NSFOCUS

2019 工业控制系统信息安全保障框架

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 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，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，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安全运营等专业安全服务。

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。

特别声明

为避免合作伙伴及客户数据泄露，所有数据在进行分析前都已经过匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

目录

1

工控信息安全的发展

1.1 工业智能化发展概述

工业控制系统的发展历程如图所示。

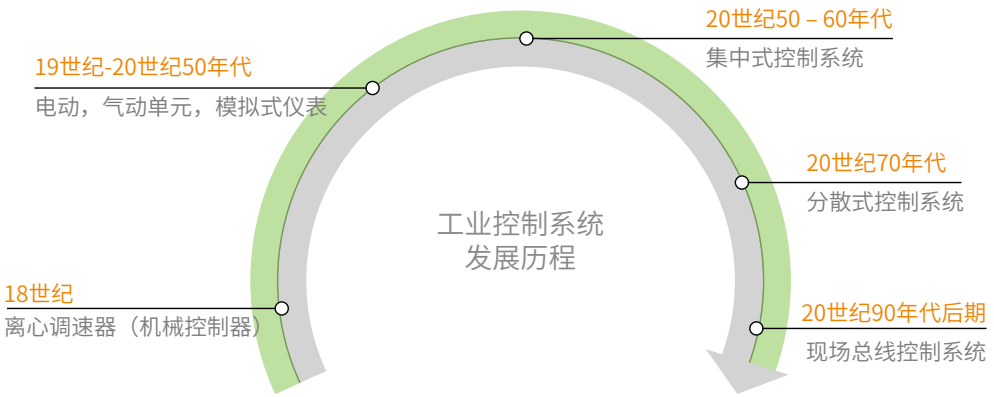


图 1.1 工业控制发展历程

工业控制系统最早可以追溯到 18 世纪。詹姆斯·瓦特在改良蒸汽机的工作中，给蒸汽机加装了一个节流控制器，即离心调速器。离心调速器通过一根与蒸汽机共同转动的轴来获得反馈信号，通过离心力来调节飞球的位置，进而调节蒸汽节流器以控制蒸汽机转速。这种离心调速器被认为是自动调节与自动控制的开始。

从离心调速器出现以后的一个多世纪的时间里，绝大部分的工业控制系统所关注的重点是对蒸汽系统中的温度，压强，液面以及机器转速的控制。随着工业系统的发展以及第二次世界大战中军事上的诸多控制问题的需要，从 19 世纪中期到 20 世纪中期，控制理论和控制系统有了全面的发展，相继出现了气动控制装置，继电器控制装置，伺服系统，反馈回路控制部件等工业控制设备，同时，负反馈，控制系统稳定性等理论也相继出现。

到了 20 世纪 50 – 60 年代，计算机技术进入到工业控制系统中，工业控制系统中的模拟控制电路逐渐被数字控制电路所取代，可编程逻辑控制器（Programmable Logic Controller, PLC）逐步替代继电器控制电路。由于系统全面数字化，控制系统可以使用更加先进复杂的控制算法来实现更加复杂的控制过程，工业控制系统发生了质的飞跃。但是到目前为止，工业控制系统还是集中式控制系统。

到了 20 世纪 70 年代中期，由于工业设备大型化，工艺流程连续性要求的增加，以及需要控制的参

数增多，集中式控制系统已经无法满足工业控制系统的需要。因此，集中式控制系统逐渐被分布式控制系统所取代。越来越多的工业控制领域，包括机械制造，石油化工，冶金，汽车，轻工业等都逐渐采用了分布式控制系统。

到了 20 世纪 90 年代后期出现了集计算机技术，网络技术，控制技术于一体的现场总线控制系统（Fieldbus Control System, FCS）。相比于分布式控制系统，现场总线控制系统具有更高的可靠性，更强的功能，更灵活的结构，更强的适应性等特点。

1.1.1 工业控制的基本架构

工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，如监控和数据采集系统（SCADA），分布式控制系统（DCS），还有其他较小的控制系统如可编程逻辑控制器（PLC）等。工业控制系统的逻辑架构如下图所示：

图 1.2 工业控制系统架构图

工业控制系统的现场设备层主要用于采集现场仪表的模拟量和数字量，不同场景下定义不同，如压

力、温度、湿度等内容。现场控制层主要通过控制器采集各个现场仪表的数据，通过内部既定的逻辑来对仪表的运行状态进行监视。在有闭环控制的场景下，实现对采集量的调整和处理。监督控制层是基于 IT 计算机的计算环境，通过与控制器之间的多种连接方式实现对控制器数据的采集、处理和展示。组态软件通过对业务对象的数据指标进行配置实现对业务逻辑的控制。同时，为了适配不同应用场景下的展示，可以通过画面组态的方式把采集的 I/O 点与业务应用场景进行对应，对于生产的历史数据进行分析和呈现。生产管理层主要完成对生产计划的处理，业务工艺指令的调优及调度指令的控制等，更加偏重于计划任务的管理。

1.1.2 工业 4.0 的发展

德国于 2013 年在汉诺威工业博览会上提出“工业 4.0”的概念，预计投资 2 亿欧元，推动以信息物理系统（CPS）为基础，以生产高度数字化、网络化、机器自组织为标志的工业革命。通过提升制造业的计算机化、数字化与智能化，建立具有适应性与资源效率的智能工厂（Smart Factory），并在商业流程及价值流程中整合客户以及商业伙伴。

从工业发展的历程来看，蒸汽机技术推动机械化生产的普及，使人类社会进入工业 1.0 时代；电力的出现推动规模化生产，从此工业进入 2.0 时代；信息化技术的应用，使得自动化生产成为可能，工业进入 3.0 时代；而物联网等新技术与工业技术的深度融合，使得工业进入智慧化的时代，即工业 4.0。工业 4.0 是在个性化智能产品的需求驱使下，并在物联网、大数据等新技术的有力支撑下出现的新一代变革。

工业 4.0 具备三个主要特征：

- 垂直整合：各机器及生产线的自控系统、工厂的制造执行系统（MES）、以及 ERP 等系统的整合，打破信息化系统与自动化系统之间的历史鸿沟，使工厂与企业的生产制造能力得以优化；
- 水平整合：企业内部及跨企业边界的各业务系统之间的整合，使得信息的共享、业务功能的组合可以跨越组织的边界，使价值链的整体竞争力得以提升；
- 端到端价值链的数字化整合：这是实现“智能制造云”的愿景，用户只要提交需求，就可以获得所需的产品，而云端相关价值链各企业的制造与业务能力都以 API 的方式发布，使得快速柔性组合与安全调度执行成为可能，最大化发挥生态系统的设计、制造、服务等多方面的综合能力。

随着物联网等技术的成熟，传统工业将经历企业内的厂际互联（M2M），到价值链上所有企业互联（B2B），再到消费者与相关工厂间互联（C2M），逐步完成向着工业 4.0 的变革。工业 4.0 的转型将为企业带来全面的业务价值与能力的提升，主要集中在加速产品创新，优化生产运营及交付全新服务三个方面。具体而言：

- 企业具备生产制造的高灵活性和更能适应市场的生产流程；
- 在完善全面产品生命周期管理，企业生产价值链互联互动之后，企业已经具备专业化的聚焦特定用户需求的能力；
- 提升以价值链为单位的整体竞争能力；
- 通过新的服务与业务模型开创新市场。

工业 4.0 可以促使制造型企业以前所未有的速度应对客户需求。这些技术将提升生产流程的柔性，速度，效率和质量。此外，工业 4.0 将催生新的商业模式、生产流程和其他创新。随着越来越多的制造型企业通过投资工业 4.0 技术实现或者增强其产品定制化程度，更高级别的大规模定制将成为可能。

1.1.3 工业互联网的发展

工业互联网是全球工业系统与高级计算、分析、传感技术以及互联网的高度融合。它通过智能机器间的连接并最终将人机连接，结合软件和大数据分析等技术，重构全球工业，激发生产率，让世界更快速、更安全、更清洁且更经济。在传统的工业控制系统中，虽然目前大部分的工控场景都实现了 IT 化，但是各工业企业之间的信息交互较少，也很少有工业企业与用户，供应商之间的实时的信息交互。因此，传统的工业企业之间，企业与用户之间的协调效率较低。而工业互联网可以有效的整合工业系统中的信息资源，有效降低工业生产的成本，提高生产效率，并能够实现工业生产的个性化，智能化。

工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的工业云平台。其本质是通过构建精准、实时、高效的数据采集互联体系，建立面向工业大数据存储、集成、访问、分析、管理的开发环境，实现工业技术、经验、知识的模型化、标准化、软件化、复用化，不断优化研发设计、生产制造、运营管理等资源配置效率，形成资源富集、多方参与、合作共赢、协同演进的制造业新生态。关于工业互联网平台有四个定位：

第一，工业互联网平台是传统工业云平台的迭代升级。从工业云平台到工业互联网平台演进包括成本驱动导向、集成应用导向、能力交易导向、创新引领导向、生态构建导向五个阶段。工业互联网平台在传统工业云平台的软件工具共享、业务系统集成基础上，叠加了制造能力开放、知识经验复用与开发者集聚的功能，大幅提升了工业知识生产、传播、利用的效率，形成了海量的开放 APP 应用与工业用户之间相互促进、双向迭代的生态体系。

第二，工业互联网平台是新工业体系的“操作系统”。工业互联网的兴起与发展将打破原有封闭、隔离又固化的工业系统。扁平、灵活而高效的组织架构将成为新工业体系的基本形态。工业互联网平台依托高效的设备集成模块、强大的数据处理引擎、开放的开发环境工具、组件化的工业知识微服务，向下对接海量工业装备、仪器、产品，向上支撑工业智能化应用的快速开发与部署，发挥着类似于微软 Windows、谷歌 Android 系统和苹果 iOS 系统的重要作用。

第三，工业互联网平台是资源集聚共享的有效载体。工业互联网平台将信息流、资金流、人才创意、制造工具和制造能力在云端汇聚，将工业企业、信息通信企业、互联网企业、第三方开发者等主体在云端集聚，将数据科学、工业科学、管理科学、信息科学、计算机科学在云端融合，推动资源、主体、知识集聚共享，形成社会化的协同生产方式和组织模式。

第四，工业互联网平台是打造制造企业竞争新优势的关键抓手。当前，GE、西门子等国际领军企业围绕“智能机器 + 云平台 + 工业 APP”功能架构，整合“平台提供商 + 应用开发者 + 海量用户”等生态资源，抢占工业数据入口主导权，培育海量开发者，提升用户粘性，不断建立、巩固和强化以平台为载体，以数据为驱动的工业智能化新优势，抢占新工业革命的制高点。

1.1.4 国内工业控制系统的发展

新中国成立尤其是改革开放以来，我国制造业持续快速发展，建成了门类齐全、独立完整的产业体系。2013 年以来，我国相继出台了一系列政策鼓励工业云的发展。2015 年，我国提出了《中国制造 2025》的制造战略计划，旨在实现我国制造业从制造大国向制造强国的转变。但是我国仍处于工业化进程中，与先进国家相比还有较大差距：制造业大而不强，自主创新能力弱，关键核心技术与高端装备对外依存度高，以企业为主体的制造业创新体系不完善；产品档次不高，缺乏世界知名品牌；资源能源利用效率低，环境污染问题较为突出；产业结构不合理，高端装备制造业和生产性服务业发展滞后；信息化水平不高，与工业化融合深度不够；产业国际化程度不高，企业全球化经营能力不足。

1.1.5 泛在化的工业设施

泛在技术也叫泛在网络技术，是指广泛存在的网络。它以无所不在、无所不包、无所不能为基本特征，以实现在任何时间、任何地点、任何人、任何物都能顺畅地通信为目标。泛在化的工业设施是将泛在化的技术应用在工业控制系统中，是工业控制系统的进一步延伸与发展。传统的工业控制系统多是指工厂中的生产控制，过程控制等系统。随着互联网技术，信息技术的发展，工业控制系统已经不仅仅局限在工厂中，其思想和方法进入了各个领域，例如路灯控制与维护，智能楼宇，车联网等。

路灯系统的特点是点多，面广，路灯设施陈旧且分散，灯具数量种类多，设施维修费用高。每年用于路灯的控制，巡检及更换灯具的人工机具车辆等需要花费不少费用。采用智能控制器取代传统的人工基于钟控方式的控制系统，可以自动调整路灯的开关时间，在有效节约电能的同时，可以减少人工成本。将路灯进行联网，将物联网与节能技术相结合，可以减少路灯的巡检及维护的费用。将路灯的巡查管理交由计算机系统自动完成，每天自动生成故障报表，并且将故障自动报警到值班人员的手机上，可以大大提高管理水平和管理效率，节约维护费用，也使市政路灯管理上升到一个新的高度和水平，对国家发展低碳经济，节能减排也起到积极的推动作用。

楼宇智能化也是未来的发展趋势。正如工业中生产设备的调度与管理越来越智能化一样，楼宇中的设备，包括暖通空调系统，照明系统，安防系统，消防系统，智能电网系统等也需要智能化的调度与协调。例如暖通空调系统和照明系统可以根据环境情况和室内人员的喜好智能调整状态，给人员提供个性化的生产生活环境。智能消防系统可以在发生火情的时候高效的进行人员疏散和控制火情。智能电网系统可以根据建筑的用电负荷与建筑自身的光伏，风机，热电联产等发电设备的状态实时调节清洁能源的接入比例，达到节能减排的目的。同时，智能楼宇是智慧城市的一部分。在智慧城市中，建筑之间必将要彼此交互信息，例如建筑的能耗信息，新能源的产出信息，停车位信息等。通过信息的交互，可以对建筑的资源进行有效的协调，并达到低碳环保的目的。

不论是智能化的路灯系统，还是智能建筑和智慧城市，都是分布式系统，其运转都离不开云计算技术和边缘计算技术。云计算技术能够将 IT 应用和业务化繁就简，服务于企业和最终用户。但是位于数据中心的云计算技术并不能很好的满足那些延迟敏感的应用。这些应用需要在其附近的节点完成计算，以满足最小时延的要求。因此，边缘计算应运而生。边缘计算技术扩大了以云计算技术为特征的网络计算范式，将网络计算从网络的中心扩展到网络的边缘，从而广泛运用于更多的应用形态和服务类型。边缘计算的基本特征有以下几点：低延迟和位置感知，更加广泛的地理分布，更大范围的移动性，适合更

多的节点等。边缘计算在无线接入的应用中起主导作用，在实时和流媒体应用中更有价值。

边缘计算为工业互联网系统提供了更加完备的解决方案。云计算技术不能够满足工业互联网的实时性的要求，因此，工业互联网将普遍采用边缘计算技术。将部分分析和控制的计算任务放在网络的边缘可以满足工业系统的实时性要求。同时，通过边缘的分布式智能和自治系统相互协同，而不是依靠中心化的智能，可以保障整个系统的本地存活能力，提高工业系统的稳定性。

以车联网为例，车联网应用和部署要求具有丰富的连接方式和相互作用：车到车，车到接入点（无线网络连接、3G/4G/5G、路边单元、智慧交通灯），以及接入点到接入点等。随着人工智能的发展，自动驾驶时代即将来临。在整个行驶的过程中，自动驾驶车辆除了通过各类传感器感知车外的道路状态之外，还需要不断地获取前方道路的交通流量情况，用来做路径的动态规划。而车辆获取实时交通路况以及交通事件就需要实现车辆与路边基础设施的通信。车辆进入收费通道，实现不停车无人收费，也需要实现与路边基础设施的通信。车联网技术可以使自动驾驶更加安全可靠。为了保证自动驾驶的安全可靠，车联网对实时性具有很高的要求。边缘计算技术能够更加实时的提供车联网服务所需的信息和数据分析能力，以及地理分布（整个城市和公路沿线）情况。因此，边缘计算技术将是未来车联网的技术依托。

