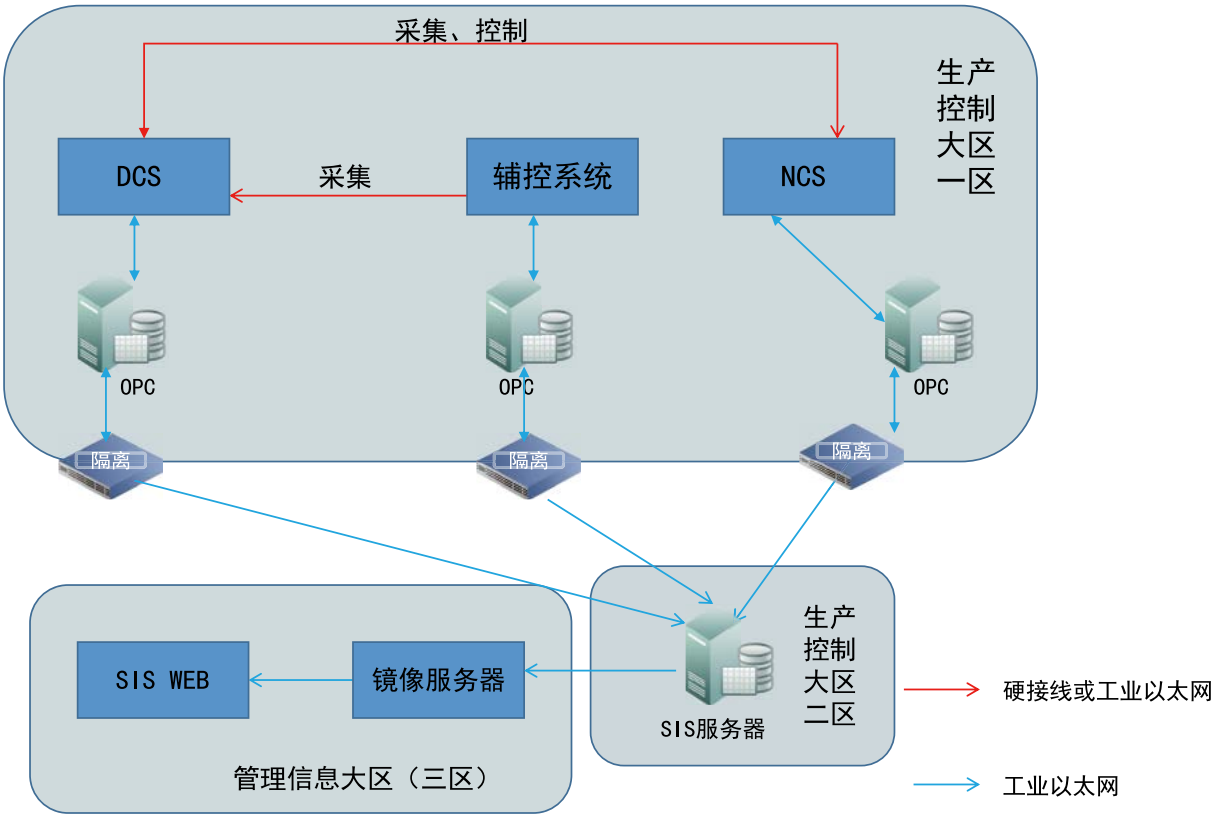


图 6 火电厂NCS逻辑架构图

2.4.3 发电控制系统面临的主要安全威胁

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。

与通用 IT 信息系统安全需求不同，工业控制系统设计需要兼顾应用场景与控制管理等多方面因素，以优先确保系统的高可用性和业务连续性。在这种设计理念的影响下，缺乏有效的工业安全防御和数据通信保密措施是很多工业控制系统所面临的通病。

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，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。

缺乏有效的安全策略部署。

工业控制系统与信息系统之间缺乏有效的隔离措施，即使采用了隔离装置等隔离措施，也存在安全策略设置不当的问题，造成信息系统的威胁可以畅通无阻的进入到工控系统中。同时在边界处缺乏有效的威胁检测手段，外部的威胁可以悄无声息的进入到系统中。现有的安全设备缺乏相关的工控识别能力，对于工控报文缺乏有效的解析，在部署的环境中极容易引起生产系统的生产中断。

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。

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。工业控制系统相对封闭的环境，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。

但电厂现实环境中缺乏针对工业控制系统的安全日志审计及配置变更管理。这是因为部分工业控制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。

外部运维带来的安全风险。

由于工控系统采用的控制器和设备的种类繁多，外部人员运维成为一个潜在的安全风险点。某些电厂已经通过工作票的机制来从管理上保障运维过程的可管理，但是在没有有效技术手段支撑的情况，本地管理人员很难监测到外部人员的越权操作或者故意改变运行逻辑的行为，在出现问题时，也很难去追踪。

移动介质缺乏有效管控。

工业生产环境中存在备份导出生产数据的需求，移动介质是一种比较好的满足生产环境数据备份的介质。但是在介质的使用在管理方面普遍存在安全隐患，文件拷贝的介质无法做到专盘专用，可以采取的安全措施只限于使用杀毒软件对全盘进行扫描。而杀毒软件是针对已知病毒的查杀，并且主要针对传统的信息系统，而对于未知病毒的检测和工控特定病毒的检测基本上无能为力。从已经发生的安全事件看，移动介质是一个重要的传播恶意代码到工控环境的手段。

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，会与业务的过程进行贴合，攻击过程强调技术的精心组合与攻击者之间的协同。一旦进入到目标系统后，为了达到有效的攻击，会持续寻找攻击的宿主目标，而且攻击过程缓慢，对潜在系统的影响具有渐进、持续、不易被发现的特性。

现有的技术手段很难有效的发现 APT 攻击。在工业现场普遍缺乏防护手段和现有工业控制系统安全防护产品不够成熟的情况下，需要把业务的运行过程与相应的防护手段结合，运用综合的防护手段（包含技术、管理和人员），降低由于 APT 攻击给工业控制系统带来的安全隐患。

工控安全管理职责定义不清。

电厂工控系统的管理归口到相关的生产业务部门，信息安全管理归口到信息化部门。当工业控制系统涉及信息安全问题时，由于生产技术部的人员缺乏信息安全知识，而信息化部门的人员对工控系统业务了解不足，组织内部缺乏两个部门之间的协同、合作机制，可以把信息安全和工控安全进行结合。在遇到安全事件时，无法对事件做详细的定位，只能基于业务的运行逻辑定位为相关的功能安全事件或者误操作事件，无法对其中可能潜在信息安全要素进行分析和排除，造成潜在的安全隐患就残留在系统中，为日后的安全带来了极大的隐患。

系统建成验收过程中缺乏信息安全的环节。

由于工业控制系统设备到货周期长，设备一般直接投入使用，很少进行详细的验收测试，只是做基本功能验收，但不会涉及信息安全的验收环节。由于工控设备以强调工控实现为主要目标，基本不会考虑信息安全需求，可能会把安全隐患留在工控系统中，如果外部的安全威胁获取到相关的信息后，就有可能对系统带来极大的，甚至可能是致命的影响。

没有足够的安全政策、管理制度，人员安全意识缺乏。

电厂针对生产业务制定了相应的管理制度、管理流程，但未制订完善的工业控制系统安全政策、管理制度和操作规程，未形成全面的信息安全管理制度体系。给工业控制系统信息安全管理工作带来极大的隐患。

随着工业控制系统在国计民生中的重要性日益凸显以及 IT 通用协议和系统在工控系统的逐渐应用，人员安全意识薄弱成为导致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使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）。

2.4.4 安全防护的原则

在方案构建时，充分参考遵循发改委 14 号令对发电厂安全防护建设的要求，从管理、技术等方面的具有要求中体现出防护的思路。

在方案构建时，以安全审计作为主要的安全防护方向，以管理制度和人员职能的明晰化定义，为主要的安全管理建设方向；对于新建电厂需要充分考虑在安全防护方面要符合 14 号令对电厂安全建设的要求，在方案中落实 14 号令在安全建设方面的具体防护措施和管理要求，同时考虑在系统验收环节、系统运行、系统维护和系统检修环节中的安全防护。

对于工控系统的安全防护，在符合了相关政策（14 号令要求，电力等保）要求的基础上，需要进一步考虑符合电厂控制系统生命周期的安全防护要求。逐步完善发电厂工控的安全防护措施，使发电厂工控系统安全防护由安全策略的部署向安全能力的部署能力迁移，逐步实现安全技术能力、安全管理能力的全面提升，实现管、控、防一体化。安全能力逐步覆盖从系统上线、系统运行、系统运维、系统检修等各个环节，实现工控系统安全的闭环管控。如下图所示：

图7 工控系统安全闭环管控

2.4.5 安全防护的思路

2.4.5.1 合规性安全建设

依据国家发改委【2014】14 号令要求，电厂的安全防护我们建议从物理安全、网络安全、主机安全、应用和数据安全等多个维度进行考虑。安全防护框架如图 8 所示。

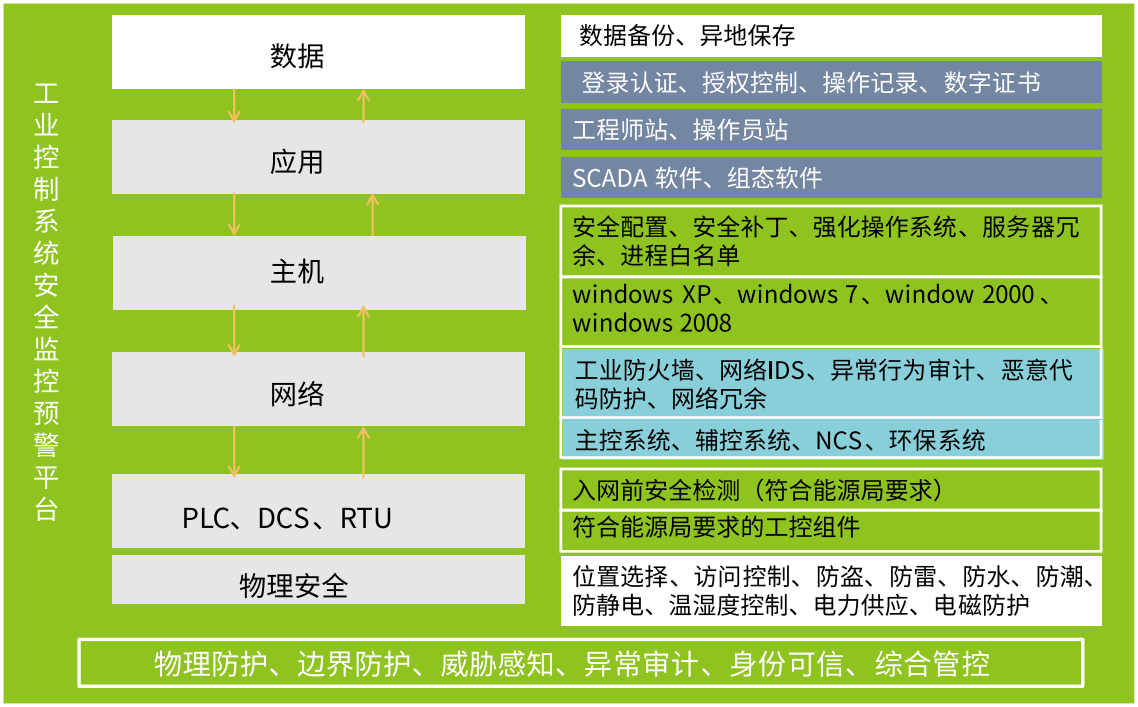


图8 安全防护框架

物理安全策略的目的是电力监控系统等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限、防止用户越权操作；确保电力监控系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入电力监控系统相关区域和各种偷窃、破坏活动的发生。

网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。电力监控系统的网络安全主要是指网络信息信息的完整性、保密性和可用性。

主机安全其核心内容包括安全应用交付系统、应用监管系统、操作系统安全增强系统和运维安全管控系统。它的具体功能是保证主机在数据存储和处理的保密性、完整性，可用性，它包括硬件、固件、系统软件的自身安全，以及一系列附加的安全技术和安全管理措施，从而建立一个完整的电力监控系统主机安全保护环境。电力监控系统主机包括各种服务器、操作员站等各种以计算机为主体的设备。

应用安全，顾名思义就是保障应用程序使用过程和结果的安全，就是针对应用程序或工具在使用过程中可能出现计算、传输数据的泄露和失窃隐患，通过其他安全工具或策略来消除。

数据安全有多方面的含义：

- 数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、双向强身份认证等。
- 数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。
- 数据处理的安全，主要是指如何有效的防止数据在录入、处理、统计或打印中由于硬件故障、断电、死机、人为的误操作、程序缺陷、病毒或黑客等造成的数据库损坏或数据丢失现象，某些敏感或保密的数据可能不具备资格的人员或操作员阅读，而造成数据泄密等后果。
- 数据存储的安全，主要是指数据库在系统运行之外的可读性，一旦数据库被盗，即使没有原来的系统程序，照样可以另外编写程序对盗取的数据库进行查看或修改。

2.4.5.2 安全能力提升

上线前的安全检测

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，立足于系统上线过程，基于验收规范的整体规程要求，通过对工控系统的安全性进行分析，发现系统中潜在的安全漏洞，基于发现的安全漏洞与相应的工控设备和系统提供商进行联系，获取相关的漏洞解决方案。漏洞的检测主要从已知漏洞的漏洞扫描如采用漏洞扫描技术和工控设备、系统主动漏洞挖掘技术等，来发现系统中潜在的安全隐患。

1. 漏洞扫描技术

- **主机层安全**
  该层的安全问题来自网络运行的操作系统：UNIX 系列、Linux 系列、Windows 系列以及专用操作系统等。安全性问题表现在两方面：一是操作系统本身的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是操作系统的安全配置存在问题。主要检查内容包括：
  - 操作系统（包括 Windows、Linux、UX、Solaris 等）的系统补丁、漏洞、病毒等各类异常缺陷；
  - 空 / 弱口令系统帐户检测，例如：身份认证：通过 telnet 进行口令猜测；
  - 访问控制：注册表 HKEY_LOCAL_MACHINE 普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录；
  - 系统漏洞：System V 系统 Login 远程缓冲区溢出漏洞，Microsoft Windows Locator 服务远程缓冲区溢出漏洞；
  - 安全配置问题：部分 SMB 用户存在薄弱口令，试图使用 rsh 登录进入远程系统。
  - 专用设备的安全隐患：如 PLC 采用 VXWORDS 系统，存在远程调用 WDB 漏洞。
- **网络层安全**
  该层的安全问题主要指网络信息的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性、远程接入、域名系统、路由系统的安全，入侵检测的手段等。主要检查内容包括：
  - 版本漏洞，包括但不限于设备操作系统存在的漏洞，涉及设备包括实验室所有在线网络设备及安全设备，并实施加固；
  - 开放服务，包括但不限于路由器开放的 Web 管理界面、其他管理方式等，并实施加固；
  - 空弱口令，例如空 / 弱 telnet 口令、snmp 口令等，并实施加固；
  - 网络资源的访问控制：检测到无线访问点；
  - 路由器：Web 配置接口安全认证可被绕过，交换机 / 路由器缺省口令漏洞，网络设备没有设置口令。
- **应用层安全**
  该层的安全考虑网络对用户提供服务所采用的应用软件和数据的安全性，包括：数据库软件、Web 服务、电子邮件系统、域名系统、交换与路由系统、防火墙及应用网管系统、业务应用软件以及其它网络服务系统等。主要检查内容包括：
  - 应用程序（包括但不限于数据库 Oracle、DB2、MS SQL，Web 服务，如 Apache、WebSphere、Tomcat、IIS 等，其他 SSH、FTP 等）缺失补丁或版本漏洞检测；组态软件存在安全漏洞。
  - 空弱口令应用帐户检测；
  - 数据库软件：Oracle tnslsnr 没有设置口令，Microsoft SQL Server 2000 Resolution 服务多个安全漏洞；
  - Web 服务器：Apache Mod_SSL/Apache-SSL 远程缓

冲区溢出漏洞，Microsoft IIS 5.0 .printer ISAPI 远程缓冲区溢出，Sun ONE/iPlanet Web 服务程序分块编码传输漏洞；

- 防火墙及应用网管系统：Axent Raptor 防火墙拒绝服务漏洞；
- 其它网络服务系统：Wingate POP3 USER 命令远程溢出漏洞，Linux 系统 LPRng 远程格式化串漏洞。

2. 主动漏洞挖掘

主要采用 FUZZ 技术来对工控设备进行健壮性测试，同时结合人工分析的手段，来发现现场工控设备在协议标准遵循度上的差异，来发现在协议安全性方面存在的漏洞。

- **异常行为检测**

  发电企业工业控制统是一个通过以太网或者总线形式连接的小型的局域网，网络相对来说较为封闭，厂站端与调度主站之间通信、DCS 不同 DPU 信息之间多采用专用的通信协议，但是，上位机软件与 DCS 通信多采用通用的 OPC 或者 MODBUS 进行通过，为了确保上位机与下午机的 DPU 之间通信的可靠性，在系统校验存在异常时或者网络问题导致的通信不畅时，多采用多次重传的机制，另一方面相关上位机与 DPU 之间通信之间交互存在潜在的未声明的通信端口。而对于工业环境中的网络设备一般不会基于业务的通信过程的安全性来考虑，网络的有效隔离，整个控制网络处于一个大的冲突域，在极端的通信环境中，有可能引起整个网络的广播风暴，一起网络通信的阻塞，最终一起 DPU 之间通信无法进行有效的通信，导致发电机组的故障，影响电网的稳定。从最近几年发生的发电侧的安全事件中已经出现了，网络广播风暴所导致的通信终端，最终引起发电机组故障，影响到区域性电网的运行。

  对于主控系统内流量的监测、辅控系统内流量的监测、主控系统与辅控系统之间流量的监测和现场总线的流量进行监控，形成通信过程中的流量基线，对于流量过载情况及时进行预警。同时，可以对于系统内出现的非正常通信规约的流量进行有效的监控预警，避免由于上位机无意开启的端口的通信行为，对网络流量带宽的消耗。另一方面，也可以通过网络异常流量的感知发现其中存在潜在的恶意行为提供分析参考依据。

- **主机进程的白名单**

  对于工控系统来说，上位机服务器对安装软件一般有比较的严格的限制，但是，移动介质和网络的通信的不可控因素的存在。另一方面，基于 windows 开发的易用性，多数上位机软件是基于 windows 开发的，并且普遍采用较早的 windows 系统，移动介质使用的不可控及运维过程的不可控都会为移动代码的执行制造了潜在的“温床”。对于上位机服务器安装相关的安全管控软件，建立可信的进程白名单，限制移动代码在控制系统的执行。安装在上位机的安全管控软件，一定要在实验环境中进行了充分测试，在确信不会对实际生产业务的运行产生影响的情况才能部署到实际的生产环境中。上位机的安全管控软件只允许白名单中的软件被执行（授权的组态软件等），只允许那些被认为安全和在“运行认可名单”中的程序和执行文件通过，反之将被阻止，从而实现系统保护。

- **基于行为的安全管控**

  工控系统中各个组件之间的通信需要按照相关的操作规程要求来建立相关通信的通道。并且不同的组件之间的通信行为和操作行为相对固定，如一个继电保护的开分闸操作只能在相关的操作规程要求下执行相关的动作，并且相关的动作可执行的范围是规程要求的范围。

  如在规程要求的范围外的操作，如执行定值修改的动作，如修改 PMU 的定值，完全可能引起电网中继电保护的连续跳闸甚至于引起越级跳闸的情况出现，甚至于引起电网的震荡。与规程结合的操作度量和构建一套基于行为的基线模型，在出现与规程操作不一致的操作时，系统应该可以对相关的高危操作进行告警，同时管控中心下发相关的管控指令到行为管控执行装置来阻断相关的高危操作，避免由于恶意操作所带来的生产安全事故。

- **工控安全综合管控系统**

  集中监控措施目的主要是采集并监测工业设备的调试信息与日志信息，采集相关网络设备和安全设备的日志信息，通过对设备重要性、安全威胁、安全脆弱性的综合计算，提供设备性能与日志的综合管理，关注于设备的运行状况与安全事件，在监管设备服务能力的同时分析是否存在异常的事件发生，协助运维人员快速解决故障及安全事件；对工控网络流数据进行采集与协议解析清晰呈现出网络行为的性质，及时发现网络中的异常通信行为，并支持流行为的历史追溯，增强对异常行为的检测与定位能力；综合的风险管理呈现当前网络中的主要威胁与脆弱性和当前安全状况。

2.5 石油、石化行业安全解决思路 / 保障框架

2.5.1 石油石化行业综述

石油石化行业分为上游、中游和下游。其中，上游从事的业务包括原油、天然气的勘探、开发，中游主要是油气的存储与运输，下游则涵盖炼油、化工、天然气加工等流程型业务及加油站零售等产品配送、销售型业务。通常情况下，将以石油和天然气为原料生产石油产品和石油化工产品的加工工业称为石油化学工业（简称石化工业），而其余统称为石油工业。

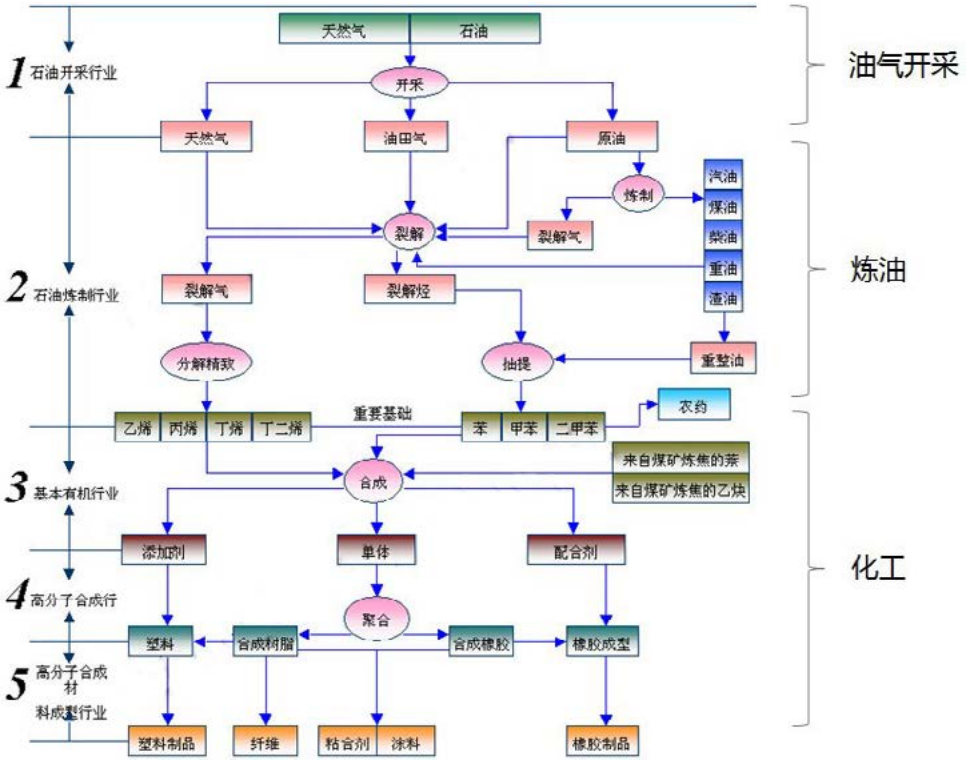


图9 石油石化行业分层

由于石油化工行业的业务工艺流程不通，上游的油气田开发和中下游的存储传输、化工炼化等在工业控制系统的组成和构建是不尽相同的，本章节主要是上游业务的油气田开发的工业控制系统的组成和环境重点针对 SCADA 系统的网络结构，介绍对于石油石化行业的工控安全解决思路。