综上所述，传统的工业控制系统及其思想正在走出工厂，应用到生活的方方面面。而云计算技术和边缘计算技术是泛在化工业设施的技术依托。

1.2 工控信息安全的发展

随着工业信息化进程的快速推进以及工业互联网、工业云等新兴技术应用的兴起，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。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采用的专用系统、封闭运行的模式，开始在系统中采用一些标准的、通用的通信协议及软硬件系统，甚至有些工业控制系统也能以某些方式连接到互联网中，打破封闭网络的屏障优势，使得工业控制系统面临更多的威胁。由于工业控制系统多被应用在电力、交通、石油化工、核工业等国家的重要行业中，网络攻击行为所导致的工业控制系统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、信仰等目的，敌对的组织、国家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。

以“震网病毒”为代表的一系列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。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没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提供的系统或者应用软件更加关注工业控制系统的功能实现，往往忽视信息安全的因素，尤其是在国内的工控系统即使有工控安全的解决方案，往往由于业主方没有明确需求而不会主动配置。

工业控制系统脆弱的安全状况以及所面临的日益严重的攻击威胁已经引起了各个国家的高度重视，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，各个国家也在政策和科研层面上积极开展工业控制系统的安全保障工作。

1.2.1 工控信息安全与 IT 信息安全的差异

随着工业信息化的快速发展，工业控制系统也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。这将促使基于 IP 的通信方式成为工业控制系统中的基础通信支撑手段。例如，采用 PC 服务器，通用操作系统和通用数据库等 IT 产品，逐步采用基于 TCP/IP 协议的工业以太环网和 OPC 通信协议等。为了保证工业控制系统的兼容性，网络的应用层将逐渐采用专用的工业控制协议。互联网技术的应用将打破企业生产系统的封闭性，实现企业管理与控制的一体化，提高企业信息化水平，为企业实现生产、管理系统的高效集成奠定基础。但是，工业控制系统与传统 IT 信息系统建设目标不同，这导致它们在技术、管理与服务等很多方面有相当大的差异。一些典型的差异见表 1.1 。

表 1.1 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。	由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，并有可能根据需要进行功能裁减或定制。	采用通用操作系统（Windows、UNIX、Linux 等），尤其是 Windows 系列操作功能更加强大。
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）。
数据保密性	控制数据的保密性除特定行业外要求不高。	数据保密性要求高。
存储空间限制	系统存储空间较少，可实现的功能比较单一	存储空间大，可实现更加复杂的功能。

工控信息安全的发展

对比项	工业控制系统（ICS）	传统 IT 信息系统
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根据 IT 系统的要求而定。
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。

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。在大部分情况下，保密性是传统信息安全领域最重要的部分。在工业控制系统领域则有较大的不同。工业控制系统强调的是工业自动化程度及对相关设备的智能控制、监测与管理能力。工业控制系统在系统架构、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。因此，在工业控制系统中需要首先保证系统设备的可用性和完整性。而由于工控系统中传输的数据通常是控制指令和采集的原始数据，而且多是实时数据，需要放在特定的环境下分析才有意义，因此对保密性的要求最低。

工业控制系统作为工业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机制。除了工控系统供应商人员外，外部人员一般情况下不允许进入到控制系统运行的物理环境中。同时，工业控制系统本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，也就是说其工作环境相对封闭。而且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）实现系统间的通信。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的资料支持。因此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，从而相关的工业系统及通信规约的安全缺陷（或漏洞）也很少被发现。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缺乏系统的考虑。

从 2000 年以后各种由于信息安全问题导致的工业控制系统运行问题的情况层出不穷，尤其以 2010 年“震网”为代表的安全事件及后续一系列工控安全事件表明，工业控制系统已经不是一方净土，其面临的威胁及导致的影响日益严重。

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 1.2 从多个角度对这些差异进行了讨论分析。

表 1.2 工业控制系统安全与传统 IT 系统安全对比

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 （例如 StuxNet、Duqu 等）。 • 采用有组织的多攻击协同模式。	• 常用攻击方式：拒绝服务、病毒、恶意代码、非授权使用、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。 • 部分控制设备采用硬件方式认证，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。 • 用户身份管理系统多采用软件实现，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。 • 使用相对陈旧的系统， 也可能因厂商已经不存在或厂商不再进行产品的安全升级支持，造成系统漏洞无法及时被修补。	• 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需要严格防止系统被误操作与蓄意破坏。 • 通常缺乏针对 ICS 的安全日志审计及配置变更管理机制。	• 一般有比较完善的 IT 系统及网络行为审计机制。
	应急响应	• 需要具备保障 ICS 系统业务连续性的应急响应计划，强调快速响应。	• 应急响应计划视实际需求而定。

1.2.2 工控信息安全在国内的发展

工控信息安全的发展

当前，随着我国工业化和信息化的深度融合以及物联网的快速发展，工控系统面临的风险点在逐步增多。同时，工控系统中信息安全问题对业务系统的影响也由于外部威胁情况的变化在不断加剧。建立全面的工控信息安全保障体系，减少工控系统面临的内外部的威胁，为两化深度融合、工业转型升级保驾护航，是当前工控信息安全领域面临的重大挑战。

现阶段我国工控系统的安全形势非常严峻。调查发现，约 80% 的企业从来不对工控系统进行升级和漏洞修补；有 52% 的工控系统与企业的管理系统、内网甚至互联网连接；此外，一些存在漏洞的国外工控产品依然在国内的某些重要装置上使用。更为严重的问题还在于，我们缺乏发现风险源头的手段，缺乏必要的控制风险的技术与方法的研究。

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，相继出台了一系列的标准与法规。

- 2010 年全国信息安全标准化技术委员会（TC260）制定了《工控 SCADA 安全指南》。
- 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的工业控制系统安全管理的要求。
- 国务院也在 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。加强对核设施、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；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进行安全测评，实行安全风险和漏洞通报制度。
- 2016 年工信部为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28 号），保障工业企业工业控制系统信息安全，制定《工业控制系统信息安全防护指南》，主要从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任 11 个方面对工业控制系统安全的防护提出了指导性意见。

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的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。另外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，缺乏与实际工业现场应用习惯的融合，导致现场人员的使用仍然存在的一定的障碍。而工业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。

建立在融合实际业务特征与信息安全技术特性的基础上的工业信息安全技术才能满足业务运行保障的需求，符合实际工业环境的特点，真正满足工业控制系统的安全保障需求，相关的产品业务发展才能真正进入到正轨。

在政策法规方面，目前国内已经出台了一系列相关的法规和标准来指导和规范工控信息安全，如下所示。

政策法规：

- 《中华人民共和国网络安全法》
- 《关于加强工业控制系统信息安全管理的通知》—工信部协 [2010]451 号
- 《工业控制系统信息安全防护指南》—工信部信软 [2016]451 号文
- 《工业控制系统信息安全事件应急管理工作指南》—工信部信软 [2017]122 号
- 《工业控制系统信息安全防护能力评估工作管理办法》—工信部信软 [2017]188 号
- 《电力监控系统安全防护规定》—发改委 14 号令
- 《电力监控系统安全防护总体方案》—国能安全 [2015]36 号文

国家标准：

1. **全国信息安全标准化技术委员会（TC 260）已在编和计划制定如下标准：**

- 《信息安全技术 SCADA 系统安全控制指南》
- 《信息安全技术 安全可控信息系统（电力系统）安全指标体系》

- 《信息安全技术 工业控制系统安全管理基本要求》
- 《信息安全技术 工业控制系统安全检查指南》
- 《信息安全技术 工业控制系统测控终端安全要求》
- 《信息安全技术 工业控制系统安全防护技术要求和测评方法》
- 《信息安全技术 工业控制系统安全分级指南》

2. **全国电力系统管理及其信息交换标准化技术委员会（SAC/TC 82）已制定如下标准：**

- GB/Z 25320.1-2010《电力系统管理及其信息交换 数据和通信安全 第 1 部分：通信网络和系统安全 安全问题介绍》（2010 年 11 月 10 日发布，2011 年 5 月 1 日起实施）
- GB/Z 25320.2-2013《电力系统管理及其信息交换 数据和通信安全 第 2 部分：术语》（2013 年 2 月 7 日发布，2013 年 7 月 1 日起实施）
- GB/Z 25320.3-2010《电力系统管理及其信息交换 数据和通信安全 第 3 部分：通信网络和系统安全 包括 TCP/IP 的协议集》（2010 年 11 月 10 日发布，2011 年 5 月 1 日起实施）
- GB/Z 25320.4-2010《电力系统管理及其信息交换 数据和通信安全 第 4 部分：包含 MMS 的协议集》（2010 年 11 月 10 日发布，2011 年 5 月 1 日起实施）
- GB/Z 25320.5-2013《电力系统管理及其信息交换 数据和通信安全 第 5 部分：GB/T 18657 等及其衍生标准的安全》（2013 年 2 月 7 日，2013 年 7 月 1 日起实施）
- GB/Z 25320.6-2011《电力系统管理及其信息交换 数据和通信安全 第 6 部分：IEC 61850 的安全》（2011 年 12 月 30 日发布，2012 年 5 月 1 日起实施）
- GB/Z 25320.7-2015《电力系统管理及其信息交换 数据和通信安全 第 7 部分：网络和系统管理（NSM）的数据对象模型》（2015 年 5 月 15 日发布，2015 年 12 月 1 日起实施）

3. **全国工业过程测量控制和自动化标准化技术委员会（SAC/TC 124）已制定和在编如下标准：**

- GB/T 26333-2010《工业控制网络安全风险评估规范》（2011 年 1 月 14 日发布，2011 年 6 月 1 日起实施）
- GB/T 30976.1-2014《工业控制系统信息安全 第 1 部分：评估规范》（2014 年 7 月 24 日发布，

2015 年 2 月 1 日起实施）

- GB/T 30976.2-2014《工业控制系统信息安全 第 2 部分：验收规范》（2014 年 7 月 24 日发布，2015 年 2 月 1 日起实施）
- 《工业控制计算机系统 通用规范 第 2 部分：工业控制计算机的安全需求》（在编）

4. **工业和信息化部已发布以下标准**

- JB/T 11961-2014《工业通信网络 网络和系统安全 术语、概念和模型》（2014 年 5 月 6 日发布，2014 年 10 月 1 日起实施）
- JB/T 11962-2014《工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术》（2014 年 5 月 6 日发布，2014 年 10 月 1 日起实施）

行业标准

1. **全国电力监管标准化技术委员会（TC 296）已在编如下标准：**

- 《电力二次系统安全防护标准》（强制）
- 《电力信息系统安全检查规范》（强制）
- 《电力行业信息安全水平评价指标》（推荐）

2. **中国电力企业联合会已制定如下标准：**

- GB/T 31991.1-2015《电能服务管理平台技术规范 第 1 部分：总则》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31991.2-2015《电能服务管理平台技术规范 第 2 部分：功能规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31991.3-2015《电能服务管理平台技术规范 第 3 部分：接口规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31991.4-2015《电能服务管理平台技术规范 第 4 部分：设计规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31991.5-2015《电能服务管理平台技术规范 第 5 部分：安全防护规范》（2015 年 9 月

11 日发布，2016 年 4 月 1 日起实施）

- GB/T 31960.1-2015《电力能效监测系统技术规范 第 1 部分：总则》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.2-2015《电力能效监测系统技术规范 第 2 部分：主站功能规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.3-2015《电力能效监测系统技术规范 第 3 部分：通信协议》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.4-2015《电力能效监测系统技术规范 第 4 部分：子站功能设计规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.5-2015《电力能效监测系统技术规范 第 5 部分：主站设计导则》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.6-2015《电力能效监测系统技术规范 第 6 部分：电力能效信息集中与交互终端技术条件》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.6-2015《电力能效监测系统技术规范 第 7 部分：电力能效监测终端技术条件》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）
- GB/T 31960.8-2015《电力能效监测系统技术规范 第 8 部分：安全防护规范》（2015 年 9 月 11 日发布，2016 年 4 月 1 日起实施）

3. **国家烟草专卖局**

- 《国家烟草专卖局办公室关于转发公安部 2016 年公安机关网络安全执法检查工作方案的通知》（国烟办综〔2016〕257 号）
- 《烟草工业企业生产网与管理网网络互联安全规范》（YC/T 494-2014）
- 《国家烟草专卖局关于印发烟草行业信息化发展规划（2014—2020 年）的通知》（国烟办〔2014〕370 号）
- 《烟草行业信息系统安全等级保护实施规范》YC/T 495-2014

- 《烟草行业工业控制系统网络安全技术规范》—修订稿

- **国内产业联盟发展动态：**

2014 年 4 月 17 日，“工业控制系统信息安全产业联盟”由中国电子技术标准化研究院信息安全研究中心、全国工业过程测量控制和自动化标准化技术委员会、公安部第三研究所、工信部电子科学技术情报研究所、中国软件评测中心、中国仪器仪表行业协会等涉及国家主管部门、工控系统厂商、信息安全厂商以及行业用户的 24 家单位共同发起，以“搭建政府、用户、企业、科研院所、大专院校之间的交流平台，发挥纽带与桥梁的作用，共同推进我国工业控制系统信息安全产业发展，保障关键基础设施安全稳定运行，支撑中国工业健康可持续发展”为宗旨，致力于为我国工业控制系统信息安全在体系建设、等级保护、风险评估、标准制定、产品开发和评测等方面搭建一个交流平台。

2017 年 6 月 8 日，国家工业信息安全产业发展联盟成立。该联盟接受工业和信息化部业务指导，其使命和任务为：一是要通力合作，将联盟打造成为政府和产业界协同联动的平台；二是要融合发展，将联盟建设成为自动化、信息化与信息安全领域的跨界融合平台；三是要牵引带动，将联盟培育成为行业资源整合、对接、推广的平台。工业和信息化部将会同有关部门加强业务指导，支持联盟开展技术研发、标准化、试点示范、公共服务平台建设、国际交流合作等工作，促进形成政产学研用高效联动的发展格局。目前联盟首批成员单位已达 149 家，包括神华集团、中车集团、航空工业、中国兵装、中国电子信息产业集团等 18 家副理事长单位，中核集团、中船重工、中石化、中钢集团、中国烟草等 45 家理事单位。

- **行业现状：**

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。在 2014 年后，随着发改委 14 令和已经预制配套的国能安全 36 号的发布，各个电力企业尤其是发电企业在原有的“网络专用、安全分区、横向隔离、纵向加密认证”的基础上增加了对综合防护的要求，强化了不同区域之间的安全隔离及系统内部的安全防护。

烟草行业逐步开展了生产网与办公网之间隔离，增强了办公网与生产网之间连接的安全性，同时开展了针对中烟生产系统的安全建设试点工作，商业烟草的物流和分拣也开始了相关的试点建设工作。

石油石化领域是国内较早开始工控安全建设的行业，目前在一些主要的采油厂、联合站或者炼化车间都实现了控制网络与 MES 网络之间的隔离，部分生产单元开展了系统的工控安全建设的试点。另外，

轨道交通、冶金、关键制造业等领域随着相关的监管要求的加强及控制系统面临的安全问题不断出现及导致的影响加剧，都在逐步开展相关的工控安全建设。

1.2.3 国外工控信息安全的发展

自从 2010 年震网病毒事件之后，世界各国对工控系统安全问题的关注被提升到一个新的高度。世界各国都在政策、标准、技术、方案等方面展开了积极应对。

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基于 CIP 系列标准的要求在北美开展针对电力企业的安全检查（包含核电）；欧洲已经按照 WIB 标准来检测工控产品安全。以德国为代表的国家已经开始基于 ISO 27000 系列的 ISO 27009 标准进行工控安全的建设；日本基于 IEC 62443，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。