2.5.2 油气田工业控制系统现状

油气田的工业控制系统建设以生产现场的生产数据采集和传输，以及安全监控为主，主要包括：生产单元的自动化数据采集及传输系统建设；覆盖生产场所的传输网络建设；各类站场的视频监视系统建设等。

油气田行业专业名词涉及如下：阀室、井站（油井站、气井站）、站场、监控中心和调度中心其涵盖范围如下：

- 阀室包括监控阀室和监视阀室；
- 油井站包括自喷井、抽油机井；气井站包括非高含硫无工艺单井、非高含硫单井、非高含硫丛式井、高含硫无工艺单井、高含硫单井，高含硫丛式井；
- 站场包括集气站、输气站、配气站、增压站、回注站和脱水站；
- 监控中心包括区域控制中心（RCC）、中心站（SCS）及其它有人值守站场的监控室；
- 调度中心包括地区调度管理中心（DCC）和总调指挥中心（GMC）

油气田企业的工业控制系统一般分三个层级，上级站提供全局范围内各要素的遥测服务、采油生产分析；中继站负责数据的采集和指令的下发；底层 RTU 实现现场数据采集和控制过程，并提供应急响应服务。实现油井图像实时采集、油井状况分析，并可远程对抽油机进行启停控制，注水井远程配注监控。一般由井场数据采集与控制系统、站点数据采集与控制系统、视频监控与闯入报警系统、以太网络传输系统及控制中心等系统组成。主要对油压、套压、产油量、注水量、含水率等生产工艺参数进行监控和采集，并通过生产管理系统采用实时数据库、历史数据库为分析和管理平台，实现对监控子系统的数据采集、存储、处理、异常分析、远程管理、异常报警。

油气田工业控制系统在结构上大致可分为总调指挥中心（GMC）、地区调度管理中心（DCC）、区域控制中心（RCC）、中心站监控室及部分井 / 站场监控系统等部分。根结规划的功能结构，具体业务需求及实现的不同，按四级架构进行分层：即应用层、调度层、监控层和现场层。而 SCADA 系统做为油气田生产信息化建设的一个重要组成部分，只涉及调度层、监控层和现场层三层，不涉及应用层，SCADA 系统的数据在 DCC 和非 SCADA 系统的数据汇聚后，统一提供给应用层，以便开发各种应用。整条体系通过对数据采集传输、视频图像监视、数据存储转出、数据发布及网络浏览、生产调度及管理等的优化完善，实现工艺流程和管理流程进一步优化，提升生产效率。

- **应用层：**主要指生产数据经过处理之后的应用部分，包括数据平台的应用展示、各种基于数据分析和数据解释的应用。企业办公网从数据平台读取的数据主要用于 OA、生产运行管理指挥系统等的应用。
  调度层：指油气生产物联网建设中主要行使调度功能的集中管理单元，是实现生产调度管理的重要平台。调度层通常指设置在分公司的总调指挥中心和设置在各二级单位的区域调度管理中心。
- **监控层：**指油气生产物联网建设中主要行使监控功能的集中管理单元，是实现生产监控、执行生产指令的重要平台。监控层通常指设置在作业区的区域控制中心、中心站监控室和站场监控室；
- **现场层：**主要指实现现场生产数据采集、物联设备状态采集、声光报警、入侵探测、工业视频监控、双向语音对讲及喊话、远程控制、状态检测及实时故障报警、电量检测及智能管理等功能的单元，包括现场仪表、RTU 控制器、控制柜、工业视频监控设备、双向语音对讲及喊话设备、声光报警设备、入侵探测设备、太阳能供电系统、电动阀、ESD 系统等。

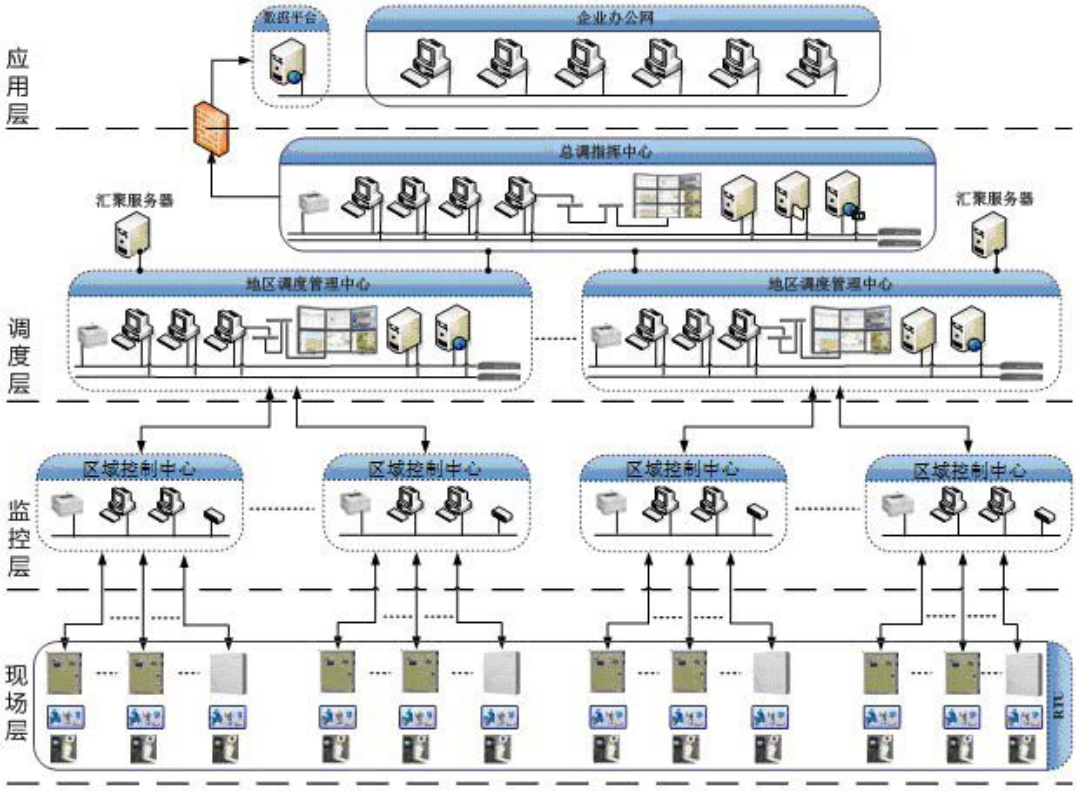


图10　油气田工业控制系统结构

生产信息化自动采集的生产数据与 SCADA 系统数据在作业区区域控制中心 RCC 进行融合，进入 SCADA 系统，通过 SCADA 系统上传至二级单位 DCC 的 SCADA 系统数据库，再经 DCC 的 SCADA 系统数据库上传至成都总调度指挥中心（GMC）和备用调度指挥中心（BGMC）。此外，在二级单位 DCC 系统数据库中所有的站场数据传输至设置在二级单位的生产数据平台数据库，再上传到位于总调度中心的生产数据平台数据库。所有生产数据和图片数据由生产信息网单向传输入办公网，由生产数据平台向各上层应用系统统一提供数据服务。在 SCADA 系统控制流传递模式上主要使用两种传递方式，分布式和集中式，两种模式可以并存，根据实际的油气田工业控制系统环境来选择不同的控制流模式。

SCADA 系统分布式控制流如下，SCS 实现就地控制，RCC 实行两级控制，SCADA 系统的控制流有两种模式，与数据流模式相关联，在两种模式中， GMC 均不实现控制，即控制流不到 GMC。

SCADA 系统集中式控制流如下，SCS 实现就地控制，DCC 实现远程控制，RCC 不实现控制功能，只实现数据监控功能。

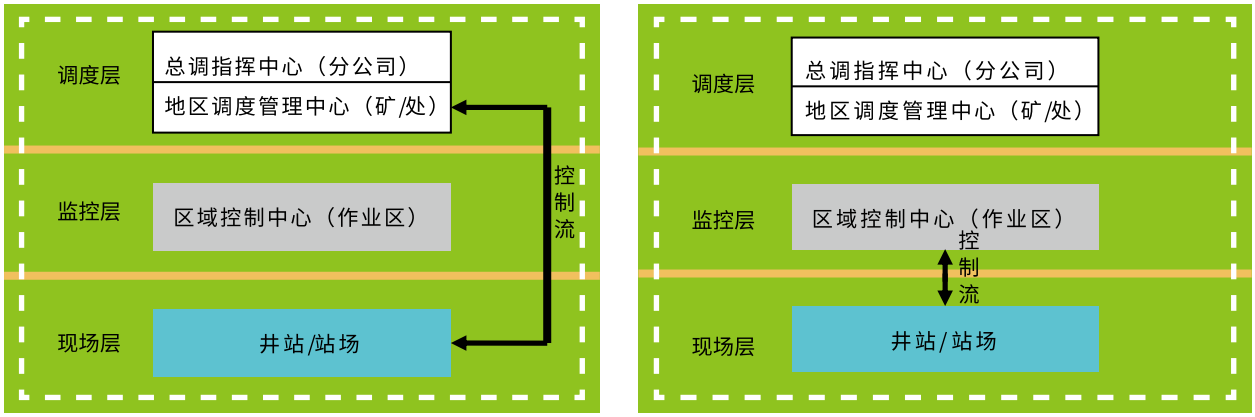


图11 SCADA系统控制流

2.5.3 安全风险分析

传统的工业控制系统，是孤岛式、封闭式的结构，只是在本企业或者本行业内部建立相对应的生产流程。同时，工业控制系统的要求，第一位是可用性，即生产设备能购完成生产所需；第二位是可靠性，就是要连续不间断的工作，而不会出现任何问题；第三位才是安全性。但是，随着信息技术的不断发展，两网融合的契机，特别是不断地在工业控制领域的推广，原本封闭孤岛式的工业控制系统变成了开放的形式。很多企业将生产环境转变为网络自动化形式，所有的设备都通过网络连接、搭建、管理和控制，很多工业生产现场都实现了完全的无人化，个别甚至将企业对外宣传和内部管理的网站同生产网络进行了互联，其间没有任何保护设备和防护措施。只是单纯的增加防火墙、网闸就可以有效的保护工业网络安全的想法，是不切实际的。

2000 年以后，在全球范围内，工控网络安全事件呈爆炸式增长。尤其在中国网络遭受黑客攻击增长 15 倍以上，其中 30% 是对国家基础设施，涉及天然气、运输、制造、医药、核设施以及汽车等众多行业，给国家和企业造成了大量的损失。

通过利用生产网络的漏洞，黑客轻而易举的入侵工控系统，轻而易举的进行漏洞挖掘和破坏，导致了很多安全事件的发生，而这些危险的发生主要由操作系统、应用系统、工控设备、网络通信协议、工业协议漏洞和移动介质等风险源造成。