作为信息产业发展的领导者，美国很早就十分重视工控系统的安全，2003 年将其视为国家安全优先事项；2008 年则将其列入国家需重点保护的关键基础设施范畴；2009 年颁布《保护工业控制系统战略》，涵盖能源、电力、交通等 14 个行业的工控系统的安全。同年，在 CERT 组织下面成立工业控制系统网络应急响应小组 (ICS-CERT)，专注于工业控制系统相关的安全事故监控、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；通过信息产品、安全通告以及漏洞和威胁信息的共享来监控工业控制系统安全事件及分析行业安全态势，并以季度报告的方式公开发布。美国国土安全部 (The U.S. Department of Homeland Securty，DHS) 启动的控制系统安全计划 (Control System Security Program，CSSP) 则依托工业控制系统模拟仿真平台，综合采用现场检查测评与实验室测评相结合的测评方法来实施针对工业控制系统产品的脆弱性分析与验证工作。美国国家标准与技术研究院、能源局则分别发布了《工业控制系统安全指南》(SP800-82。2013 年推出最新修订版本)[NIST]、《改进 SCADA 网络安全的 21 项措施》等相关的工控系统的安全建设标准指南或最佳实践文档。同时其国内的传统信息安全厂商赛门铁克、MCAFEE、思科以及传统工控厂商如罗克韦尔、通用电气以及一些新兴的专业工控安全厂商在工控系统的安全防护及产品服务提供方面也都展开了深入研究、实践及产业化工作，在总体上处于领先的地位。

在欧洲，以德国西门子、法国施耐德电气为代表的工业控制系统提供商为用户提供相应的安全产品、

服务及相应的解决方案。例如，德国西门子研究院设有工控安全实验室，可提供安全咨询服务、培训。工控安全产品方面则有工控防火墙及相应的工控安全解决方案。在工控系统领域的许多行业，例如来自欧洲的西门子、施耐德电气具有绝对的技术与市场优势。而工控系统的信息化、智能化以及所带来的安全问题的解决离不开工控厂商的支持。西门子和施耐德等企业的市场和技术优势也将奠定未来很长一段时间内其在工控安全领域的领先地位。

在专业的工控安全厂商方面，加拿大 Tofino(多芬诺) 公司曾凭借其业内著名的工控系统防火墙成为业内领先的工控系统安全的专业厂商，其产品在石化等多个行业应用广泛。科诺康公司 (Codenomicon) 则以其用于漏洞发现的 fuzzing 测试工具而在工控系统安全领域拥有重要的地位。此外，还有一些开源组织提供相应的工控安全工具，例如 Nessue。它分为专业版 (收费) 和免费评估测试版。其专业版可利用相应的工控系统安全插件，对 SCADA 系统或 PLC 的控制设备的脆弱性进行检测评估。

在工控安全的国际标准研究方面， 2007 年，国际电工委员会 IEC/TC65/WG10 工作组与国际自动化协会 ISA 99 委员会共同制定 IEC 62443 系列标准。该系列标准自 2011 年调整后名称更改为《工业过程测量、控制和自动化网络与系统信息安全》，包括 4 个部分共 12 个文档：

- IEC 62443-1-1《术语、概念和模型》
- IEC 62443-1-2《术语和缩略语》
- IEC 62443-1-3《系统信息安全符合性度量》
- IEC 62443-2-1《建立工业自动化和控制系统信息安全程序》
- IEC 62443-2-2《运行工业自动化和控制系统信息安全程序》
- IEC 62443-2-3《工业自动化和控制系统环境中的补丁更新管理》
- IEC 62443-2-4《对工业自动化控制系统制造商信息安全政策与实践的认证》
- IEC 62443-3-1《信息安全技术》
- IEC 62443-3-2《区域和通道的信息安全保障等级》
- IEC 62443-3-3《系统信息安全要求和信息安全保障等级》
- IEC 62443-4-1《产品开发要求》

- IEC 62443-4-2《对 IACS 产品的信息安全技术要求》

为避免标准冲突，该系列标准也对荷兰石油天然气组织 WIB 标准和美国电力可靠性保护协会 NERC-CIP 标准等进行了整合。根据该系列标准开展的主要研究有：

1. 2010 年，美国开始 ISA 99 工业基础设施认证计划，在内华达实验室进行工控漏洞的挖掘和检测技术的研究，实现对相关工控设备的漏洞挖掘和漏洞验证；
2. 2013 年，日本开展基于 IEC 62443 的工控安全标准，针对日本上线前的工控系统进行安全验证；
3. 2015 年，IEC 针对产品生产商、供应商 / 系统集成商、运营商 / 资产拥有者建立了一套基于 IEC 62443 标准的网络安全评估体系。该评估体系是对产品、流程和人员的网络安全认证，能为资产拥有人提供保障，证明其产品符合 IEC 国际标准的安全要求。

1.3 工控信息安全的技术趋势

1.3.1 工控信息安全技术趋势

伴随着 IT 技术在工业现场应用的深度和广度不断扩大，工业控制系统所面临的安全风险也不断增加。工业控制安全系统原有的以边界隔离和边界防护为主要技术措施的安全防护体系逐步向与业务相关联、相融合的方向发展。在工业云与工业大数据等新的应用形态下，工控安全产品需要在功能和应用形态上突破现有产品的特点，以便于更好的适配新应用的需要。

1.3.2 主流工控信息安全产品介绍

工业控制系统的信息安全技术从大类上主要包括防护类，隔离类，监测类，检测类、运维管控类等。

- 防护类：
  - 网络防护：区别于传统 IT 防火墙，工业防火墙对进入工业网路中的数据包进行从 IP 层到应用层的深度分析，以白名单的方式来限制对 IP、协议功能码、操作行为等相关资源的访问。
  - 主机防护：通过构建主机的白名单体系或者构建主机应用软件的可信体系来判断相关的软件或者应用是否可以在本系统中运行，阻止不在白名单范围内的软件执行与进程启动。
- 隔离类

- 网闸类：主要采用 2+1 的方式或者 3+1 的方式，在两主机之间通过隔离卡进行通信，或者通过第三主机对两主机来下发策略实现有限的通信，目前在石油石化、冶金领域中广泛应用。
- 正反向隔离装置：内网和外网之间不建立 TCP/IP 的连接，内网主机和外网主机之间的通信通过单字节的回应机制来实现。对于反向隔离装置仍然需要进行基于数字证书的认证，在内外网之间建立有限的通信。目前在电力行业广泛应用。
- 工业隔离网关：目前有多种形式，有采用 2+1 的隔离形式，有采用两个防火墙对接的形式，可以有效对 OPC、modbus、S7 等工业协议进行过滤和处理，尤其是可以对读取和更改 OPC 的点表做细粒度的控制。

• 监测类：

- 工控审计：通过自定义或者自学习方式来构建通信行为基线，通过对通信行为的判别来发现超出基线行为的异常，对于出现的违背基线行为的操作进行告警并提供相关的处置建议。
- 工控 IDS：通过对数据包的深度解析，基于特征分析和异常检测来发现进入到或者潜藏在工业控制系统内的攻击行为，实现对攻击行为的有效感知和监测。
- 工业监测预警平台：基于对安全日志、网络日志、主机日志的管理和关联分析，同时结合工业现场运行的特点来发现和还原工业现场潜在的恶意行为。

• 检测类：

- 工控漏洞扫描：可以对工业现场中常见的 IT 操作系统、数据库、工业现场应用软件和工业控制器如 PLC、DCS 等设备和装置进行探测，发现其中潜在的安全漏洞。
- 工控漏洞挖掘：主要通过 FUZZ 等技术手段实现对协议健壮性的测试，通过发送指定协议的畸形报文，观测被检测设备在处理畸形报文时的异常，如通过 DOS 来发现系统潜在的漏洞。

• 运维管控类：

- 工业堡垒机：可以实现对运维过程的安全审计和身份管理。目前在工业现场不能通过前置机安装工业软件的情况下，通过集成与组态和 SCADA 等软件的接口来实现与上位机主机的通信，并对运维过程进行监控。
- 移动工业运维审计：针对现场外部运维人员的运维操作进行监控，发现运维操作中潜在的恶意行为，对恶意行为进行记录和阻断。

1.3.3 工控信息安全技术面临的问题和困难

工业控制系统信息安全目前面临着信息安全与工控系统自身安全融合的要求。目前工控安全产品还处于产品阶段的 1.0 版本的时代，与目前 IT 信息安全和 IT 系统的适配程度相比还有比较大的差距。工业控制系统安全产品是与业务应用相关度比较高的产品。目前的工控安全产品体现在与业务的融合度不够，在深度检测与业务相关的攻击行为的时候往往乏力，缺乏创新性的安全检测思路，防护思路往往缺乏真正有效的方法。

另一方面，随着工业领域中的一些新的应用，如工业云、工业大数据等的普及，工业控制的业态也必将发生一些变化。而信息安全技术与新的业态融合时，必然需要与业务进行融合。而目前工控信息安全技术的融合还没有完全展开，需要在技术方向和应用上有所突破。

2

工控信息安全态势

2.1 典型工业信息安全事件

随着工业控制系统信息化程度越来越高，系统越来越开放，针对工业控制系统的攻击也越来越多，造成的损害也将越来越大。针对工业控制系统的攻击主要是以系统中的 IT 网络为突破口，进而影响其 OT 系统的运行。目前针对工业控制系统攻击的目的主要三类：破坏工业控制系统的正常运行，获取工控系统数据和获取钱财。

破坏工业控制系统正常运行的攻击中比较典型的案例有震网病毒事件和乌克兰电网事件。

震网病毒被认为是最早的专门针对工业控制系统的攻击。攻击者通过病毒攻击伊朗核工厂的铀浓缩设备，包括上位机和物理系统，即离心机，从而缩短离心机的使用寿命，延缓伊朗的铀浓缩进程，严重破坏了伊朗核计划。此次攻击事件中，黑客最终的攻击目标是西门子公司的 SIMATIC WinCC 系统（该系统主要用于工控系统的数据采集与监控，通常都部署在专用的内部局域网中）。前期为了渗透到内部网络，攻击者首先通过社工的方式感染外部主机，然后感染 U 盘，利用快捷方式文件解析漏洞传播到内部网络。在内网中，通过对三种不同漏洞的利用实现联网主机之间的传播，最后抵达安装了 SIMATIC WinCC 软件的主机并展开攻击，攻击中共使用了 3 个零日漏洞。本次攻击中使用到的很多技术和方法皆非寻常攻击所能做到。

乌克兰电网在一年左右的时间内多次遭到攻击，导致停电事故。这些攻击涉及的恶意软件有两大块：BlackEnergy 木马和 KillDisk，旨在破坏文件，使系统无法运行插件。攻击者直接与系统的交互，发送切断电源命令，然后用 KillDisk 使用电恢复更加困难。另外，恶意软件 Industroyer 同样以破坏工控系统正常运行为目的，这个恶意软件使用的是全球范围内的工业通讯协议，它最终会实现对各地变电站的能源开关及断路器的控制。可以说，针对工业控制系统的攻击从针对 PLC、OPC 等通用性部件逐渐扩展到针对专用部件（例如变电站系统）的攻击。

以获取工业控制系统数据为目的的攻击主要是为了盗取生产工艺，监视企业或者国家的工业行为特征等。典型案例包括感染了全球至少 50 万台网络设备的 VPNFilter。VPNFilter 是一个多阶段模块化的恶意软件。在其第三阶段扩展的恶意组件中，有专门针对工控协议进行嗅探的组件，不仅对工控 modbus SCADA 协议进行情报收集，同时还会嗅探基于 http 协议的登录凭证信息和 Authorization 信息。

还有恶意软件 HAVEX 通过感染工业控制系统中的 SCADA 系统和 OPC 盗取系统中的信息与数据，包括被感染主机的操作系统版本，计算机名，用户信息，文件和目录的列表等，并上传到远程

C&C(command-and-control) 服务器，以达到监控企业和国家的工业行为特征的目的。

以获取钱财为目的的攻击是最近一些年出现的攻击方式，其主要攻击手段为勒索软件，例如 warnecry、clearenegy 等。

2016 年 11 月 28 日，旧金山 MUNI 城市捷运系统受到勒索软件攻击，所有的售票站点都显示出“你被攻击了，所有数据都被加密”，攻击者发出公告索要 100 比特币，按照当时价格换算合计 70000 多美元。

2017 年 5 月 13 日，受 WannaCry 的影响，雷诺宣布法国桑都维尔和罗马尼亚的工厂停产，以防止勒索软件在系统内扩散。除了雷诺，日产位于英国东北部桑德兰的制造工厂也受到影响。

2018 年 3 月，亚特兰大市遭受一起勒索软件攻击，导致关键的城市服务瘫痪了几天。亚特兰大市对此花费了近 500 万美元以获得紧急 IT 服务，成本包括事件响应服务、危机公关、扩充支持人员和主题专家咨询服务相关的费用。

2018 年 8 月 3 日，台积电位于台湾新竹科学园区的 12 英寸晶圆厂和营运总部遭遇勒索软件 WannaCry 变种的攻击，导致生产线停摆，造成 1.7 亿美元的损失。此次在生产线隔离网络中出现的事故是由于失误操作造成的。机台上线之后才进行扫毒，导致未安装补丁的新机台受到病毒感染，最终传染至全部机台。受到攻击的机台由于没有联网，并没有弹出勒索的界面，但是这次攻击却导致了被感染设备的停产。台积电事件虽然发生在工控系统内部，但本质上还是由一般的病毒引起。这次事件表明，即使是普通病毒的攻击，在工控系统内也有可能造成严重的生产事故。

此类勒索软件攻击事件说明，勒索软件已经开始逐渐向工业控制系统进行渗透。有些事故的发生暂未造成生产事故和人身事故，但数据恢复成本有时远超过赎金成本，给企业和社会都带来了重大损失和影响。

虽然勒索病毒与传统的类似震网病毒等专门针对工控系统的病毒都可以导致工控系统无法正常运行，但是它们之间有很大区别。首先，勒索病毒针对一般的 IT 系统设计，而传统的工控系统病毒针对工控设备进行设计，有明确的攻击目标和预期结果。其次，目前的勒索病毒主要基于通用操作系统进行设计，例如 Windows，所以其主要运行在工控系统中的 HMI 中。而传统的工控系统病毒往往针对特定的工控设备进行设计，例如 PLC，DCS 等。最后，勒索病毒的主要目的在于获取钱财，而传统的工控系统病毒主要是为了破坏工控系统的完整性，使其无法正常运行。而随着工业信息系统的发展，有研究指出已经出现了针对 PLC 等工控设备的勒索病毒，其既能够导致工控系统无法运行，同时还能从中获利。

除了勒索软件以外，还出现了其他形式的旨在非法获取钱财的攻击，例如使用者对三一重工的重型机械进行非法解锁，导致三一重工公司的销售损失。

总体来说，随着 IT 与 OT 的加速融合，工业控制系统所面临的威胁越来越多。

2.2 工业控制系统恶意软件介绍

近年来，针对工控系统的恶意软件越来越多，破坏力也越来越大。下面针对几种主要的工业控制系统的恶意软件进行分析。

2.2.1 恶意软件 Industroyer 的介绍

- **Industroyer 事件概述：**

2017 年 6 月 8 日，安全公司 ESET 发现了针对工控系统的恶意软件 Win32/Industroyer， Dragos 通过对 ESET 分析结果进行验证后，6 月 12 日公布了 Win32/Industroyer 的 hash 信息以及分析报告。Industroyer 恶意软件的作者具有深厚的工控背景，尤其对电力系统工控协议非常熟悉。Industroyer 支持四种工控协议：

- IEC 60870-5-101 (aka IEC 101)
- IEC 60870-5-104 (aka IEC 104)
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

与 2015 年乌克兰断电恶意软件相比，Industroyer 功能结构更加高级，可以造成系统崩溃，无法提供正常服务。根据 Dragos 分析并推测，Industroyer 与 2016 年 12 月乌克兰断电事件有关。