2.5.3.1 操作系统漏洞

企业整个 SCADA 系统数据服务器多数采用 Unix 操作系统，工作站均采用 Windows 操作系统，由于工业控制网络与互联网及企业网络的隔离，同时为保证过程控制系统的相对独立性，以及考虑到系统的稳定运行，现场工程师未对 Windows 平台安装任何补丁，但是存在的问题是，不安装补丁系统就存在被攻击的可能，从而埋下安全隐患。如 Unix 操作系统发布开发都是以打补丁（Patch）的方式进行，操作系统的程序可以动态链接包括 I/O 驱动程序与系统服务，这些都为不法人员提供了可乘之机。常见的 0day 漏洞、UPNP 服务漏洞、RDP 漏洞等 ，不法人员轻易通过这些漏洞通过入侵、控制主机，进行破坏和窃取机密信息。

2.5.3.2 应用系统漏洞

SCADA 系统包括 SCADA 系统监控软件、数据服务器、操作员工作站、工程师工作站、磁盘阵列、授时系统、仿真软件、OPC 软件、网络管理软件等应用系统，由于应用软件多种多样，很难形成统一的防护规范以应对安全问题。国内外主流 SDCAD 软件都有可能存在较大的权限泄露风险，如下：

漏洞名称	发布时间	危害等级	漏洞类型	漏洞简介
ICONICS GENESIS32 缓冲区溢出漏洞 GENESIS32 缓冲区溢出漏洞	2012-4-19	危急	缓冲区溢出	ICONICS GENESIS32 是由美国 ICONICS 公司研制开发的新一代工控软件。ICONICS GENESIS32 8.05 版本、9.0 版本、9.1 版本、9.2 版本与 BizViz 8.05 版本、9.0 版本、9.1 版本和 9.2 版本中的 Security Login ActiveX 控件中存在缓冲区溢出漏洞。远程攻击者可利用该漏洞借助长密码导致拒绝服务（应用程序崩溃）或者执行任意代码。
Siemens SIMATIC WinCC 拒绝服务漏洞	2012-2-7	高危	高危	Siemens SIMATIC WinCC 多个版本中的运行加载器中的 HmiLoad 中存在拒绝服务漏洞，远程攻击者可利用该漏洞通过越过 TCP 发送特制数据，导致拒绝服务（应用程序崩溃）。这些版本包括：Siemens WinCC flexible 2004 版本、2005 版本、2007 版本、2008 版本，WinCC V11 （也称 TIA portal），TP、OP、 MP、Comfort Panels 和 Mobile Panels SIMATIC HMI 面板，WinCC V11 Runtime Advanced 以及 WinCC flexible Runtime。
WellinTech KingView KVWebSvr.dll ActiveX 控件栈缓冲区溢出漏洞	2011-8-17	危急	缓冲区溢出	WellinTech KingView 6.52 和 6.53 版本的 KVWebSvr.dll 的 ActiveX 控件中存在基于栈的缓冲区溢出漏洞。远程攻击者可借助 ValidateUser 方法中超长的第二参数执行任意代码。
Siemens SIMATIC WinCC 安全漏洞	2012-2-7	危急	授权问题	Siemens SIMATIC WinCC 多个版本中存在漏洞，该漏洞源于 TELNET daemon 未能执行验证。远程攻击者利用该漏洞借助 TCP 会话更易进行访问。这些版本包括：Siemens WinCC flexible 2004 版本、2005 版本、2007 版本、2008 版本，WinCC V11 （也称 TIA portal），TP、OP、 MP、 Comfort Panels 和 Mobile Panels SIMATIC HMI 面板、WinCC V11 Runtime Advanced 以及 WinCC flexible Runtime。
Invensys Wonderware Information Server 权限许可和访问控制漏洞	2012-4-5	高危	权限许可和访问控制	Invensys Wonderware Information Server 4.0 SP1 和 4.5 版本中存在漏洞，该漏洞源于未正确实现客户端控件。远程攻击者利用该漏洞借助未明向量绕过预期访问限制。
GE Proficy iFix HMI/SCADA 任意代码执行漏洞	2011-12-22	危急	缓冲区溢出	GE Proficy iFix HMI/SCADA 的 installations 中存在漏洞，远程攻击者可利用该漏洞执行任意代码。对于利用这个漏洞来说并不需要认证。通过默认 TCP 端口号 14000 监听的 ihDataArchiver.exe 进程中存在特殊的漏洞。在这个模块中的代码信任一个通过网络提供的值，并且使它作为把用户提供的数据复制到堆缓冲区的数组长度，通过提供一个足够大的值，缓冲区可能会溢出导致在运行服务的用户上下文中执行任意代码
Sunwayland ForceControl httpsvr.exe 堆缓冲区溢出漏洞	2011-8-1	危急	缓冲区溢出	Sunway ForceControl 6.1 SP1，SP2 和 SP3 版本的 httpsvr.exe 6.0.5.3 版本中存在基于堆的缓冲区溢出漏洞。远程攻击者可借助特制的 URL 导致拒绝服务（崩溃）并可能执行任意代码。

表2 主流SCADA软件脆弱性

并且，从分公司到场站现场都采用 NTP 授时服务，本地向远程 NTP 服务器发送 NTP 数据包，用的不可靠的 UDP 协议，一方面会造成信息泄露，另一方面会被不法人员利用 NTP Reply 洪水攻击，对整个系统或网络造成影响。

2.5.3.3 控制设备 / 系统安全风险

现场 PLC、终端、RTU 等控制设备大部分使用国外的控制组件，未实现自主可控，一方面存在逻辑炸弹和后门（如 Siemens 固件后门、圣诞节彩蛋等），另一方面现场控制设备基本没有安全防护能力，利用常规的手段对某知名 PLC 测试就可以获取如下信息：

图12 某知名PLC 测试截图

我们可以下载和上传设备 IOS 配置文件，并通过查看配置文件，瞬间就可以破解 TYPE- 7 的加密得到超级管理的明文密码，从而完全控制网络设备， 即使拿到加密后的密码串无法破解，也可以把下载来的 IOS 文件内的密码清空，再上传后，依然可以不用密码登陆设备。不法人员可以对现场设备进行篡改和恶意控制。

2.5.3.4 网络通信漏洞

在油气田的现场，由于作业区域广阔，经常通过光传输网、DDN、卫星、GPRS/CDMA 等传输手段将数据传到控制中心的路由器，各传输信道间的通道切换使用 HSRP 协议。

一方面 CISCO HSRP 协议，不法人员截获 HSRP 组的信息，并通过此信息结合相关的攻击手段可以造成 SR 路由器上的 HSRP 组频繁切换，进而给整个网络造成中断甚至瘫痪。另一方面一些不具备光纤通讯条件的场站，通过卫星、GPRS/CDMA 等无线方式通过 PAN 虚拟专用网络采集数据、下发指令，缺少安全论证手段和加密措施，存在较大的安全风险。

TCP/IP 以太网通讯技术、智能组件的广泛使用给数据传输带来便捷的同时，也给控制网络带来了传统的病毒、木马、入侵等新的问题。

2.5.3.5 工业协议漏洞

工业通讯协议是整个系统安全的重要环节，修改工厂的运行过程并不需要破坏组件，只需要构造一个满足工业协议的 IP 数据包然后将其发送给控制器即可。在标准的 PLC 中，没有任何安全安全校验和认证，它会接收任何满足 IP 数据包格式的数据包并根据数据包中的请求信息来执行实际控制过程。多数工业协议仅仅是对串行帧的简单封装如 Modbus、DNP3 协议，整个过程缺乏加密认证的机制，故很容易被窃取、欺骗和篡改 。

本系统中大量使用 OPC 协议通讯，而 OPC Classic 协议 (OPC DA, OPC HAD 和 OPC A&E) 基于微软的 DCOM 协议，DCOM 协议是在网络安全问题被广泛认识之前设计的，极易受到攻击，并且 OPC 通讯采用不固定的端口号，导致目前几乎无法使用传统的 IT 防火墙来确保其安全性。

2.5.3.6 移动介质安全

移动存储介质严重影响控制系统安全，控制系统和生产网络安全，对生产网和办公网进行了逻辑物理隔离，但有一些用户非法使用移动存储介质，如 U 盘等。移动存储介质有意无意的违规使用、非法拷贝、介质丢失、无意连接到互联网而导致信息泄密，同时也很容易导致 U 盘病毒的传播。一旦移动存储介质受到病毒攻击并作为病毒传输媒介，将病毒带入内网，在很大程度上破坏了严格意义上的物理隔离。统计数据表明，大部分内网的计算机遭受病毒攻击的事件，就是因为不规范使用移动存储介质造成的。

2.5.4 安全防护思路

通过以上对工业控制系统现状和安全风险分析，可以看到工业控制系统自身存在的脆弱性风险，而“两化融合”“全球能源互联网”“智慧油田”等全新的概念结合工控系统自身的脆弱性，进一步加剧了的工业控制系统的安全风险。工业控制系统安全是传统 IT 系统安全的延伸，在工控系统的安全方法论上可参考信息安全的方法论，但同时工业控制系统又具有自身的特点，在属性上优先考虑可用性然后再考虑完整性和保密性。

根据以上的特点，石油石化行业工业控制系统安全防护思路，主要从四个方面考虑工业控制系统安全问题。首先各个工业控制系统的环境是不尽相同的，即使是同为油气田行业的不同分公司，所使用的架构和具体的工业控制系统也是有很大区别的，在进行安全建设的前提下参照国际、国内相关的工业信息安全风险评估技术标准要求及能源行业内对工控评估的行业规范需要对具体的工业控制系统安全现状进行评估，根据评估结论提出有针对性的抵御安全威胁的防护对策和整改措施，以防范和缓解信息安全风险，将风险控制在可接受的水平，最大限度地为保障工业控制系统安全提供科学依据。

其次需要构建工控系统安全体系架构，对工业控制系统进行纵向分区、横向分层，根据不同作业区域的功能与作用不同，进行不同等级的有针对性的防护，达成安全防护重点突出，使安全防护资源得到合理分配，从而构建工控系统安全防护架构，从根本上建立工业控制系统的安全基础。

再次需要根据前两部的结论有针对性的做具体的安全防护工作，比如：系统主机安全、工业控制系统网络安全、工业控制系统应用层安全、移动介质安全、运维安全、容灾备份体系等。

最后是对工业控制系统进行全面监控和审计，构建安全管理平台来对生产网中的链路、网络设备、服务器、存储、负载均衡设备、防火墙、数据库、中间件、业务应用服务等的运行状态和指标参数进行实现实时数据采集和运行状态监控，利用科学、高效的技术手段和已有的成功经验实现对工业控制系统的精细化、及时化、准确化的运维保障和管理。

2.6 烟草行业安全解决思路

2011 年，国家烟草专卖局印发了《国家烟草专卖局办公室关于卷烟工业企业信息化建设的指导意见》(国烟办综[2011]212 号)，明确了构建智能化工厂、建设信息化企业的主要任务。各烟草工业企业在进一步构建一体化“数字烟草”，推进烟草行业的“两化融合”过程中，以太网技术与工业控制网络技术的融合程度逐渐加深，工业控制网络和企业管理网业务信息数据交换的关联性也越来越紧密，工业控制信息系统的机密性、完整性，特别是可用性保障问题也成为目前需要解决的问题。

由于工业控制系统安全与传统的信息系统安全不同，它通常关注更多的是物理安全及生产设备功能的高可用性，随着信息化与工业化技术的深度融合以及潜在网络威胁的影响，工业控制系统也将从传统的仅关注物理安全、功能高可用性转向更为关注生产网中信息系统的安全，特别是工业控制系统安全。这种转变将在推动传统的烟草工业企业信息化进程中产生较大的影响。

2.6.1 卷烟生产应用系统架构

参考《国家烟草专卖局办公室关于卷烟工业企业信息化建设的指导意见》(国烟办综 [2011] 212 号)，适用于卷烟工业企业生产管控的应用系统层次从上到下主要分为三层：管理协同层、生产执行层及工业控制层。共同构成卷烟工业企业应用系统层次结构。

图13 卷烟工业生产应用系统层次结构

1) 管理协同层

核心系统：企业资源计划系统（ERP）

卷烟工业企业生产应用系统结构层次结构中，管理协同层信息系统处于最上层，负责企业内部运营与管控，实现工业企业与上下游企业业务协同。其关键应用系统是全面集成企业物流、信息流和资金流，为企业提供经营、计划、控制与业绩评估的企业资源计划系统（ERP）。该系统使各烟草生产管理部门和生产执行部门之间信息通畅，形成一个有机整体。实现生产管理信息和生产控制信息一体化管理，经营信息和生产信息一体化管理，设备资源和人力资源一体化管理，达到对企业生产，经营管理各环节的有效控制和管理。

管理协同层其它应用系统可包含了许多子系统，如: 生产管理、财务管理、质量管理、车间管理、能源管理、销售管理、人事管理、设备管理、技术管理、综合管理等等，管理信息系统融信息服务、决策支持于一体。

2) 生产执行层

核心系统：生产执行系统（MES）

生产执行层处于管理协同层和工业控制层之间，核心应用系统是生产执行系统（MES）。烟草工业企业生产过程中，MES 系统是生产自动化与管理信息化之间的重要桥梁，主要负责生产管理调度指挥和执行，烟草工业企业的 MES 系统对上层生产计划管理是执行，对下层生产控制系统是调度指挥。它起到管理协同层和工业控制层数据双向通道的核心作用。MES 的数据直接来源于生产过程控制系统（PCS），监控系统和数据采集系统采集的实时数据经过处理后，生成生产过程信息，供 MES 系统使用。

MES 系统负责生产作业计划制定、资源（人和设备等）优化调度、物料管理、生产质量、工艺控制、能源供应控制、生产过程监控以及必要的数据信息转换等数据集成和应用。

3) 工业控制层

核心系统：生产过程控制系统（PCS）

工业控制层处于最下层，直接面向烟机设备，负责采集各类卷烟生产设备自动化控制系统生成的实时生产数据，接收生产执行系统下达的生产作业等控制指令。烟草工业生产控制系统是指生产车间的制丝生产线、卷接包机组、动力能源中心、物流中心等生产系统，用来承载 MES（生产执行系统）。主要完成加工作业、检测和操控作业、作业管理等功能。

卷烟生产过程控制系统主要有制丝集控系统、卷包数采系统、物流自动化系统、动力能源自动化系统。

2.6.2 烟草工业企业生产网架构

根据卷烟工业企业生产管控的应用系统层次，目前典型的卷烟工业企业生产网网络架构也是依据这三个层级来设计和构架。

注：由于国内各卷烟生产企业之间的生产规模和信息化建设程度还存在一定的差距，部分卷烟生产企业已经实现了基于 ERP、MES 及 PCS 三层应用架构的生产管控一体化信息模型，基本实现了“两化融合”。而有部分卷烟生产企业管理协同层和生产执行层大部分功能模块都集中在省级中烟工业公司，生产厂仅保有基本的工业控制层生产能力。

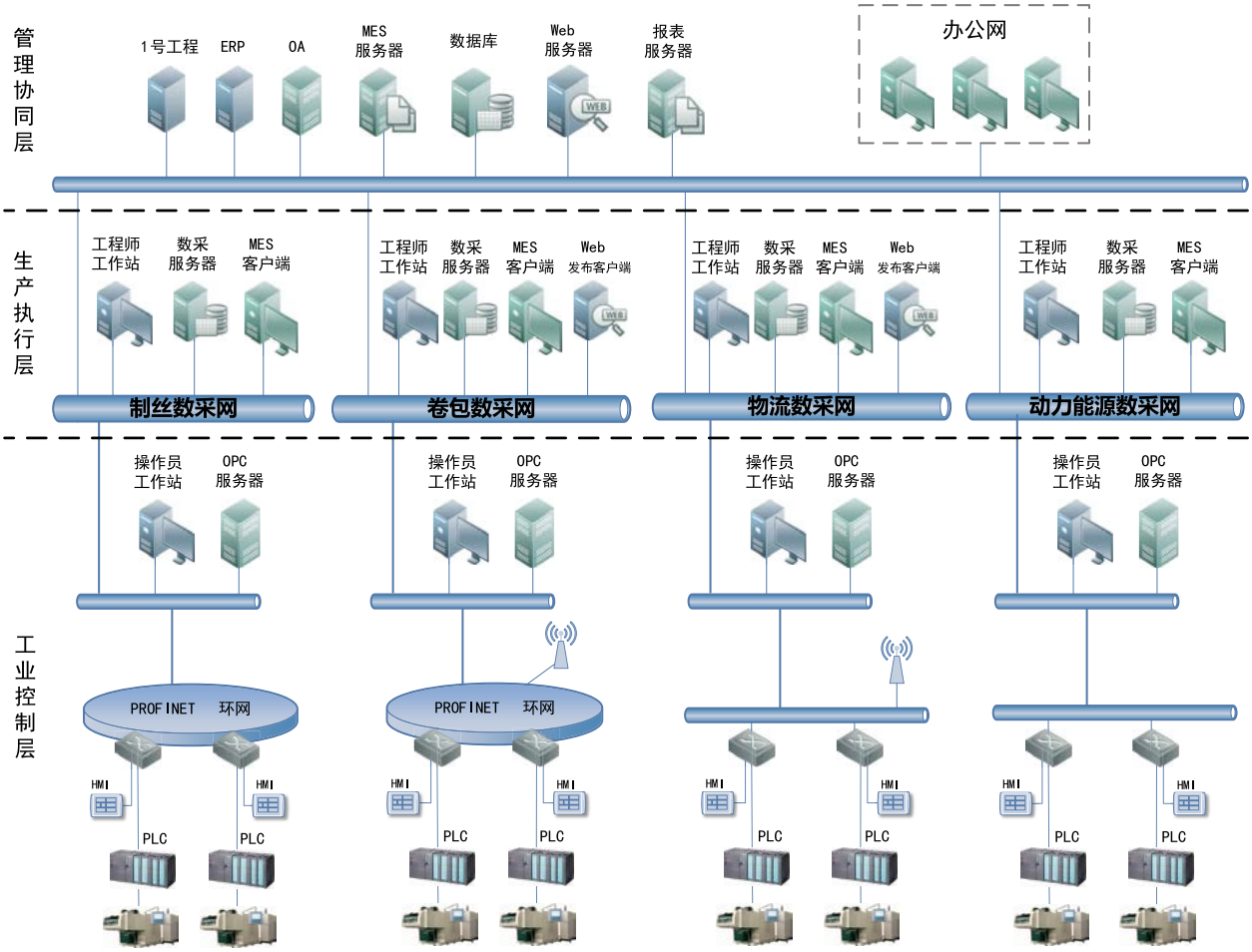


图14 典型烟草工业企业生产网网络架构示例

因此，根据前面卷烟生产应用系统三层架构及网络架构的描述，我们可以看出，要实现卷烟生产管理、执行与控制的一体化，传统卷烟企业工业控制网络和企业管理网络的分离建设或者物理隔离的方式，已无法满足当前“两化融合”的业务发展需求，为了提高卷烟生产企业高效的信息自动化水平，企业管理网络与生产控制网络之间的数据交换已经是发展趋势，各生产车间卷烟生产线设备的生产数据信息需要实时传输到生产执行层和管理协同层，为管理者提供准确统一的生产数据；同样，管理者可以通过对实时生产数据的分析，下发产生调度指令，实时调整生产计划，有效指导卷烟生产线的生产活动。

2.6.3 烟草行业工业控制安全风险描述

2.6.3.1 网络与通信层面

1. 安全域架构设计缺失

目前部分卷烟生产企业由于建厂时间较早，最初生产网网络规划设计的时候没有考虑网络互联互通产生的通信安全问题，也没有考虑安全域的设计思路，或者安全域设计不合理，导致企业管理网与生产网之间，生产网内部各生产车间中控之间，都缺失明确的安全边界的界定，内部数据的传输没有得到合理的访问控制，这可能会导致生产网及管理网的业务系统、生产系统、工业控制系统和生产数据未经授权的访问、病毒感染，生产业务拒绝式服务攻击等安全风险。

而近几年，随着部分卷烟生产企业技改项目，生产网网络架构重新规划设计，安全域的理念已经被广泛应用，但仅限于考虑到生产网与管理网的安全隔离要求，而对于生产网内部生产执行层安全域的划分仍然不全面。生产网内部不同生产区域之间的安全防御机制没有建立起来，容易造成某一生产系统遭受到攻击很快就会扩散到整个生产网内部当中。

2. 生产网与管理网之间安全隔离机制不合理

管理网办公人员需要了解底层生产设备的运行状态信息，及时掌握生产工艺各流程的运行状况、工艺参数的变化、实现工艺的过程监视与控制；所以需要通过 MES 系统对生产控制系统进行管理。在这个过程中，多数卷烟生产企业都没有严格且有效的安全管理机制，以防止管理网对生产控制系统的非授权访问和滥用（如业务操作人员越权操作其他业务系统）、失误操作、篡改指令、违规操作等行为。

目前，在网络建设中已经考虑到生产网与管理网之间需要安全隔离机制的卷烟生产企业，隔离或访问控制机制一般有以下三种方式：

1) 服务器双网卡访问控制

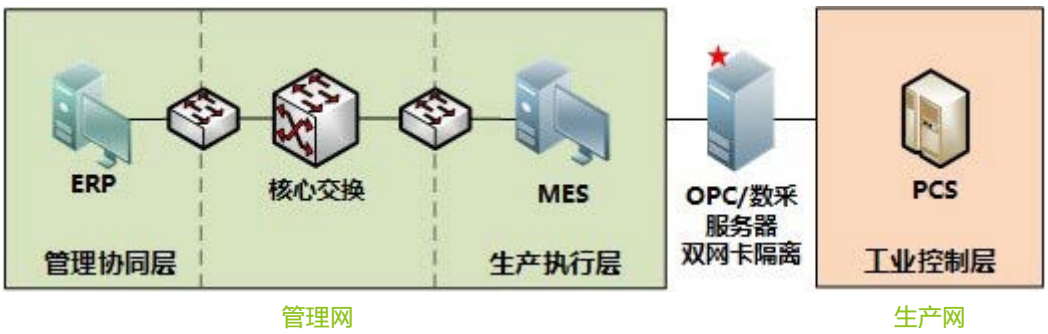


图15 服务器双网卡访问控制示意图

该访问控制机制是通过在数据采集服务器或 OPC 服务器安装双网卡，一块网卡与管理网通讯，另一块网卡与生产网通讯，两块网卡不在同一网段，并在服务器（以及生产执行层前端交换设备）设置访问控制策略对管理网和生产网进行隔离。

使用双网卡隔离的方式，由于数据采集服务器或 OPC 服务器同时存在于生产网和管理网，会存在未经授权的访问和数据从生产网和管理网相互传递的风险。

另外，采用双网卡的数采服务器或 OPC 服务器本身已经暴露在管理网（可能连接互联网），存在被扫描和攻击的风险，而该服务器又与内部生产网是互通的，如果该服务器在管理网中病毒，则会传播到生产网工业控制系统当中，直接影响到生产业务。