- **Industroyer 恶意软件的攻击流程如下图所示。**

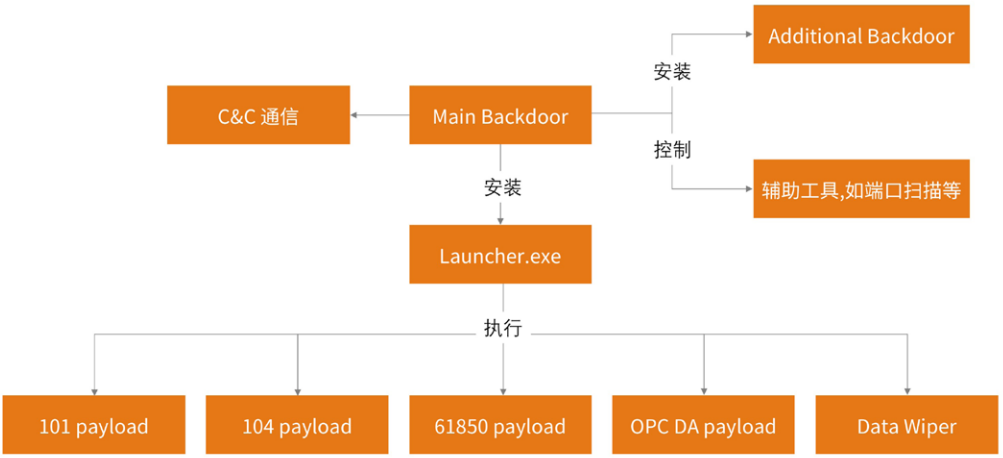


图 2.1 Industroyer 恶意软件的攻击流程

- **模块的功能如下：**

1. Main Backdoor

   Main Backdoor 通过本地代理 IP 的 3128 端口与远程 C&C 的 443 端口通信。远程可以通过 C&C 服务器在本地执行任意命令。

2. Launcher

   Launcher 模块负责加载 payload。一个新线程加载 payload.dll 文件，调用导出函数 crash，执行针对工控协议的攻击操作。另一个线程加载数据清理模块 haslo.dat，调用其导出函数 Crash，执行清理操作。

3. Data wiper component

   Data wiper 主要功能为如下：

   ① 遍历 SYSTEM\\CurrentControlSet\\Services 注册表项，将所有服务的 ImagePath 替换为空。该操作将导致系统服务不可用，系统无法重启。

   ② 遍历所有本地以及网络磁盘驱动器，遍历盘符从 C 到 Z。若发现相应扩展名的文件，则创建新线程，对文件内容进行覆盖，破坏文件。

③ 枚举系统进程，结束相关的系统进程，该操作将导致系统崩溃：

4. Scanner

Industroyer 内置了端口扫描器，可以通过 -ip 和 -port 参数指定扫描的 ip 范围以及端口范围。

5. 其他攻击手段：DoS tool

Dos 攻击利用漏洞 CVE-2015-5374，针对西门子 SIPROTEC 设备，通过向目标 50000 端口发送特定的 18 字节的 UDP 包。攻击完成后，将导致设备停止响应正常指令，直到手动重启设备才能恢复正常。

- **总结：**

Win32/Industroyer 是一款专门针对工控系统的恶意软件，支持 IEC101、IEC104、IEC61850 以及 OPC DA 四种工控协议。样本分为多个模块，主后门程序负责安装并运行其他模块，并与 C&C 通信，接收 C&C 指令，根据指令执行下一步操作。针对工控协议的攻击分别由独立的 payload 完成，攻击能够导致工控系统崩溃，无法提供正常服务。

2.2.2 Dragonfly2.0 恶意软件介绍

Dragonfly 组织也被称为 Energetic Bear，主要针对电力运营商、主要发电企业、石油管道运营商和能源工业设备供货商进行网络间谍活动。根据美国国土安全部发布的 JAR 报告，Dragonfly 是与政府有关联的俄罗斯 APT 威胁实体。从公开信息可以看出，Dragonfly 组织是一个具有多种攻击能力的黑客组织，其能够通过窃取受害主机凭证来访问目标网络，并且还有广泛的定制化的黑客工具集来对目标网络进行攻击。从 Dragonfly1.0 到 Dragonfly2.0 的发展来看，该黑客组织的对抗手段越来越多（如 https 加密通信、实时的加密 shellcode 下载执行、预初始化代码劫持、模板注入等），并且也开始频繁的运用合法的系统管理工具如 PowerShell、PsExec 和 Bitsadmin 来进行辅助实现攻击。这在一定程度上加大了威胁发现的难度。虽然该黑客组织在攻击过程中没有使用过 0day，但是其长期对能源部门的情报收集表明该组织是一个高度专注的黑客组织。从攻击案例来看，该组织的目标可能是为了达到某种政治目的。

赛门铁克表示该公司从 2011 年起就在追踪该组织，并揭示了它与 2014 年发起的针对西方企业的网络攻击之间的关联。其攻击活动情况如下：

2011 年开始对美国和加拿大的国防和航空公司进行攻击。

2013 年初的第二阶段时期，集中精力在美国和欧洲的能源公司。

2014 年的时候，针对美国、意大利、法国、西班牙、德国、土耳其和波兰进行攻击。

2015 年后，能源行业备受其骚扰，2015 年 12 月后一直行事低调。

在沉寂了多年之后，最近又活跃了起来。研究人员发现 Dragonfly 针对欧洲（土耳其和瑞士）和美国的能源公司进行攻击。这次攻击者的目的是控制甚至破坏能源设施。

Dragonfly2.0 和一代一样，使用多种攻击方式（恶意电子邮件、水坑攻击和合法软件捆绑）对目标进行渗透并植入恶意代码。Dragonfly1.0 活动更像是一个侦察阶段，但 Dragonfly 2.0 活动有破坏性的目的。以下是黑客采用的一些策略：

攻击者使用更普遍可用的恶意软件和“自给自足”的工具，例如 PowerShell、PsExec 和 Bitsadmin 等管理工具。

Dragonfly 2.0 使用各式各样的攻击手段，从鱼叉式钓鱼邮件到水坑式攻击。

在赛门铁克 2015 年 12 月发现的一次攻击中，攻击者使用电子邮件邀请参加跨年晚会。

2016 年到 2017 年期间的其他活动中普遍使用专门针对能源部门的鱼叉式钓鱼邮件。

赛门铁克发现的网络钓鱼邮件是用 Phishery 工具包建立的，试图透过样板注入攻击来窃取受害者的登入信息。攻击者还利用水坑式攻击针对能源部门人员可能浏览的网站来获取网络凭证。赛门铁克报告说，至少在一起案例中，水坑式攻击在 11 天后透过 PowerShell 散播 Goodor 后门。

这里仅对该恶意软件和组织做一个大致的介绍。如您想要对此恶意软件有更深的了解，请参考相关的介绍报告。

2.2.3 新型 ICS 攻击框架 "TRITON" 介绍

2017 年 11 月中旬，Dragos Inc. 团队发现了针对 ICS 量身定做的恶意软件。该团队将此恶意软件命名为 TRISIS（本文中的 TRITON）。因为它将目标锁定在施耐德电气的 Triconex 安全仪表系统（SIS），从而能够更换最终控制元素中的逻辑。

TRITON 具有高度针对性，可能不会对其他施耐德电气的客户构成直接威胁，其他 SIS 产品也不会受到威胁。重要的是，恶意软件不会利用施耐德电气产品中的固有的漏洞。然而，这个特定事件中的这

种能力和方法现在可能被其他攻击者所复制，给工业资产所有者和运营商带来一类新的威胁。

在攻击过程中，攻击者首先获得对 SIS 工程师站的远程访问权限，并部署 TRITON 攻击框架来重新下装 SIS 控制器。事件中，一些 SIS 控制器进入失效的安全状态，自动关闭工业控制流程，并促使资产拥有者开始调查。调查发现，当冗余控制器之间的应用程序代码未通过验证检查时，SIS 控制器启动了安全关闭导致 MP 诊断失败，并在调查的过程中发现了 TRITON 的存在。

攻击者的长期目标是引起物理破坏的结果。基于这样一个事实，攻击者最初在 DCS 上获得了可靠的立足点，并且已经具备了操纵流程或关闭工厂的能力。入侵 DCS 和 SIS 系统以后，攻击者可以最大限度的对物理装置造成破坏。

2.3 工控资产的脆弱性

大部分工控系统安全机制无鉴别、无加密、无审计。这类工控资产比较脆弱。在和外部联网的情况下，工控系统容易被外部探测，并通过公开或私有通讯协议、WEB 服务、Telnet、FTP 等返回的信息中包含的特殊字段对资产进行识别，进而可以实现对资产的控制。另外，近年来越来越多的工控漏洞被研究人员发现。这使得暴露在外的工控系统资产十分脆弱。

2.3.1 工控系统暴露的资产日渐增多

为了最大限度地降低工控设备遭遇网络攻击的可能性，工业控制系统应该在物理隔离的环境中运行，然而在实际生产环境中情况并非如此。2016 年 7 月，卡巴斯基就发布报告表示，在全球 170 个国家中共发现 188,019 台连接互联网的 ICS 主机 [1]。

下面以绿盟科技威胁情报平台（NTI）为依托，通过多种协议探测全球工控资产在网络中的暴露情况。首先以最常见的 Modbus 和西门子 S7 协议为例，统计全球设备数据总量及分布（统计数据不分年份）。

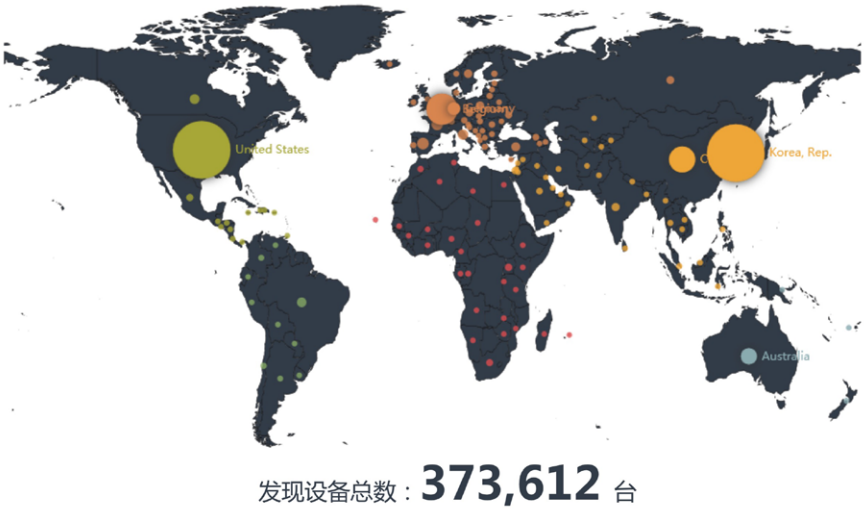


图 2.2 使用 Modbus 协议设备全球分布数据视图

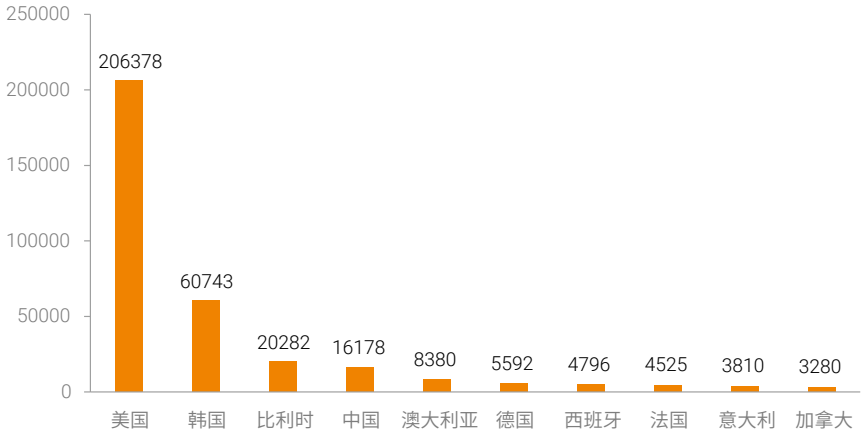


图 2.3 使用 Modbus 协议设备 TOP10 国家受影响暴露面

工控信息安全态势

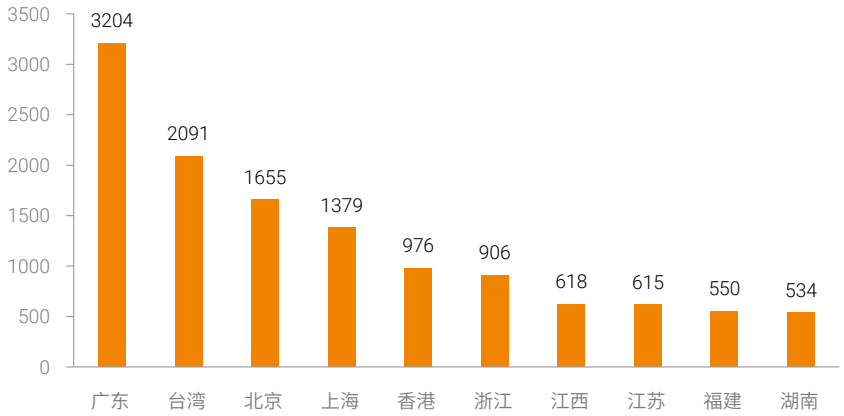


图 2.4 使用 Modbus 协议设备 TOP10 国内省份受影响暴露面

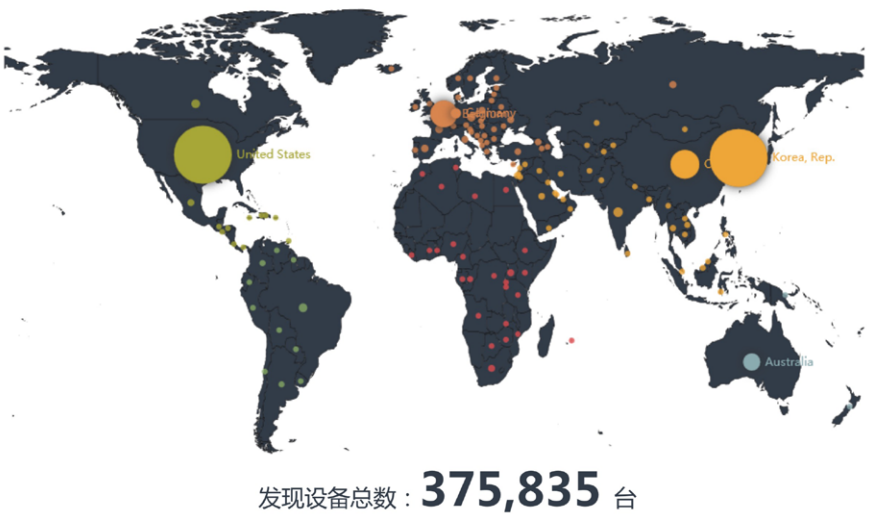


图 2.5 使用 S7 协议设备全球分布数据视图

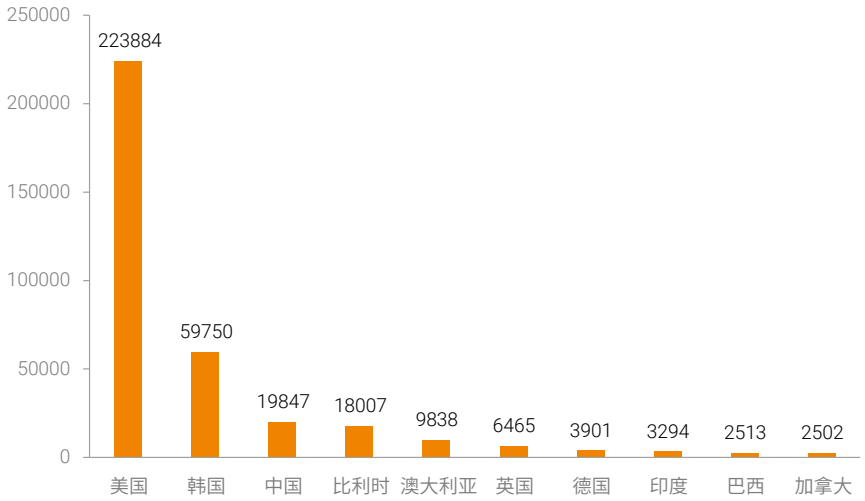


图 2.6 使用 S7 协议设备 TOP10 国家受影响暴露面

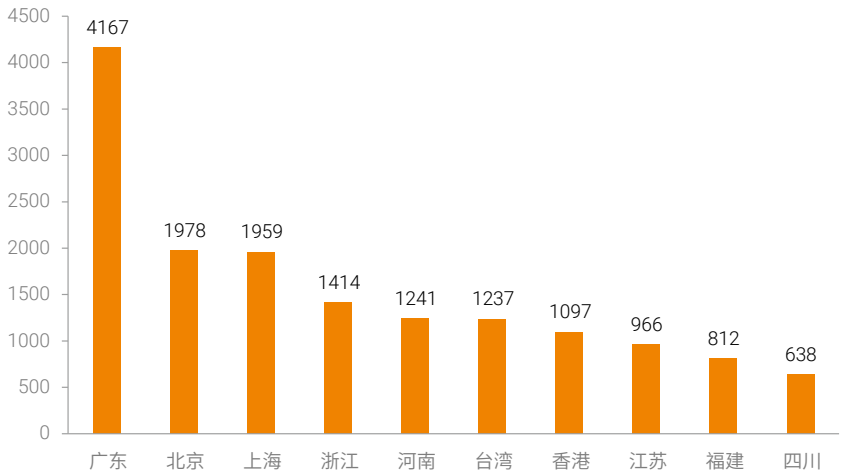
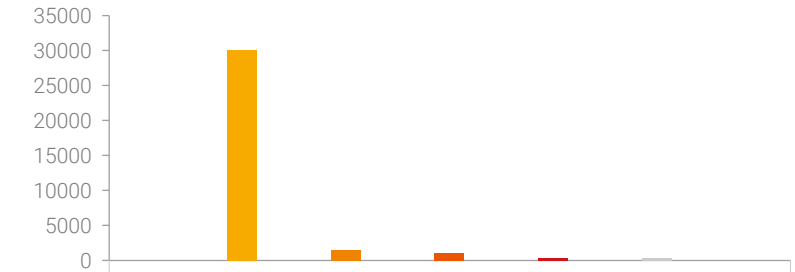