2) 交换设备访问控制

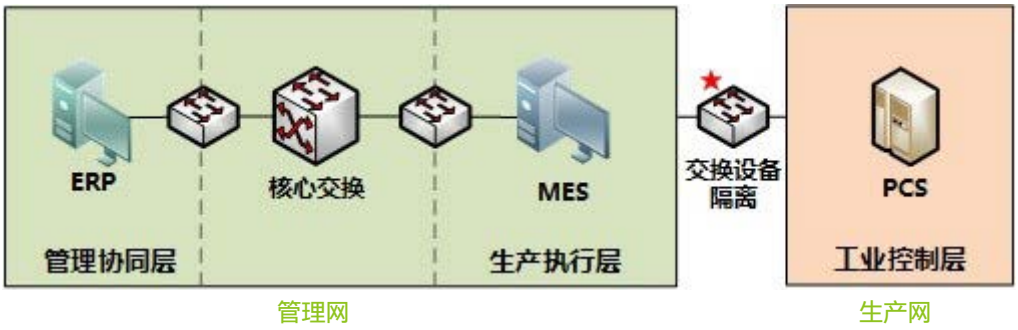


图16 交换设备访问控制示意图

该访问控制机制仅通过连接管理网与生产网的交换设备，配置 ACL 访问控制策略来规定需要限制哪些人员角色可以直接访问生产网设备。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。

尽管一些交换设备也支持类似防火墙 ACL 访问控制列表这样的控制过滤功能，但它并不具备专业防火墙针对网络攻击进行防御的功能，而且还不具备动态的包过滤，因此如果采用交换设备来替代防火墙等专业安全隔离设备，存在被攻击和入侵的风险依然很高。

3) 防火墙访问控制

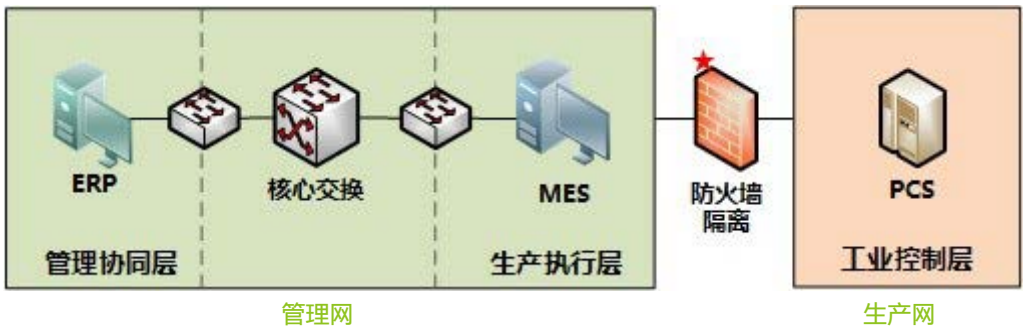


图17 防火墙访问控制示意图

目前一些网络结构规划较为完善的卷烟生产企业已经建设了管理网与生产网之间的安全隔离机制，多数都是采用专业防火墙进行访问控制与攻击防御。但对于防火墙安全策略的配置没有依据统一的规范和标准进行，有些传统防火墙仅支持访问控制及包过滤功能，并不能实现安全审计、恶意行为识别等功能，甚至不能支持基于工业以太网控制协议（如 OPC、ProfiNet/ProfiBus、ModBus 等）的数据包识别。因此，这种方式的隔离是不够全面的。

3. **控制指令数据通信明文传输**

目前多数卷烟生产企业均没有针对数据传输的加密机制。不管是管理网内部数据通讯，还是生产网内部通讯，以及管理网 PC 与生产网数采服务器之间通讯、上位机与 PLC 控制器的通讯之间都是明文数据传输。特别是目前常见的工业控制协议来控制生产设备时传输的各种指令信息都是采用明文方式（如 ProfiNet/ProfiBus、ModBus、DNP3 等），易被攻击者窃听和解析。

4. **生产网无线网络管控机制缺失或不完善**

由于多数卷烟生产企业在设计网络架构的初期，并没有考虑到无线网络将在卷烟生产过程中的广泛应用，因此也没有针对于无线网络的统一部署和管控。而在车间内部通常由于生产业务需要，会采用无线网络接入技术作为现有生产网络的延伸。然而在搭建无线网络的时候，往往仅考虑生产业务的可用性，而针对无线客户端和接入点的安全认证措施往往都被忽略（甚至存在免密码直接接入生产网），这样生产网无形当中多了一条对外的不安全网络出口，安全隐患极大。

另外很多卷烟生产企业都已经广泛应用了 AGV 无线引导小车，特别是在卷包车间及物流车间。AGV 无线引导小车通讯系统由无线 AP、上位机组态软件、车载 PLC 三部分组成。控制端与车载 PLC 之间通讯网络采用无线通信，通过无线 AP 与小车车载的 PLC 进行连接。而该无线通讯协议通常是已被泛应用的 802.11 b/g/n 协议，该无线网络也就是我们常见的 WiFi 网络。

如果生产网无线客户端和接入点之间无任何身份认证机制，使得该无线接入点很容易被恶意接入，攻击者将通过无线网络毫无阻拦的直接连接到生产网络，甚至可以直接对控制器（PLC）下达运行指令，将严重影响到安全生产。

5. **网络设备安全性配置不完善**

生产网的网络设备大多是由车间系统管理员管理（非安全管理员），网络设备配置基本都是保持出厂默认。存在很高的网络设备被未授权访问或被攻击的风险。甚至造成生产网络的瘫痪。

6. **工业控制安全审计机制缺失**

没有对工业控制网日常运行维护人员的操作行为进行统一运维审计管理，对于人为原因造成的卷烟生产业务异常事件无法溯源，也无法找到事件发生根本原因，最终无法对事件进行定性分析。

2.6.3.2 控制器、主机及应用层面

1. **工业控制系统（PLC、RTU）自身存在大量漏洞**

目前烟草行业工业控制系统使用比较主流的品牌是 Siemens S7 系列 PLC、Rockwell AB PLC 以及 GE PLC，依据绿盟科技去年发布的《2014 年工业控制系统安全研究与实践报告》的描述，工业控制系统公开漏洞所涉及的工业控制系统厂商占比中，Siemens（28%）、通用电气 GE（7%）与 Rockwell（5%）三者漏洞数总共超过 40%。

2014 年度新增漏洞按照可能引起的攻击威胁分类的统计及占比分析结果中可以看出，可引起业务中断的拒绝服务类漏洞占比最高 (约 33%)，这对强调业务连续性的卷烟生产业务来说不是一个好消息。而位居其次的是缓冲区溢出类漏洞，其占比也高达 20%；从侧面说明工控软件企业在软件开发的编码阶段缺乏严格的编程规范要求，从而造成这类漏洞占比较高的原因。当然占比较高的可造成信息泄露、远程控制及权限提升类的漏洞也必将是攻击者最为关注的，利用他们可以窃取卷烟生产企业的生产计划、工艺流程等敏感信息，甚至获得工控系统的控制权，干扰、破坏卷烟生产业务的正常生产或运营活动。

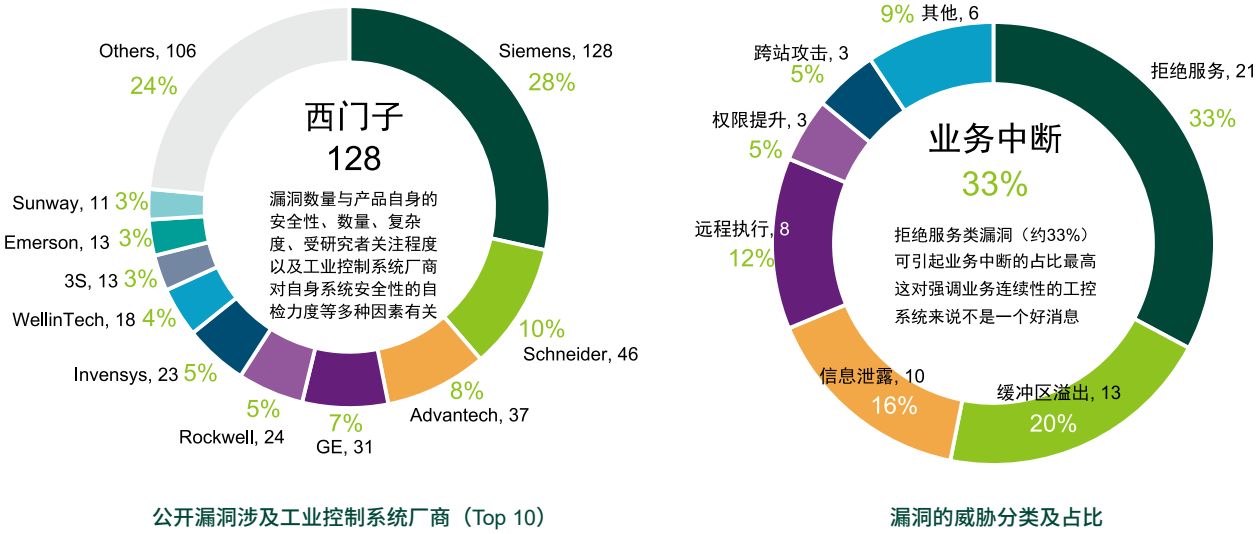


图18　绿盟科技2014年工业控制系统安全研究与实践报告

2.　关键生产设备 HMI 身份认证机制不完善

部分卷烟生产企业生产车间工业控制系统 PLC 前端现场操控触摸屏 HMI 是登陆身份认证机制不完善，弱口令情况普遍存在，甚至还有无认证机制完全开放的运行状态，同时缺失监管及监控机制，导致相关联的生产设备有可能被越权操作。

3.　工程师站、操作员站和监控终端缺乏安全加固机制

一般在卷烟生产企业，工程师站、操作员站以及监控终端均为 Windows 系统，运行多年没有系统打补丁机制。由于操作员站计算机可以直接向工业控制系统下达生产指令、监控生产设备状态，系统存在大量安全漏洞有可能导致被攻击的风险大大增加（如获取权限后，可以任意下达控制指令）。

4.　关键生产设备组件、工程师站、操作员站及监控终端远程运维操作

对于关键工业控制系统 PLC 的运维、检修工作，一般都是本地化操作，但是部分生产企业安全隔离机制不完善，导致具备被远程访问操作的可能性。比如使维护工程师和厂商获得远程访问系统的能力，应该加以安全控制，以防止未经授权的个人，通过远程访问接入到生产网。

（在某卷烟厂，车间系统管理员为了 PLC 设备检修的便利性，通过生产网操作员站计算机违规连接互联网，并通过 QQ 远程支持功能，允许 PLC 原厂工程人员远程接入生产网操作员站，对 PLC 直接进行设备维修操作。）

另外，对于工程师站、操作员站及监控终端，原则上都应在中控室本地访问操作，应禁止远程操作运维管理。但多数企业终端远程桌面端口 3389 并没有被关闭，也存在为了日常运维的便利性采用远程登录操作的情况。该运维方式容易被攻击者获取系统最高权限，对控制器（PLC）下发任意指令，会对生产设备发起恶意攻击。

5.　工程师站、操作员站及生产网业务系统服务器缺乏恶意代码的检测机制

在部分卷烟生产企业，由于工程师站、操作员站和监控终端计算机工业控制应用软件与防病毒软件存在兼容性问题，因此不安装，给病毒与恶意代码传染与扩散留下了空间。

而对于数采服务器和 Web 发布服务器，由于担心影响到生产可用性，也存在未安装防病毒软件的现象。即便部署了防病毒软件，病毒库也常年未更新。

（在某卷烟厂，已经发生过制丝和卷包车间发生过因病毒导致生产业务服务器、数采服务器等全部中断服务，所有服务器只能重装系统的事件。）

6. 工程师站、操作员站和监控终端系统身份认证机制不完善

部分卷烟生产企业为了日常运维的便利性，中控室操作员站及监控终端都采用公用账号（甚至是系统默认账号），且系统操作界面长期处于开放状态，没有配置登陆超时锁定功能。导致进出中控室的所有人员都可以对其进行操作，可能存在被无关人员访问操作员站进行未授权操作的安全风险。相当于对车间 PLC 控制器可随意操作，且发生安全事件无法追溯责任人。