图 2.7 使用 S7 协议设备 TOP10 国内省份受影响暴露面

仅 2018 年，通过检测 Modbus、S7、DNP3、ENIP、IEC 五种协议可探测到的设备数量及全球分布如下:



	设备数量
Modbus	30065
IEC	1451
DNP3	953
S7	243
ENIP	232

图 2.8 2018 年不同协议全球可探测设备统计图

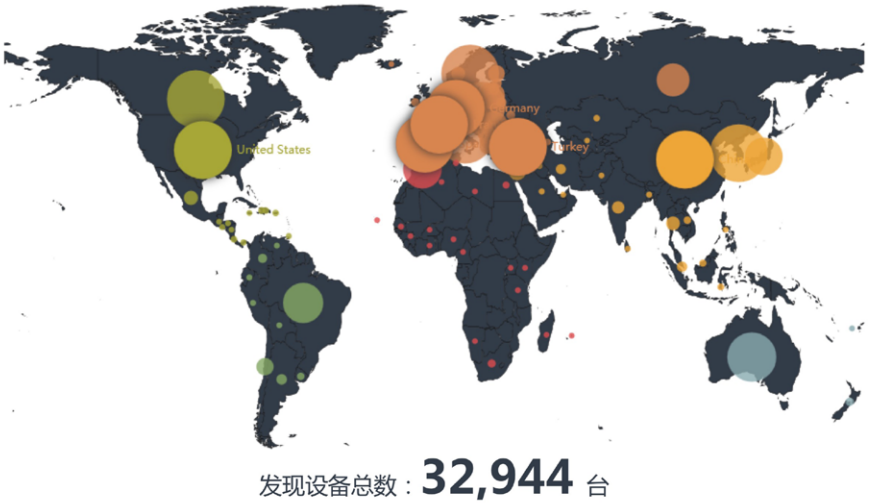


图 2.9 2018 年 5 种协议设备全球分布数据视图

全球越来越多的工控系统及设备与互联网连接，这将暴露更多的安全风险隐患。据卡巴斯基统计数据显示，2017 年上半年，有 20.6%的 ICS 计算机威胁来源就是互联网，到了 2018 年上半年这一数字达到了 27.3% [2]。

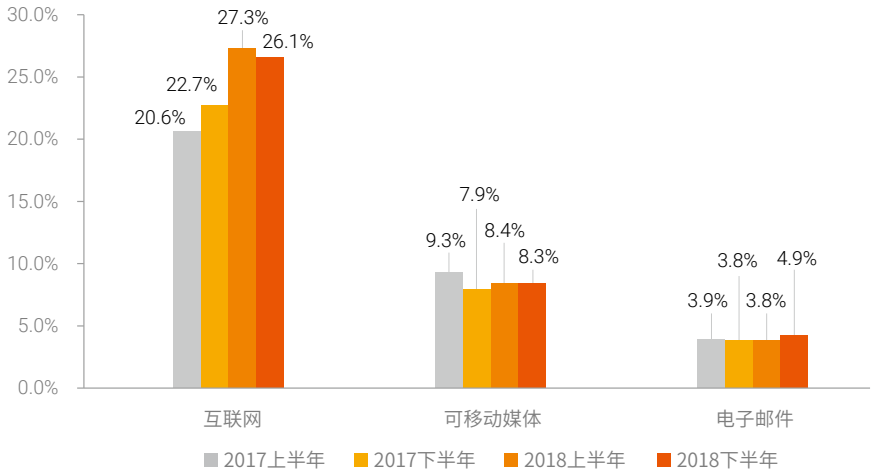


图 2.10 ICS 计算机威胁来源统计图 [3]

这些被暴露在互联网上的工控设备在攻击者看来都是感染工控网络的潜在渠道。如果其中一些工控设备本身就存在未修补的漏洞，加之部分工控系统软硬件设备漏洞信息在网上被分享和公开，那么从设备的漏洞入手便极可能成为攻击者入侵的首选。

此外，我们还对不同行业中所使用到的工控厂商设备进行了统计，得到如下结果。其中，HMI，DCS 和 PLC 中需要运行操作系统并执行相关的软件，所以漏洞主要出现在这三类设备中。因此本文主要分析 HMI，DCS 和 PLC 三类设备。

工控信息安全态势

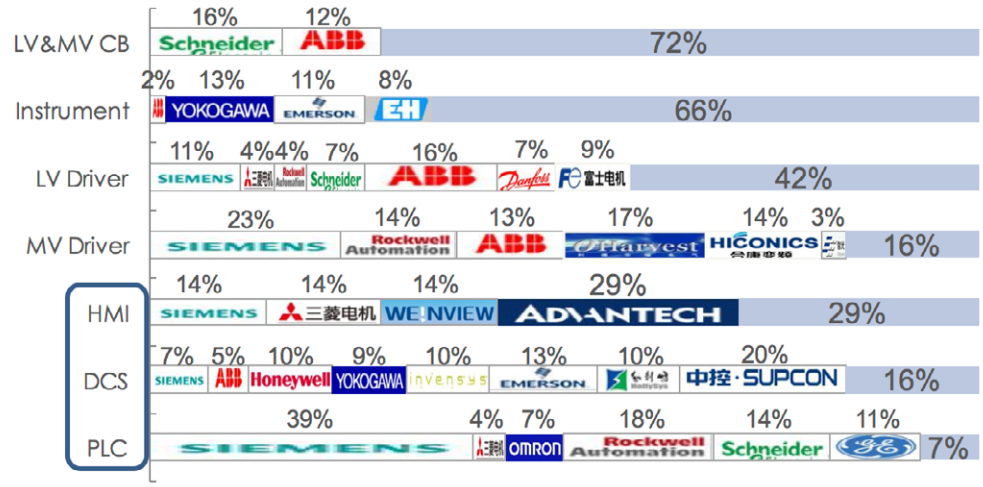


图 2.11 供水及水处理行业工控系统应用统计

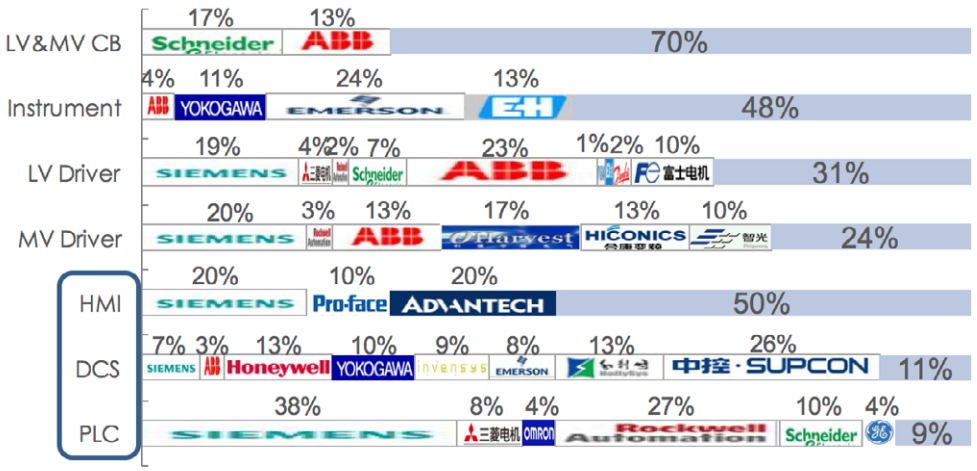


图 2.12 化工行业工控系统应用统计

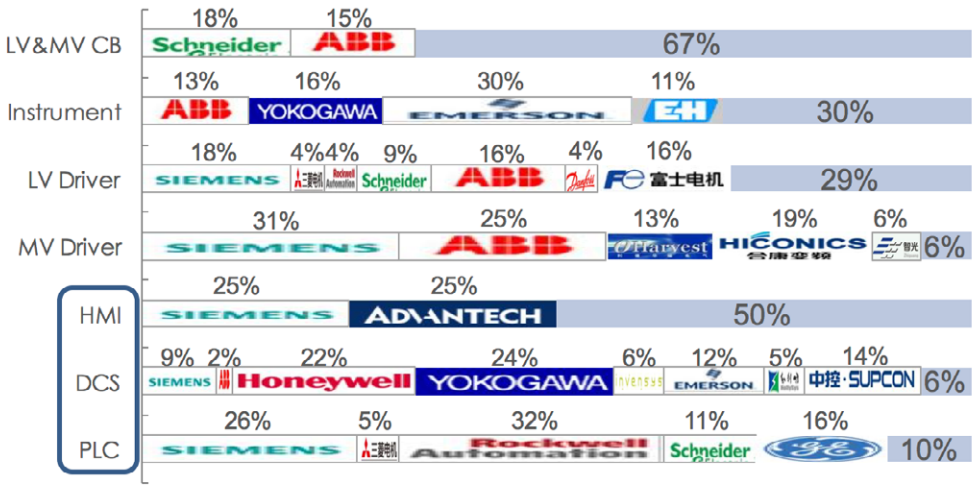


图 2.13 石化行业工控系统应用统计

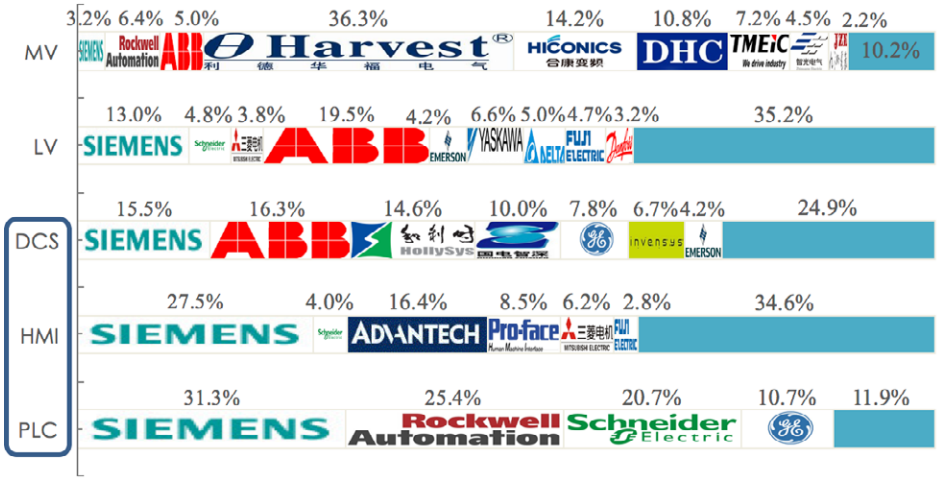


图 2.14 电力行业工控系统应用统计

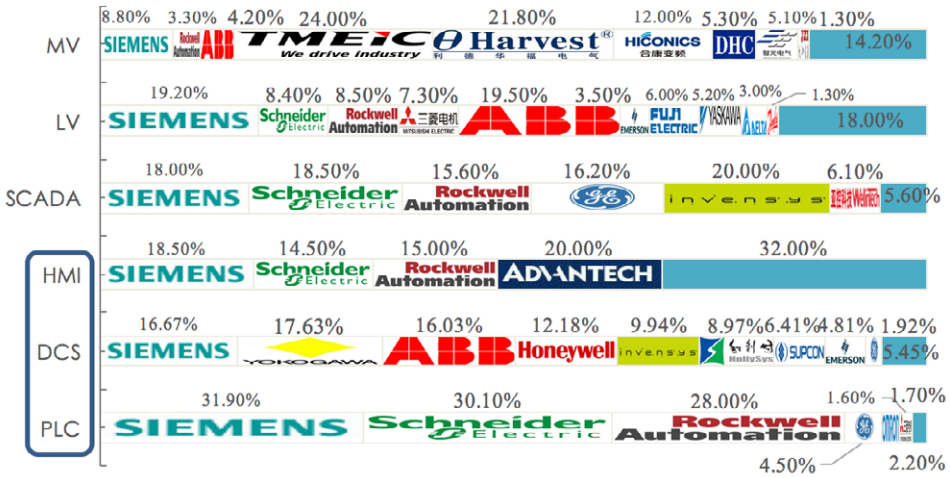


图 2.15 冶金行业工控系统应用统计

2.3.2 工控漏洞的变化趋势

随着近年来对工控安全的深入研究，越来越多的工控漏洞被研究人员发现。公开披漏出来的漏洞仅仅是冰山一角，不排除有一些工控漏洞被当做网络武器储备起来了。本节基于公开的数据进行统计，给出近年来工控系统漏洞的趋势。

2.3.2.1 基于 ICS-CERT 的数据统计

美国工业控制系统网络应急响应小组（ICS-CERT）负责协调工控行业安全事件及促进信息共享。截止 2018 年 12 月 13 日，可在 ICS-CERT 官网查看的安全通告统计共计 1046 篇 [4]。