7. 生产网 IP 地址网段划分不合理

部分卷烟生产企业生产网办公计算机与生产业务服务器规划在同一 IP 网段，导致有可能出现生产网第三方计算机 IP 地址与生产业务服务器 IP 地址冲突，导致系统中断的安全风险。

（在某卷烟厂，由于外来人员因为私设 IP 地址，造成与某生产设备的 IP 地址冲突，导致该生产线发生中断故障。）

8. 生产网移动设备管控措施不完善

部分卷烟生产企业针对工业控制网络生产设备，没有采用物理封闭 USB 接口的机制，且生产网员工 USB 移动存储介质管控机制不完善，导致生产网存在被病毒感染的安全风险。

另外，不安全的移动维护设备（比如笔记本等）的未授权接入，也会造成木马、病毒等恶意代码在生产中的传播。

9. 业务系统（如 MES）、数据库账户权限设置不合理

生产执行系统（MES）作为卷烟生产企业核心业务系统，系统登陆账户都是根据员工岗位区分角色及系统权限。但是多数卷烟生产企业员工权限申请流程执行不好，比如车间员工电话向信息管理部门系统管理员申请，系统管理员联系厂家现场运维人员更改账号权限。缺失申请审批记录。也有车间员工直接向业务系统原厂运维人员电话申请，无需任何流程确认审批，权限即刻开通。这样对于卷烟生产业务会造成极大的安全隐患。

另外对于生产车间数采服务器，部分企业未区分登陆账号划和权限，或者登录账号和初始密码都是默认账号，并且没有设置密码保护策略。攻击者可获得数据库权限，可任意破坏、篡改生产数据库。

10. 关键设备的配置文件没有存储备份措施

对于生产网中关键设备配置文件没有进行存储与备份机制，无法防偶然事故的发生，比如防止员工误操作，或者攻击者对配置文件进行更改，造成生产业务中断或生产数据的丢失。

2.6.3.3 管理制度及组织层面

1. 工业控制系统专职 / 兼职信息安全人员缺乏

一般在卷烟生产企业车间中都有系统管理员，兼职信息安全管理员。

由于工业控制系统运维与传统信息系统运维在各卷烟生产企业往往不属于同一个责任部门，他们所面对的岗位职责也不相同。工业控制系统的安全运行由相关的生产部门负责，信息部门仅处于从属的地位。随着信息化与工业化技术的深度融合以及潜在网络威胁的影响，工业控制系统也需要从传统的仅关注物理安全、生产业务安全转向更为关注信息系统安全。

2. 关键生产岗位人员工控安全知识培训不足

多数参与工业控制系统日常运维的车间系统管理员，一般只进行全员安全意识培训，缺乏针对生产网相关人员工业控制系统安全风险的培训，这些关键岗位人员也很少去关注工业控制系统的安全性，日常工作仅仅是保障系统的可用性。

3. 工业控制系统的应急保障机制缺失

一般卷烟生产企业只有针对预知的事件发布预案（如车间停电、停气等预案）。缺失针对突发安全事件而导致生产业务受到影响的应急预案。比如生产网基础设施关键软硬件故障发生，生产业务可能会造成业务中断和生产数据丢失。

4. 工业控制系统配套操作指南、故障快速恢复指南未合理保存

工业控制系统设备操作指南、故障快速恢复指南等重要文档应当及时更新并保持随时可用，这些操作指南都是卷烟生产业务发生故障时完成恢复所必须的组成部分。

但是多数卷烟生产企业工业控制系统及相应生产线已经运行很多年，最初的原厂的操作指南、故障快速恢复指南早已丢失；有的企业没有完善的关键文档保存机制，导致遇到突发事件也无法快速找到相应的指导手册。

2.6.4 烟草工业控制网络安全防护思路

2.6.4.1 生产网与管理网安全隔离合规要求

根据《YC/T 494-2014 烟草工业企业生产网与管理网网络互联安全规范》的相关要求，烟草工业企业应将网络划分为生产网和管理网两部分，在规划设计网络时应考虑生产网、管理网及其他网络互联的安全隔离要求，互连接口安全功能应包括身份鉴别、访问控制、网络互联控制、恶意行为防范、安全审计、支撑操作系统安全。

规范所示网络连接架构图如下：

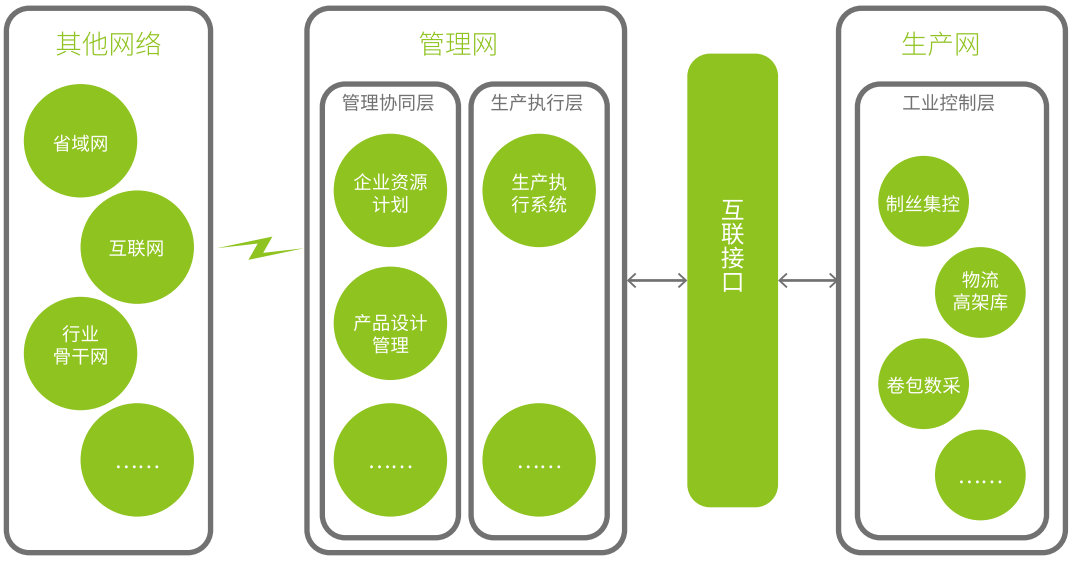


图19 烟草工业企业生产网与管理网网络连接架构图

2.6.4.2 生产网分层分域设计

生产网是卷烟生产企业的核心安全域，其主要包括为卷烟生产提供服务的业务系统及设备，可根据生产车间网络规模继续划分为动能接入域、卷包接入域、物流接入域、动力能源接入域四个子域，该安全域网络架构设计如下：

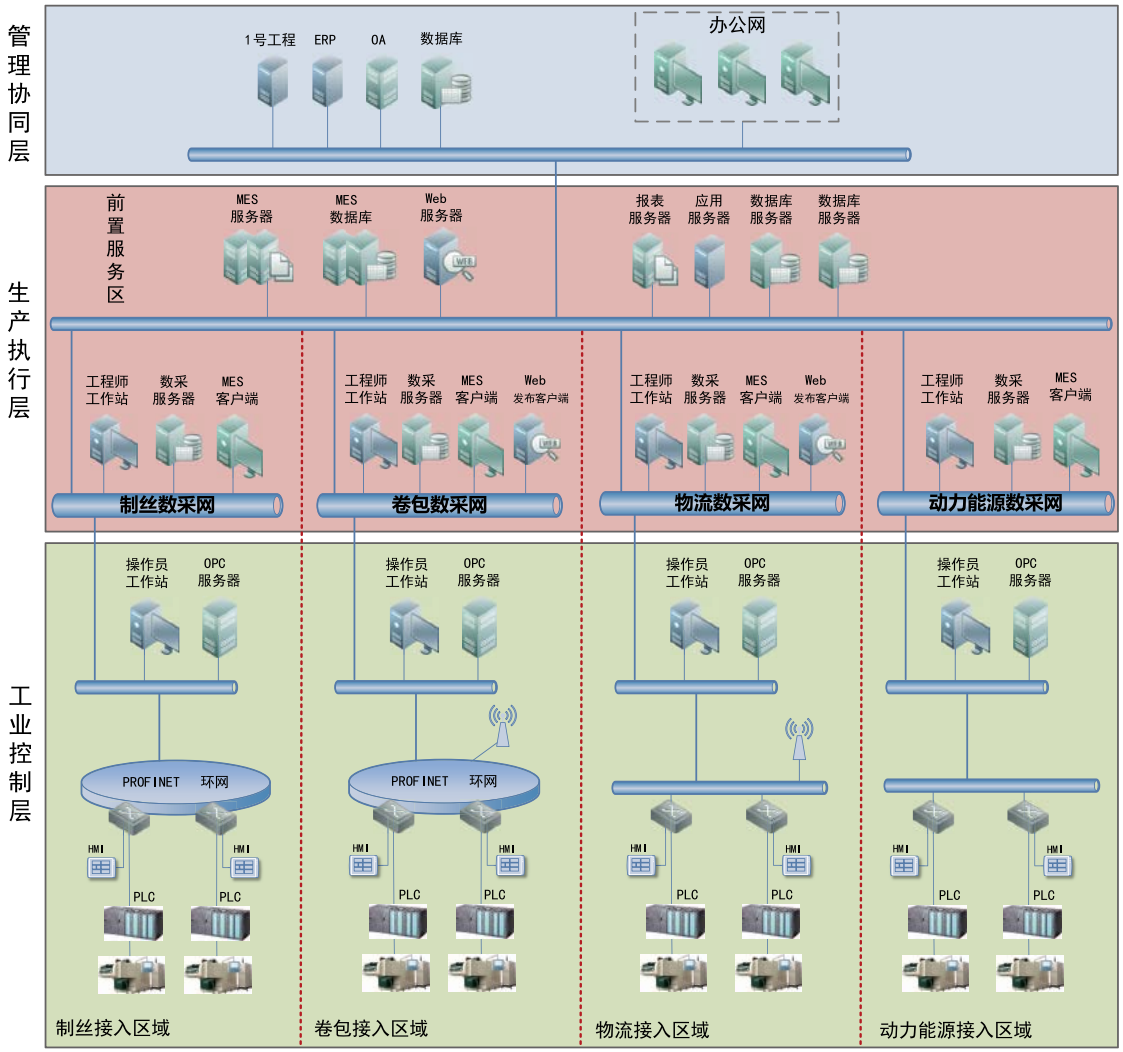


图20 卷烟生产企业安全域架构设计示例

基于对安全防护目标及重点的分析，我们设计了总体防护总体策略是：网络专用、横向隔离；安全分区、纵向防御。

- 横向：管理协同层、生产执行层、工业控制层
- 纵向：制丝接入域、卷包接入域、物流接入域、动力能源接入域

1) **管理协同层：**完成管理者和各职能科室生产管理报表生成的任务及集中监控。

2) **生产执行层：**完成各车间实时监控的任务，它对下连接现场控制层，对上通过网络连接管理协同层，它不仅负责现场控制设备的实时数据采集，而且在系统中起到上传下达的重要作用。