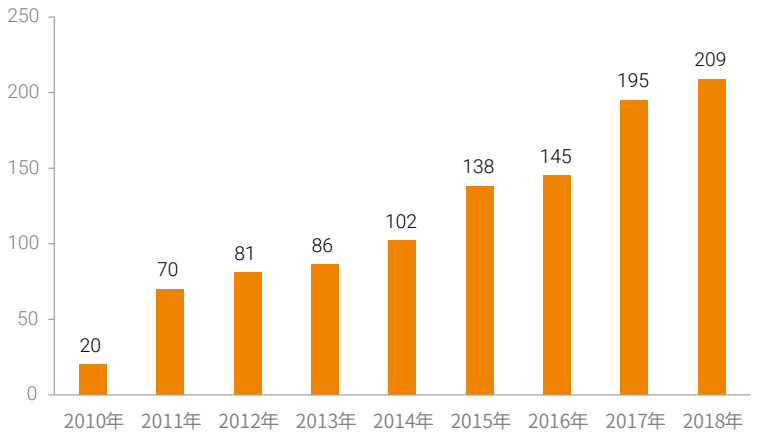


图 2.16 ICS-CERT 历年安全通告篇数

根据 ICS-CERT 官方年度报告所提供的数据 [5]，从 2010 至 2018 报告的漏洞数统计如下：

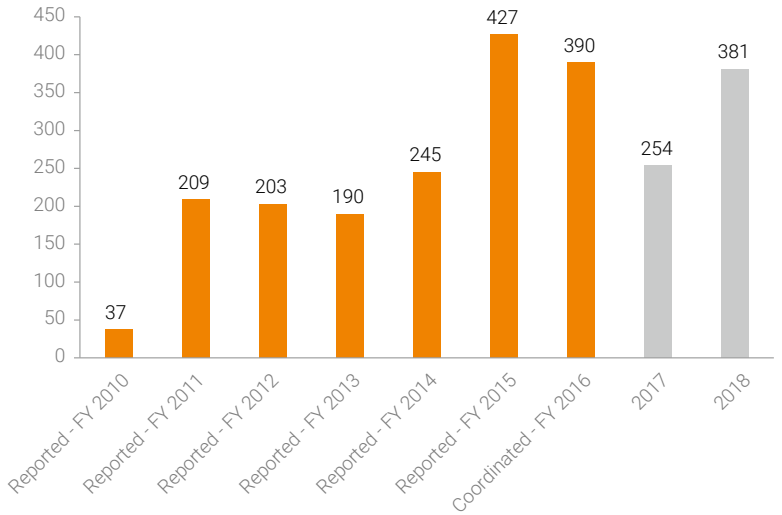


图 2.17 ICS-CERT 历年漏洞总数统计

备注：

1. FY 指会计年（自公历 1 月 1 日起至 12 月 31 日止）。
2. 2010 至 2016 年数据来源于 ICS-CERT 官方年度报告 [6]。其中 2010 至 2015 年的统计数据为 ICS-CERT 接收的漏洞个数，2016 年实际接收的漏洞个数为 2282，除去被厂商拒绝以及验证无

效的漏洞，图中 2016 年数据为验证有效且计算过 CVSS 评分的漏洞数。

3. 2017、2018 年数据 ICS-CERT 官方暂未公开，数据统计自所有拥有 CVE 编号，且来源中包含 ICS-CERT 的漏洞。介于部分 2017 年、2018 年工控漏洞的 CVE 还处在保留状态，该部分数据统计请谨慎参考。

从以上 ICE-CERT 的统计数据可以看出，工控漏洞的数量在逐年增长。其中，2015 年的情况比较特殊，存在着较大的增长，不过 2015 年的增长更像是一个反常尖峰，预测之前多年平均 5% 的增长率更有可能成为未来的趋势。

2.3.2.2 基于 CVE 的数据统计

考虑到 CVE 的影响力，且有一部分工控漏洞仅申请过 CVE，故对近年来申报了 CVE 的工控漏洞进行了筛选整理。

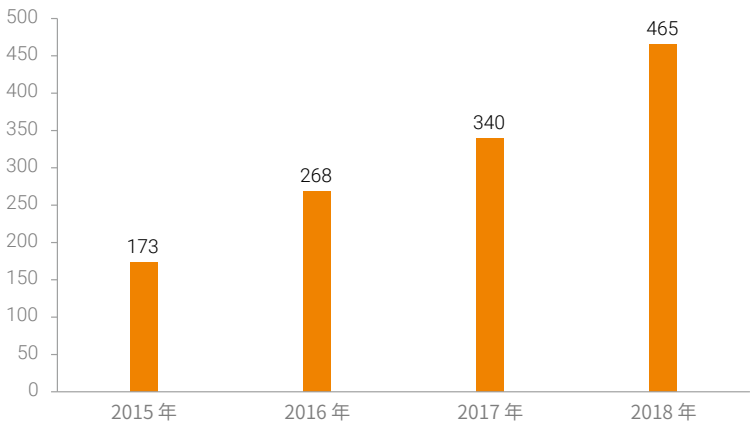


图 2.18 2015-2018 年工控漏洞 CVE 个数

备注：工控漏洞的修复时间较长 (多数工控漏洞的修复时间大于 6 个月，少数工控漏洞大于 1 年还在保留状态)。截至 2018 年 12 月 13 日，还有部分 2017、2018 年的工控漏洞的 CVE 处在保留状态，处在保留状态的漏洞不在统计范围内。

自震网病毒事件发生后，工控系统的安全性逐渐得到了各个国家的重视，很多公司和机构都在挖掘工控系统漏洞，相应的工控漏洞的数量呈逐年增加的趋势。

从存在漏洞的设备类型来看，按照运行在 PC 上还是运行在特定的设备上进行分类，主要可划分为 HMI 和 Device 两种类型。统计结果如下：

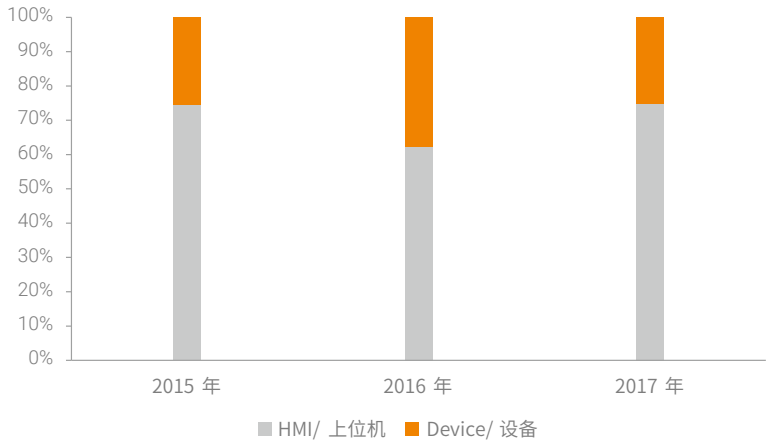


图 2.19 工控漏洞涉及设备统计

从统计结果可以看出，HMI 部分的漏洞占比较大。PC 机应用软件漏洞的挖掘是传统安全公司所擅长的。HMI 软件一般会涉及到 WEB 系统和数据库系统等，都是容易出各种安全问题的地方。相对 PC 应用来说，工控设备的漏洞挖掘难度比较高。因为工控系统使用嵌入式系统，软件和硬件都是高度定制和裁剪过的。工控设备漏洞的挖掘需要的技术难度比较高，加上工控厂商很少公开固件的下载，导致工控系统设备的漏洞被发现的数量比较少。不过随着各安全厂商和机构对工控设备的深入研究，更多的工控漏洞将会被披露出来。

工控漏洞的厂商分布如下：

工控信息安全态势

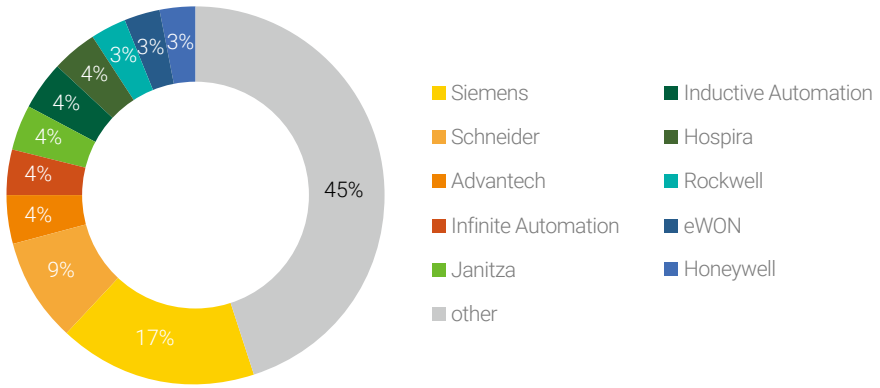


图 2.20 2015 年工控漏洞涉及厂商统计

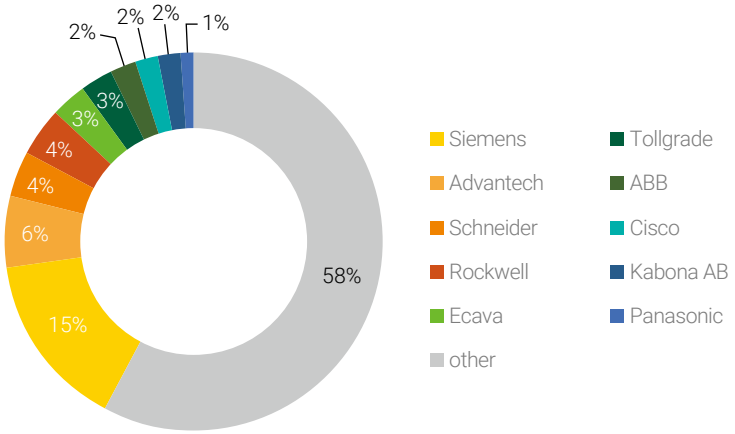


图 2.21 2016 年工控漏洞涉及厂商统计

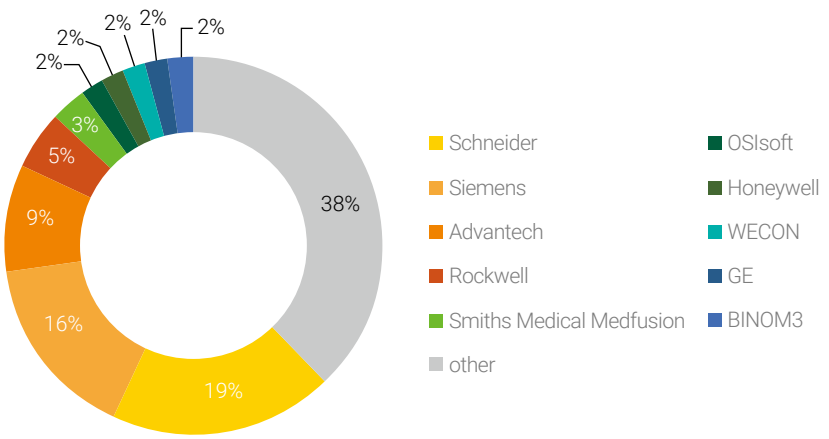


图 2.22 2017 年工控漏洞涉及厂商统计

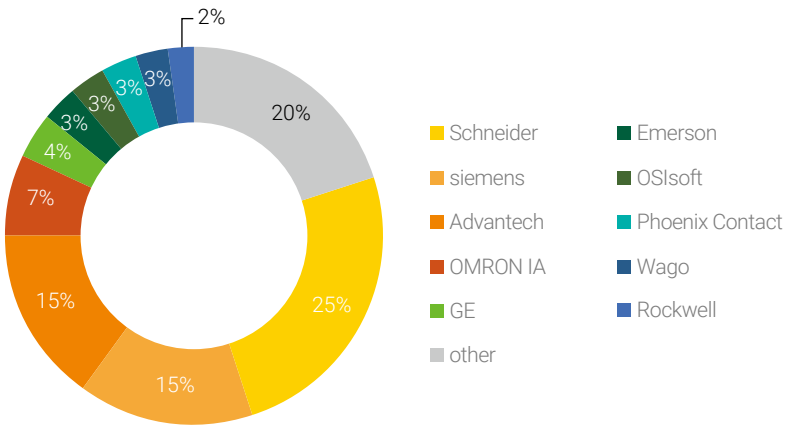


图 2.23 2018 年工控漏洞涉及厂商统计

对以上数据进行汇总，下面得出近四年来漏洞数量 TOP10 的厂商。

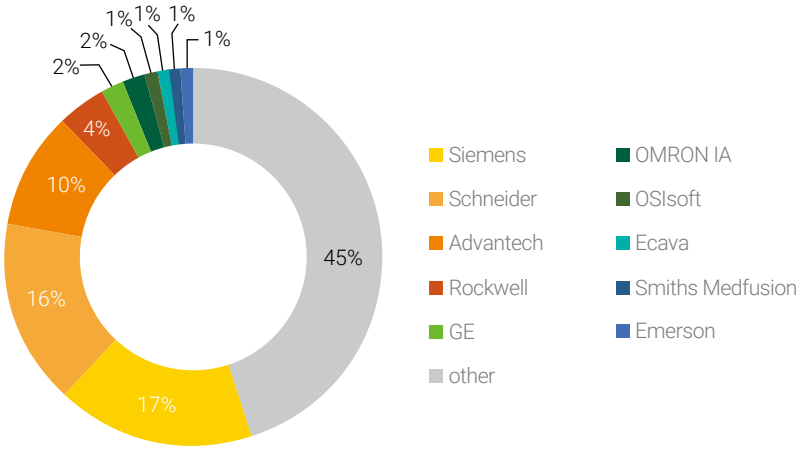


图 2.24 2015-2018 年工控漏洞涉及厂商 TOP10

西门子、施耐德、研华、罗克韦尔、欧姆龙等是漏洞大户。不过需要了解的是，被公布漏洞越多的厂商并不表示其设备越不安全，因为越是被广泛使用的设备受到的关注程度会更大，因此被发现和披露的漏洞也会更多。以我国工业 PLC 市场为例，2015 年西门子、三菱、欧姆龙、罗克韦尔、施耐德等 5 家厂商就占据了超过 80% 的市场份额。有如此之大的使用量，成为安全研究人员和攻击者关注的焦点也并不意外。

2.3.2.3 工控漏洞的风险

漏洞数量在逐年增长，那么这些漏洞在实际情况中对工控行业所造成的影响到底有多大呢，以下参考 FireEye 的 Mandiant ICS Healthchecks 所提供的数据一窥究竟 [7]。Mandiant ICS Healthchecks 评估来自多个行业组织中的网络安全风险，通过识别特定问题的可利用性、影响以及交叉影响结果来判定危害程度。经其分类统计后发现，在 ICS 组织中发现的安全问题至少有 33%被评为高风险或严重风险。这意味着攻击者极有可能利用这些问题获得目标系统的控制权并危害其他系统和网络，还可能导致服务中断、信息泄露、未授权访问等其他重大负面后果。

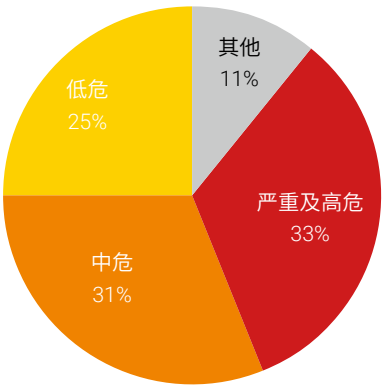


图 2.25 风险评估分布

导致这 33% 的严重及高危风险的原因中，占比最大的就是漏洞相关的问题。

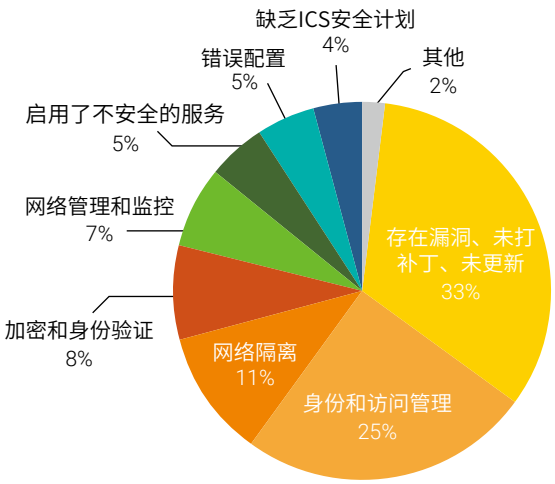


图 2.26 严重及高风险威胁来源

这一结果在近年来众多的工控安全事件中也有所体现，即安全事件中一个核心环节就是利用了工控系统的漏洞，进而攻陷整个工业控制系统。

比如于 2010 年 6 月首次被发现，第一个专门定向攻击真实世界中基础（能源）设施的“震网”病毒，就利用了四种零日漏洞，包括快捷方式文件解析漏洞（MS10-046）、打印机后台程序服务漏洞（MS10-061）、内核模式驱动程序漏洞（MS10-073）、任务计划程序漏洞（MS10-092）。

2014 年底，完善后的恶意软件 BlackEnergy（黑暗力量）利用西门子 SIMATIC WinCC（西门子过程监视系统）已经修复的漏洞攻击 SCADA HMI 系统。

2017 年发现的恶意软件 Trisis（又称为 TRITON），利用了施耐德 Triconex 安全仪表控制系统（SIS，Safety Instrumented System）中的零日漏洞，对中东一家石油天然气工厂发起了网络攻击，最终导致工厂停运。Trisis 是首款专门针对安全仪表系统的恶意软件，可能引起工厂关闭或者使人受伤，它的危害不言而喻。

据 Fortinet 全球威胁态势报告显示，截至 2018 年第二季度，被利用的最多的是 Schneider 的 Quantum Ethernet 模块中的后门访问漏洞。因为默认账户使用硬编码密码，远程攻击者可以通过 FTP 访问获得此账户访问设备的权限。利用 Siemens Automation License Manager 中缓冲器溢出漏洞的尝试居于第二位，紧接着就是 Advantech WebAccess 中的另一溢出漏洞。这两种溢出情况因对输入处理不当，均允许任意代码执行。

工控网络安全漏洞小则导致工厂瘫痪，大则造成核电站爆炸、全国停电等灾难性后果。因此，在黑客成功攻击工业控制系统之前发现漏洞、修复漏洞，促使其完善系统，是保障工业控制系统安全运行、增强企业安全健壮性的重要手段之一。

2.3.2.4 工控行业威胁分析

前面统计了不同的工控行业中所使用的控制设备厂商分布和不同的工控设备厂商的控制设备漏洞占比的情况。本节根据统计结果对不同的工控行业所面临的安全威胁进行综合的分析。

在工业控制系统中，漏洞主要存在于 HMI，PLC 和 DCS 三类设备中。因此这里针对每一个行业分别计算这三类设备的厂商的平均占比，然后分年度根据当年工控设备厂商的漏洞占比情况分别计算每个行业的威胁指数，进而得到相关行业所面临的威胁趋势的变化，计算的公式如下：

行业控制器厂商平均占比 = ((HMI 占比 +PLC 占比 +DCS 占比))/3

相关年份行业的威胁指数 = $\sum$ 行业控制器厂商平均占比 × 控制器厂商漏洞占比

根据以上公式计算出来的威胁指数结果如下。

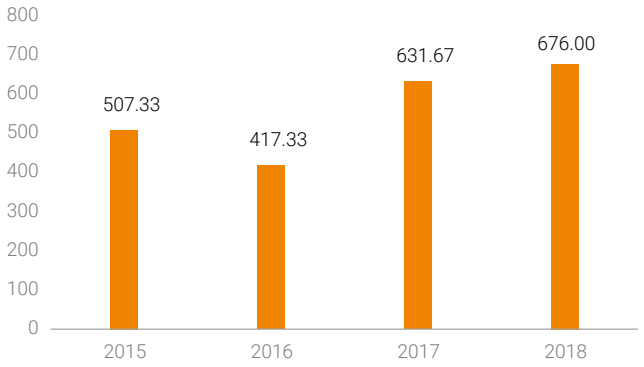


图 2.27 供水及水处理行业威胁态势

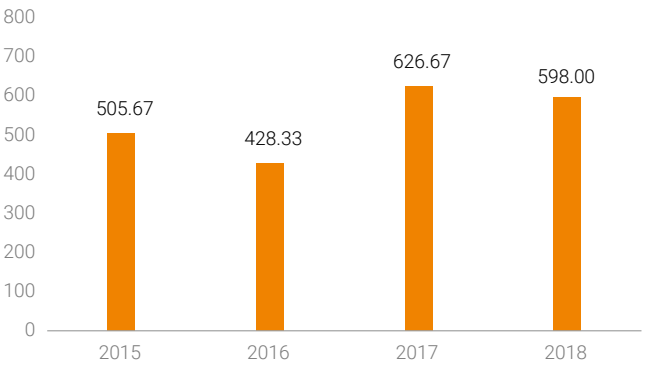


图 2.28 化工行业威胁态势

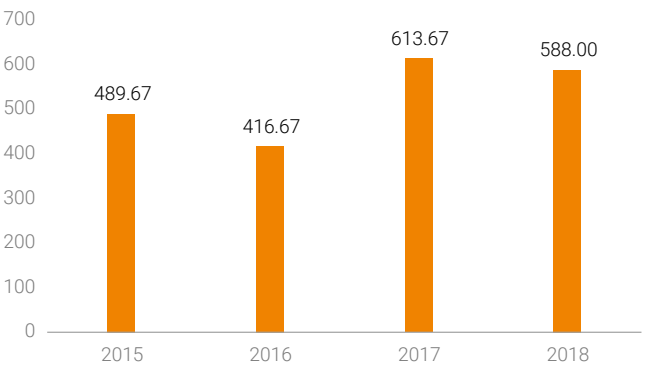


图 2.29 石化行业威胁态势

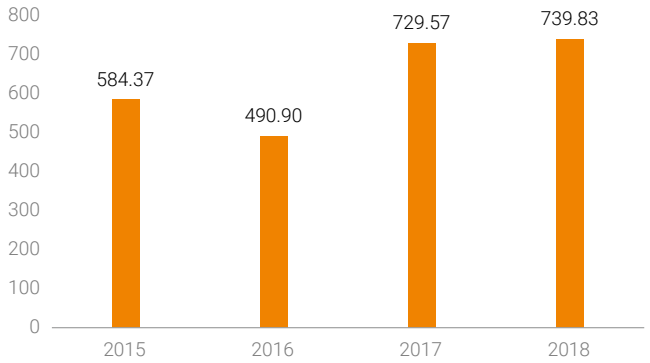


图 2.30 电力行业威胁态势

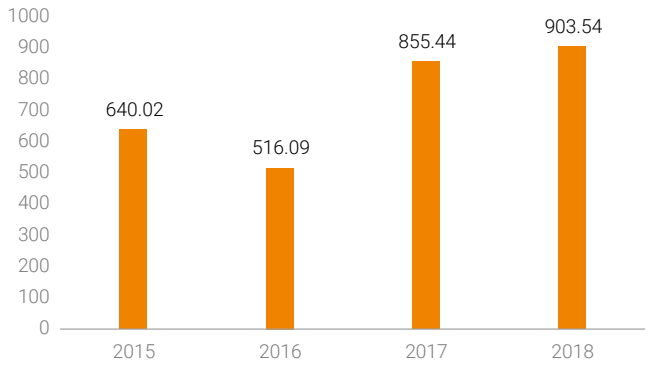


图 2.31 冶金行业威胁态势

从上面的分析结果可以看出，工业控制系统在 2017 年和 2018 年所面临的威胁要比 2015 年和 2016 年高得多。尽管从统计结果来看 2016 年的指标较低，但这并不意味着 2016 年工控系统更加安全。从前面的数据可以看出，这五个典型的工业场景中的主要工控设备在 2016 年被发现的漏洞的比例较小。随着对主流工控设备厂商生产的控制设备研究的逐步深入，越来越多的漏洞将会被发现，工业控制系统所面临的威胁也越来越严峻。

2.4 工业信息安全的变化趋势

总体来说，随着 IT 与 OT 的加速融合，工业控制系统所面临的威胁的变化也越来越快。其变化主要表现在下面几个方面：

- 工控系统由以前的彻底内网隔离到逐步接入外部网络。这是由行业发展的需要决定的，是社会进步的必然产物。但是大部分工控系统的安全机制无鉴别、无加密、无审计。在工控系统的设计之初没有考虑到会逐步接入网络，从而带来新的安全风险。
- 网络攻击已经从影响虚拟资产演变到破坏物理世界，由对电脑的攻击演变为对嵌入式系统的攻击。
- 通用化、软硬结合、互联互通的技术变化直接带来基础设施攻击面的增大。通过互联网渗透到工控系统已成为一种重要途径。任何工控系统都可能成为目标。
- 传统病毒与工控病毒相互交织，例如震网病毒。
- 以计算机为跳板的攻击在未来可能发展到直接攻击控制系统。
- 从利用未公开漏洞的高难度攻击方式延伸到常规手段组合式攻击，甚至绕过工控底层知识的壁垒。
- 发现预警难度大：硬件获取难（价格昂贵、购买困难）、故障调试难（嵌入式）、设备类型多、私有协议多、软件公开资料少。
- 工控系统设备的 0day 问题日益严重。工控厂商的维护和测试周期一般比较长，漏洞修补不及时，有时漏洞公布出来一年后才发布漏洞补丁。虽然厂商发布了漏洞补丁，工控现场的设备因为要连续运行，再加上管理上、技术上等各种原因，补丁不能及时得到安装，导致工控设备的漏洞一直得不到及时修补。
- 针对工控系统的勒索病毒会越来越多。目前的勒索病毒，例如 warnecry 等，主要是针对工控系统中的 IT 系统进行攻击，例如针对上位机，ERP 系统等进行勒索攻击。未来将会出现针对 OT 系统，例如 PLC，DCS 等系统的勒索病毒。
- 拒绝服务型漏洞在工控系统中变得越来越危险，是可能导致重大安全事故的元凶。

综上，工控系统所面临的安全威胁越来越严重，工控系统的安全也是一个长期的不断变化的过程。

3

工控信息安全保障框架

3.1 工控信息安全的保障原则

工控信息安全保障框架的构建需要充分考虑到国家、行业的相关规范要求，需要结合企业自身业务需求和自身运行的特点，做到技术和管理相结合，逐步完善工业控制系统的安全防护，使工业控制系统安全防护由安全策略的部署向安全能力的部署迁移，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。

3.2 工控信息安全保障思路

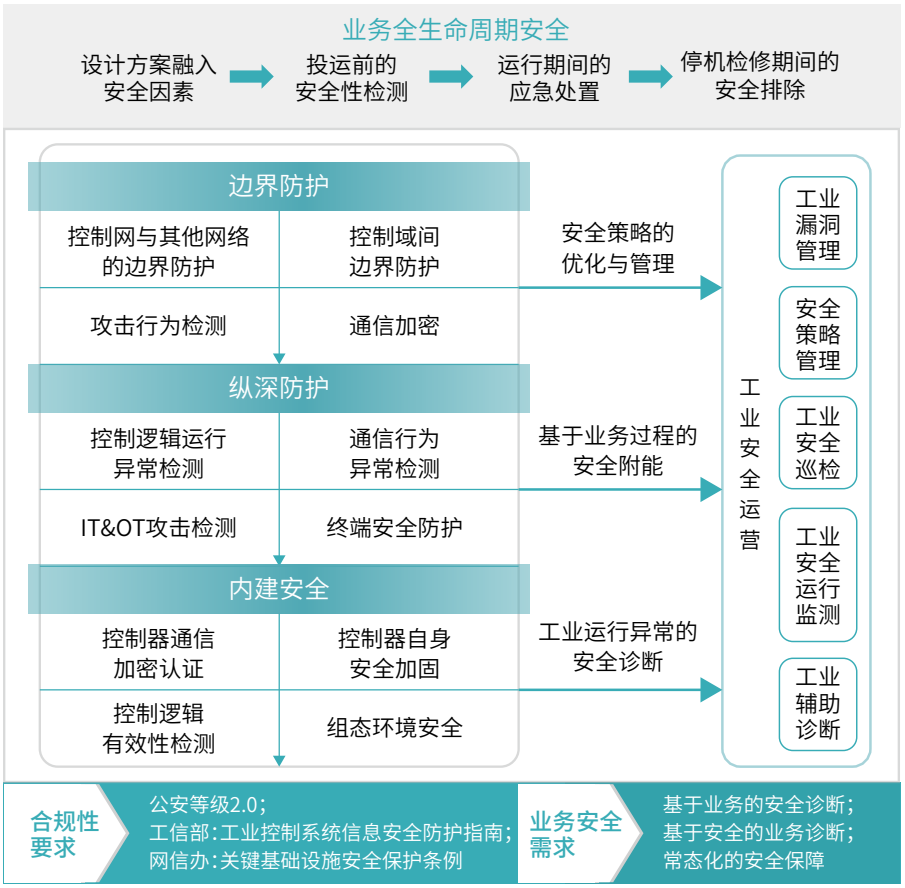


图 3.1 工控信息安全保障框架

工控安全的建设需要考虑合规性。满足合规性的同时要兼顾业务自身的安全需求，需要从业务的生命周期来考虑。从系统开发阶段的安全要求到上线前的安全检测到运行期间的应急处置再到停机检修期间的安全隐患排除，都需要把安全的因素融入到实际的业务中。工业环境的安全是一种常态的存在，因此需要构建有效的工控安全防护体系，为工控系统提供有力的安全支撑。

构建有效的工控安全防护体系需要从边界防护、纵深防护和内建安全三个方面入手。边界防护需要对不同区域之间进行有效的安全隔离，如 OT 与 IT 的边界可以采用工业防火墙或者网闸等安全设备进行隔离。纵深防护要求充分考虑控制器连接域内不同控制器之间连接的有效防护，做到通信过程可控。工控系统内部需要构建起有效的安全监测和防护手段，做到可观、可管、可控；需要对控制逻辑与业务画面之间的关系进行有效对应；需要对通信过程中的行为进行有效的感知，对于已知的攻击行为要做到及时发现及时处置，对于未知的攻击行为要做到能够及时感知出系统的异常，为进一步定位异常提供有效的依据。采用工业入侵检测、工业异常行为监测、沙箱等技术来对系统中的通信流量和文件进行有效的监测，同时对于各个终端包括工业主机、工业数据库、OPC 服务器等进行有效的监控。在内建安全方面需要考虑控制器自身固件的安全加固措施，例如对固件进行加密，对控制指令进行有效性检测，考虑组态过程中组态软件自身的纠错等，来提升工业控制系统的安全级别。

需要从安全运营的角度来考虑在降低生产企业的安全风险的同时协助企业来提高生产系统的运行效率；需要从业务合规性要求及业务能力的保证来综合考虑业务的安全需求；需要从合规性上着手，逐步扩展到提升企业的业务综合安全能力；需要考虑业务的全生命周期的安全性。

3.2.1 边界安全防护

3.2.1.1 边界防护的指导意见

1. 工信部指南对工控边界防护的指导意见

随着工信部有关《工业控制系统信息安全防护指南》的发布，工控安全又被提升到了一个新的高度。指南指出，工业企业应从十一个方面做好工控安全防护工作。作为工控安全防护重要环节的边界安全在指南的第三大点进行了重点阐述，特别指出工业控制网络与企业网或互联网之间的边界应通过工业控制网络边界防护设备进行安全防护，例如通过工业防火墙、网闸等防护设备在工业控制网络安全区域之间进行逻辑隔离安全防护。这在全行业的高度上对工控系统的边界防护提供了指导性的建议。

2. 电力行业工控边界防护指导意见

作为工控安全先行官的电力行业早在2014年就由国家发改委发布了《电力监控系统安全防护规定》，对电力企业工控系统的安全防护进行了规范。2015年初国家能源局又发布了国能安全36号文，进一步对电力企业工控安全进行了合规性阐述，提出了针对省调、地调、配电网、发电厂、变电站的安全防护方案和安全评估规范。无论是14号令还是36号文都对电力企业的工控安全防护起到了较强的推进作用。发文在“安全分区、网络专用、横向隔离、纵向加密”的十六字方针的基础上对边界安全进行了强调，在控制区与非控制区边界安全子项中规定安全Ⅰ区与安全Ⅱ区之间应当采用具有访问控制功能的网络设备、安全可靠的硬件防火墙或者相当功能的安全设备来实现逻辑隔离、报文过滤、访问控制等功能。在系统间安全防护子项中规定同属于安全Ⅰ区或安全Ⅱ区内部的不同系统之间，根据需要可以采取一定强度的逻辑访问控制措施。这些安全防护场景均可以通过工业防火墙、隔离装置或VLAN技术来满足安全防护要求，从合规性与业务需求两个方面做好电力企业工控系统的边界安全防护。