3) **工业控制层：**由 PLC、智能仪表等控制器组成，是整个生产管理系统的基础。

生产网依据分级分域的建设方式来构架，各安全域之间的安全隔离机制如下图所示：

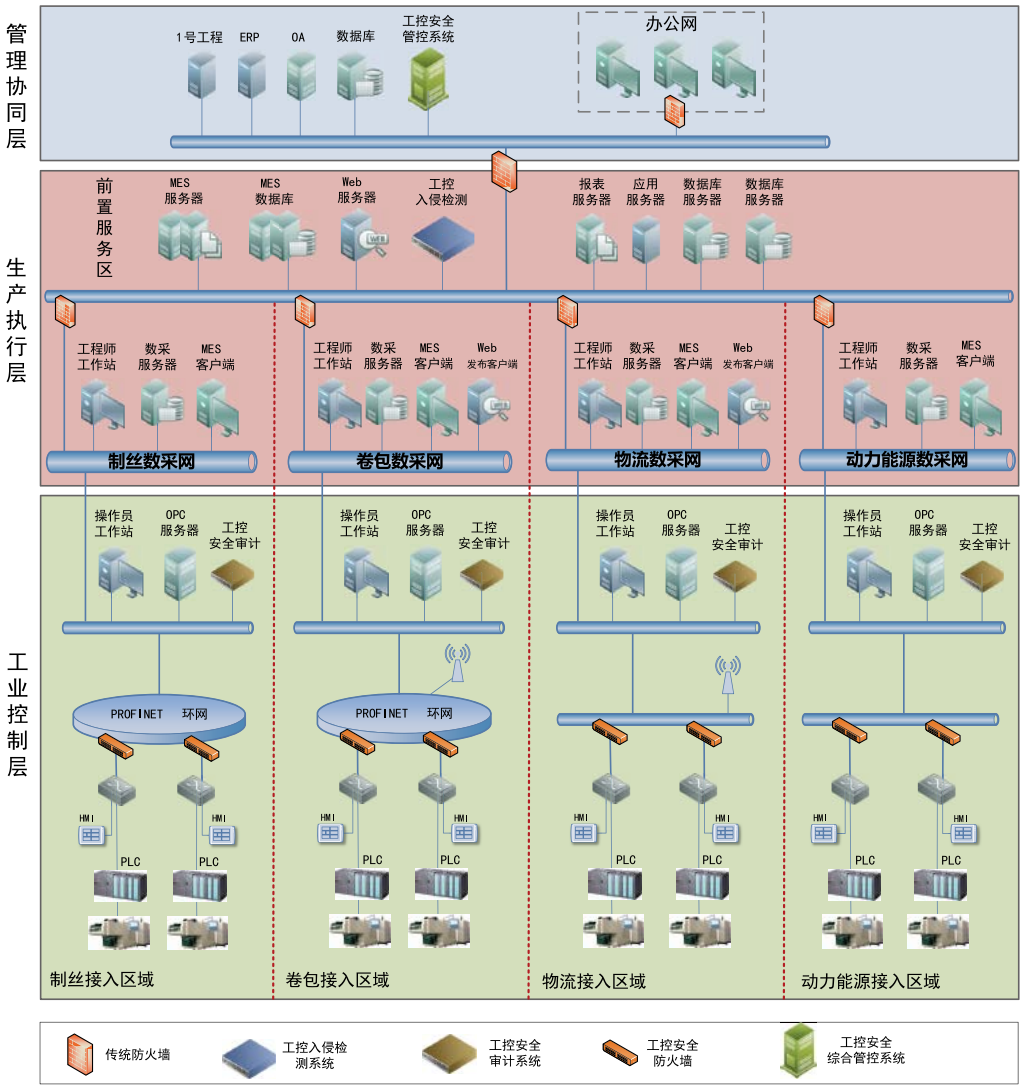


图21 卷烟生产企业安全域边界安全互联示例

为了保障个安全域的安全性，各安全域边界之间涉及到传统防火墙、工控入侵检测系统、工控安全审计系统以及工控防火墙等安全技术，下文将作简要描述。

2.6.4.3 访问控制

在生产网外部的管理协同层，生产执行层之间的访问控制要通过传统防火墙来提供包括访问控制、地址转换、应用代理、事件审核和报警等功能。

而各个卷烟生产企业工业控制层内部，在环网及总线网络各个烟机设备节点，由于需要识别工业控制协议数据包，以及对于工业网络协议和应用数据的内容进行解析和检查。因此，就需要针对工业控制网络环境的专业工控安全防火墙，除了传统防火墙的基础访问控制功能之外，更重要的是要针对工业网络中常见工业协议（如 Modbus、OPC 等）的数据包细粒度检查和深度过滤，以阻断来自管理网络的病毒传播、黑客攻击等行为，避免其对生产网络和对生产业务的影响。

2.1.4.4 安全审计

通过对基于 IEC 60870-5-101、102 和 104 协议、IEC 61850、MODBUSRTU 和 PROFINET 等工控协议的操作指令进行有效的识别，工控安全审计系统可以对从卷烟生产企业各生产车间中控室到调度中心之间的传输的指令信息进行有效审计。发现其中操作指令是否符合预制的审计规则，如果发现其中存在恶意的操作行为或者一些误操作的指令进行下发，审计设备可以进行及时的告警。并且在存在操作异常的时候追诉中，审计设备可以实现对恶意事件和行为事后追查稽核、重建事件和系统条件，生成问题报告，为事后的分析提供有效的依据。

2.1.4.5 工控安全综合管控平台

安全的统一集中管控，是“CT-155”行业信息化架构蓝图中对十三五信息安全建设过程的建设方向，基于工业控制系统安全的统一管控平台建设也将是个趋势。对于生产网中集中管控措施的目的主要是监控工业设备的日志信息，并采集相关数据至工控安全综合管控平台，通过对系统安全风险情况的综合评价，完成对生产网中的工业控制系统设备上所有不同类型的日志告警信息进行监控并生成告警信息。各车间系统运维人员可以通过监控告警的设置、筛选、告警分析完成对威胁的监视、分析、诊断工作。同时，平台可以对告警事件按照各车间系统运维人员指定的要求进行统计、分析、评估，并呈现各类事件的统计结果和发展态势趋势。

2.1.4.6 系统上线前安全评估

目前在个卷烟生产企业中，工业控制系统（PLC）的入网与上线管理机制还是比较欠缺，该阶段是整个工业控制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，立足于系统上线过程，基于验收规范的整体规程要求，通过对工控系统的安全性进行分析，发现系统中潜在的安全漏洞是上线前安全评估的首要任务。之后，再基于发现的安全漏洞与相应的工控设备和系统提供商进行联系，获取相关的漏洞解决方案。漏洞的检测主要从已知漏洞的漏洞扫描如采用漏洞扫描技术和工控设备、系统主动漏洞挖掘技术（FUZZ 技术）等，来发现系统中潜在的安全隐患。

总结及附录

03 总结

3.1 工控安全发展综述

纵观国际工控安全的发展态势，美国是最早开始研究和执行工控安全标准的国家，北美电力可靠性公司给予 CIP 系列标准的要求开展在北美电力开展针对电力企业安全安全检查（包含核电）；欧洲已经按照 WIB 标准来检测工控产品安全，并且以德国为代表的国家，已经开始基于 ISO 27000 系列的 ISO 27009 进行工控安全的建设；日本基于 IEC 62443 要求结合阿基里斯认证要求，从 2013 年起规定所有工控产品必须通过国家标准认证才能在国内使用，并且已经在一些重点行业如能源和化工行业开始了工控安全检查和建设；以色列已成立国家级工控产品安全检测中心，用于工控安全产品入网前的安全检测。

在我国国内电力企业是最早开始工控系统安全建设的行业，大部分的大型电力企业已经基于原电监会 5 号令（电力二次系统安全防护方案）的要求进行了网络专用、安全分区、横向隔离、纵向加密认证的建设，有效避免了原有开放网络所带来的安全隐患；石油、石化、冶金和关键制造等行业也已经在开展针对工业控制系统的试点建设。

从震网病毒事件后，工业控制系统的安全引起了国内各界的高度重视，在 2010 年国家信息安全标准委会（TC260）制定了《工控 SCADA 安全指南》。在 2011 年工信部发布了《关于加强工业控制系统信息安全管理的通知》即 451 号文，451 号文从连接管理要求、组网管理要求、配置管理要求、设备选择和升级管理要求、数据管理要求和应急管理要求等 6 个方面提出了加强对工业企业工业控制系统安全管理的要求。国务也在 2012 年国务院《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 号文 > 中明确提出保障工业控制系统安全。加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统，以及物联网应用、数字城市建设中的安全防护和管理，定期开展安全检查和风险评估。重点对可能危及生命和公共财产安全的工业控制系统加强监管。对重点领域使用的关键产品开展安全测评，实行安全风险和漏洞通报制度。从 2012 年开展到 2014 年工信部陆续开展了针对工业控制系统的安全检查，并且检查的内容逐步由安全检查向安全审查的方向发展。由于 2015 年底乌克兰电力攻击所导致的电网中断引起全世界范围内对电网安全的关注，国内两大主要电网基于自身电网安全的需求，陆续在开展相关的安全检查，通过检查发现电网中潜在的安全隐患，从而进行有针对性的安全加固。

从产品分布上，国内对工控安全产品的认识，也逐步从以边界防护为主工控安全网关类产品开发，向提供工控系统全生命周期安全保障的工控安全类产品开发迁移。目前主流的工控安全类产品主要涵盖，检测类产品、防护类产品、监测预警类产品，一些在传统信息系统中采用的技术开始在工控安全产品中得到应用，如大数据技术、感知技术等。从国内开发的工控安全产品的技术特点上看，原有以信息安全为背景的企业，开发出的产品在使用上仍然继承了原有信息安全产品在配置和应用上的特点，对于实际在工业现场中的应用看，缺乏与实际工业现场应用习惯等融合，对于现场人员的使用仍然存在的一定的障碍。而已工业为背景的企业开发的工控安全产品，在产品形态和易用性上存在较大的优势，但是对于信息安全基本功能的理解和攻击防护的规则匹配设置上仍然存在较大的问题，在应用真实攻击行为后，仍然略显苍白。

建立在融合实际业务特征与信息安全技术的特性基础上的工业信息安全技术，满足业务运行保障的需求，符合实际工业环境特点才能真正满足工业控制系统的安全保障，相关的产品业务发展才能真正进入到高速轨道。

伴随着国家政策的指引（发改委安全专项支持、工信部互联网 + 时代产业转型项目的支持）以及行业内对工控安全的行业引导（如发改委 14 号令）以及相关国家相关工控安全标准的发布（如 GB/T 30976）。在相关因素驱动下，工控安全产品应用实例的增多及实际应用效果得到业界的认可，预计在预期的未来，工业控制系统安全的快速发展必将成为必然。

04 附录

缩略语	英文	中文
APT	Advanced Persistent Threat	高级持续性威胁
CII	Critical Information Infrastructure	关键信息基础设施
CIP		
CNVD	China National Vulnerabilities Database	国家信息安全漏洞共享平台
	Configuration	组态
CSSP	Control System Security Program	控制系统安全项目
CVE	Common Vulnerabilities and Exposures	-
CVSS	Common Vulnerability Scoring System	通用漏洞评分系统
	Cyberwar	网络战
	Cybercrime	网络犯罪
DCS	Distributed Control Systems	集散控制系统
DHS	The U.S. Department of Homeland Securty	美国国土安全部
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
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
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院
OPC	OLE for Process Control	用于过程控制的 OLE
PLC	Programmable Logic Controller	可编程逻辑控制器
RTU	Remote Terminal Unit	远程终端
RAT	Remote Access Terminator	远程访问终端
SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制系统
RBVS	Remote block valve station	可进行数据监视的阀室
RCBV	Remote control block valve station	-
SCS	Station control system	站控系统
GMC	General Management - Dispatch Center	总调指挥中心
DCC	District Command Center	地区调度管理中心
RCC	Regional Control Center	区域控制中心

表3 缩略语中英文对照

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于网络安全技术的研究，
为政府、运营商、金融、能源等行业提供优质的安全产品与服务。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com.cn