3. 石化行业工控边界防护指导意见

在石油石化领域，中石油、中石化发布的“十三五”发展规划中也明确了工控安全的重要性。比如油化行业的油田工业控制网络覆盖油田生产现场的井口、站库、管线等设施，用于生产数据实时采集和远程控制与自动控制。其覆盖范围广，很多设备部署在野外，并采用光缆、无线等多种组网方式，容易受到来自外部的攻击。确保工业系统运行安全是油田工业控制网络安全的根本目的。因此如何防范对业务信息，特别是指令信息的窃取、破坏、篡改，防止恶意代码或黑客从远程设备和内部局域网终端对油田工业控制网络的设备进行攻击，是油田工业控制网络安全需要重点解决的问题。这些信息基础设施存在的安全隐患也都可以通过工业防火墙、隔离网闸等边界防护的技术手段提供安全保障，确保油田工业控制网络安全稳定的运行。

3.2.1.2 边界防护技术框架

1. 安全区域之间的访问控制和安全防护

在纵向不同层次网络之间部署防火墙，控制跨层访问并对层间数据交换进行深度过滤，防止攻击者通过上层网络向下层网络的渗透和攻击。

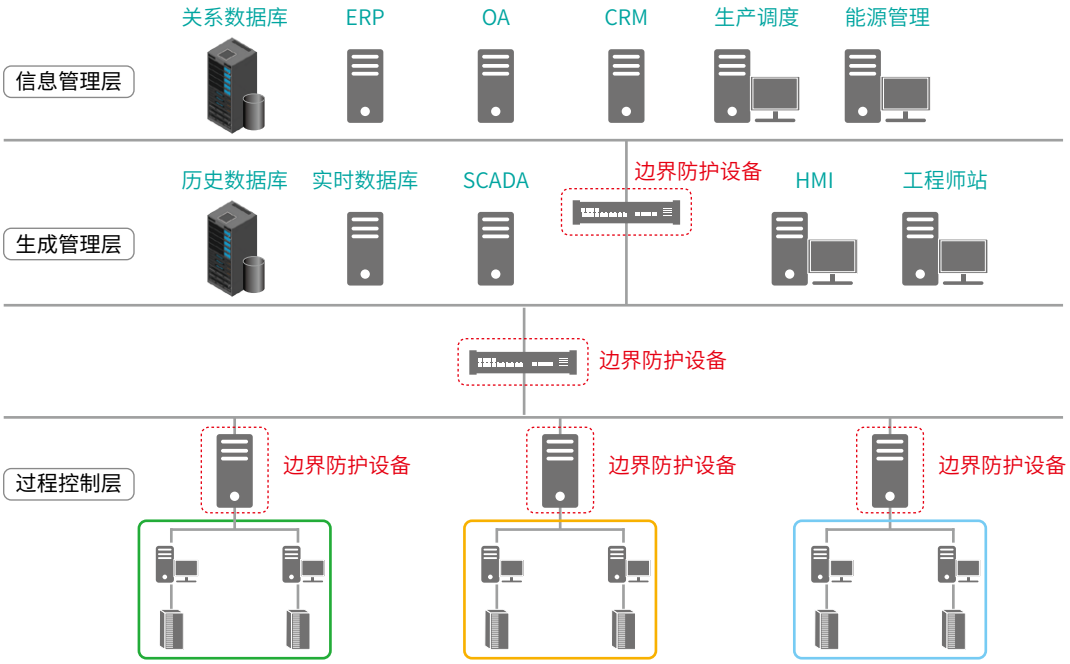


图 3.2 安全区域之间的访问控制和安全防护

在同层次中平行的厂区、工艺流程和业务子系统之间部署防火墙，将它们分割成不同的安全区域，控制不同安全区域之间的访问，并对区域间数据交换进行深度过滤，减少区域之间安全问题的扩散和影响。

2. 重点设备的安全防护

在重点设备的前端部署防火墙，限制可以访问它的 IP 地址、屏蔽非业务端口访问、过滤非法的操作指令、记录所有的访问和操作，对其进行全面的安全防护和审计。

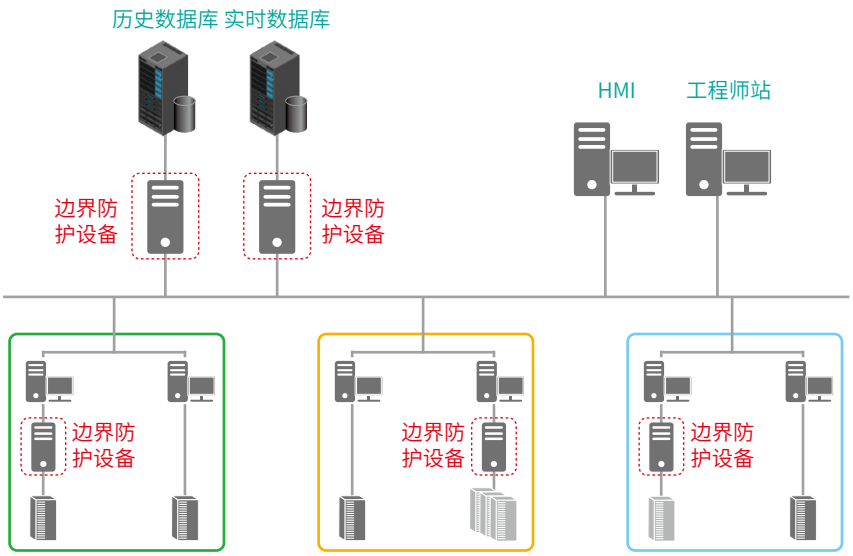


图 3.3 重点设备的安全防护

3. 不同区域工业网络的安全互联

对作业区内部的工业网络进行安全保护，阻断来自公用网络的攻击，实现作业区网络的边界安全防护。

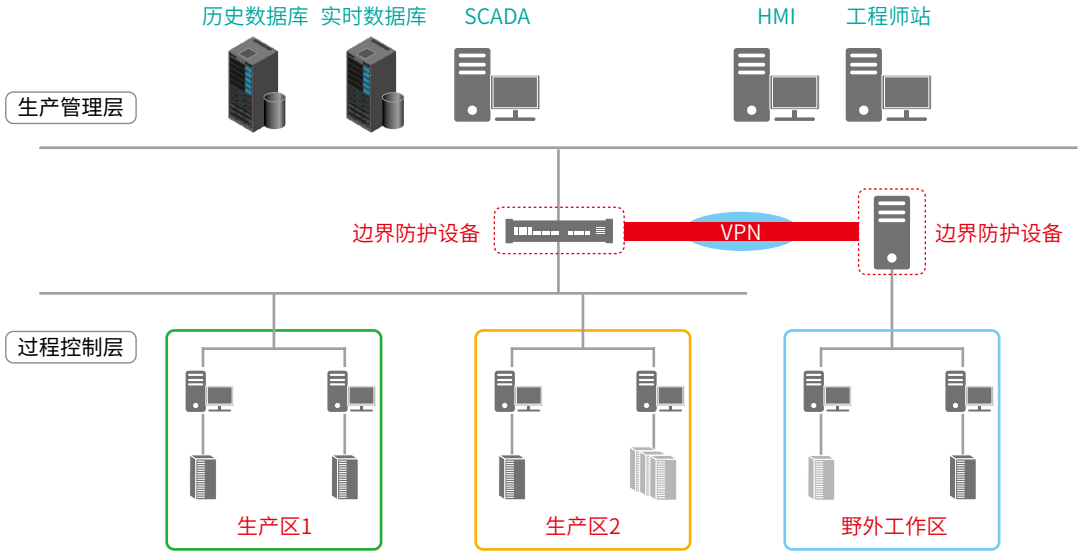


图 3.4 分散工业网络的安全互联

使用 VPN 对作业区与调度中心之间的数据传输进行加密和保护，搭建安全的数据交换通道，解决两者之间的数据传输安全问题。

4. 融合安全的远程运维管理

在工业网络与公用网络接口处部署防火墙，并启用 VPN 功能，将其作为远程维护的堡垒设备。远程维护人员使用 VPN 连接到防火墙上，一方面进行身份认证，另一方面对通过公用网络完成的远程维护操作进行加密保护，实现安全的远程维护。

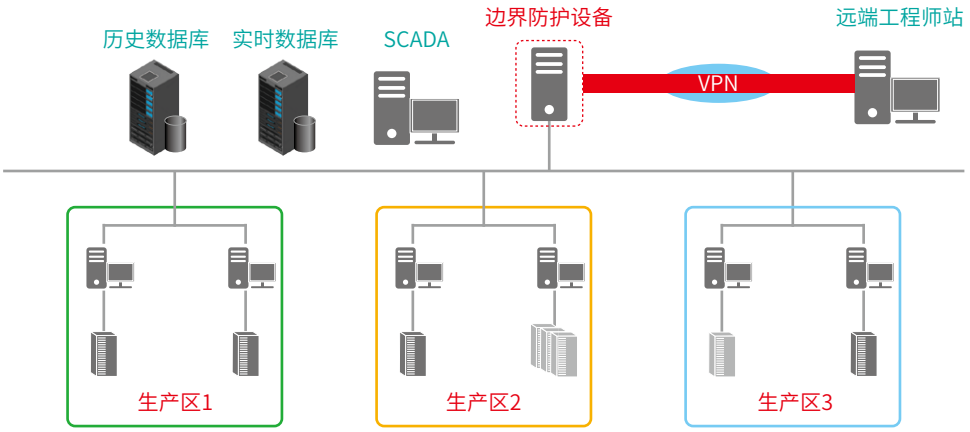


图 3.5 安全的远程维护

3.2.2 纵深防护

3.2.2.1 工控网络纵深防御框架

根据工业控制系统的特点和安全需求，需要对工业自动化控制系统引入纵深防御措施。纵深防御就是要通过采取多层次的、具有不同针对性的安全防护措施，保护关键的工业控制系统与应用的安全。其优势在于，攻击者将不得不渗透或绕过不同的多层安全机制，大大增加了攻击的难度。一旦某一层面出现问题，可被其他层面的防护措施所弥补，从而避免“一点突破，满盘皆输”的危险。

建立工业自动化控制系统纵深防御体系，首先需要对具体的工业控制系统安全需求进行分析，制定相应的安全规划；并对工控系统进行风险评估，切合实际地识别出系统面临的安全威胁及风险的来源。在此基础上，借助于产品安全操作指南以及专业的工业安全服务，建立、部署层次化的多重安全防护体系。

目前，纵深防御的工业信息安全理念覆盖了工业自动化控制系统的所有级别，是满足工业信息安全

领域关键需求的现实解决方案。安全标准控制措施具体包括制定安全策略与流程，部署防火墙进行隔离，防护不同的安全单元（安全域），采用 VPN 保护单元间通信，进行系统加固，部署账号管理等访问控制措施，以及补丁管理、恶意软件检测与防护等。

3.2.2.2 工控网络纵深防御体系构建策略

落实到具体的应用中，可通过保护工业控制系统安全的 7 个策略来进行纵深防御体系的构建。

1. 实现应用白名单（Application Whitelisting, AWL）
2. 确保合适的配置和补丁管理
3. 减少攻击面
4. 建立一个可防御的环境
5. 管理认证
6. 实现安全的远程访问
7. 监测和响应

虽然以上 7 个策略可以防止 90% 以上的攻击，但是还有一些攻击手段需要持续性的监测。此外，对于一些严重程度较低的异常，有些安全管理员很可能会忽略相关的告警，而这很可能是有黑客对工控系统进行 APT 攻击。如果将这些异常信息进行关联分析，从中发现潜在的安全隐患，不仅能够减少管理员的压力，还能更好地保护工控系统安全。

在第七个策略安全监测和响应中，需要对位于现场控制层的控制设备以及位于过程监控层的工作站的通讯过程进行安全监控。由此，可将工控安全监测预警体系的创建分为三个步骤。

1. 根据上文提到的 7 个策略，在各个节点添加适用于工控系统的安全设备，如在边界防护方面，布置工控防火墙、IDS 等。在工控网络内部，使用工控异常行为监测系统、资产识别系统等。将这些底层的安全系统部署在工控环境中，就可以很大程度地提升工控系统的安全性。
2. 在众多的底层安全系统之上，还需要一个监测审计和分析系统来对各个底层设备产生的告警记录、日志进行汇总，精炼和关联分析，深入挖掘出这些记录中隐藏的信息，以了解工控系统整体的安全态势。
3. 对未来的安全态势做出预测，如果有可能则提供必要的安全措施，同时提供更友好的可视化技术。

目前，工控网络安全监测预警方案的建立仍然处于初级阶段。我们需要根据工控安全的需求和工控设备的脆弱性，结合 7 个策略，制定适用于工控系统的安全产品，从各个威胁点上保护工控环境的安全。

3.2.3 内建安全

信息技术涉及的领域很多，但总体而言，主要包括硬件设备、软件程序和信息数据三大部分。由于对硬件设备的控制、对信息数据的操作处理需要软件来实现，因此软件是系统的“灵魂”，而程序代码是软件的具体呈现形式。可见，代码是信息化建设中的核心要素，是信息系统或基础设施中安全防护的重点。

信息技术采购全球化的发展态势使得国家或企业信息系统的产品来源更加多元化，信息技术的供应链更加复杂。软件构建方面更是如此。许多情况下，软件系统是来自世界各地的代码组合起来的，包括自主开发的、商业购买的、开源提供的、外包开发的等。VeraCode 公司曾统计过，30%-70% 自主开发软件的代码也含有第三方代码，并多以开源组件、商业或外包共享库 / 组件的形式存在。这种方式提高了软件开发的效率，但其安全性和可控程度无疑是巨大的挑战，尤其近年来 Struts2、OpenSSL 等广泛应用的基础开源组件高危漏洞频现，伊朗“震网”、乌克兰“黑暗能量”等基于基础软件漏洞的恶意程序肆意侵入工控系统，让国家和企业对软件供应链、开源软件、关键信息基础设施中软件安全性的关注程度逐渐提高，相应的措施在国家法规和战略中已有所体现。

为了保障软件安全，需要能够“尽早、尽快”的发现并修复软件系统中的漏洞。源码作为软件的原始形态，具备丰富的语义信息。对于源码的保障能够尽早且较为全面的发现软件中的问题，且符合内建安全（Build Security In，BSI）的原则。工业控制系统亦如此。工控系统内建安全需要重点关注工业应用软件、下位机以及其他智能装置的源码安全和通信协议安全，主要包括：

- 病毒运行依赖黑客对于嵌入式操作系统的了解，对下位机也是如此。无运行环境、无进入机会是解决问题的关键。操作系统不支持，病毒就无运行环境。对固件进行加密处理，黑客就无法破解固件以了解底层的机制。协议、接口私有、受限，黑客就无进入机会。因此，工控设备供货商应自主研发协议栈、控制算法、硬件平台、BIOS 以及确定性微内核，同时对固件进行加密，提高黑客入侵系统的门槛。
- 通过操作层、网络层、控制层、现场总线 / 无线层多层次数据通信加密和防护技术，保证数据的完整性和机密性；非明码传输，防止数据被窃听和篡改。

4

典型工业场景安全构建

4.1 电力行业工控典型安全解决方案

4.1.1 火电场景

4.1.1.1 系统简介

电力监控系统是以计算机、通讯设备、测控单元为基本工具，为火电厂的实时数据采集、开关状态监测及远程控制提供基础平台。它可以和检测、控制设备构成任意复杂的监控系统，在火电厂监控中发挥核心作用，可以帮助企业消除孤岛，降低运营成本，提高生产效率，加快变配电过程中异常的反应速度。

火电厂电力监控系统包括火电机组分散控制系统 DCS、火电机组辅机控制系统、火电厂厂级信息监控系统 SIS、调速系统和自动发电控制功能 AGC、励磁系统和自动电压控制功能 AVC、网控系统、相量测量装置 PMU、五防系统、远动系统、继电保护故障信息子站以及电能量采集装置等系统。其中，调速系统和自动发电控制功能AGC、励磁系统和自动电压控制功能AVC、网控系统、继电保护故障信息子站、远动系统、电能量采集装置是与调度中心有关的电力监控系统；火电机组分散控制系统 DCS、火电机组辅机控制系统、火电厂厂级信息监控系统以及五防系统是电厂内部监控系统；相量测量装置 PMU、继电保护故障信息子站以及电能量采集装置是调度中心监控系统的厂站侧设备。其架构如下图所示。

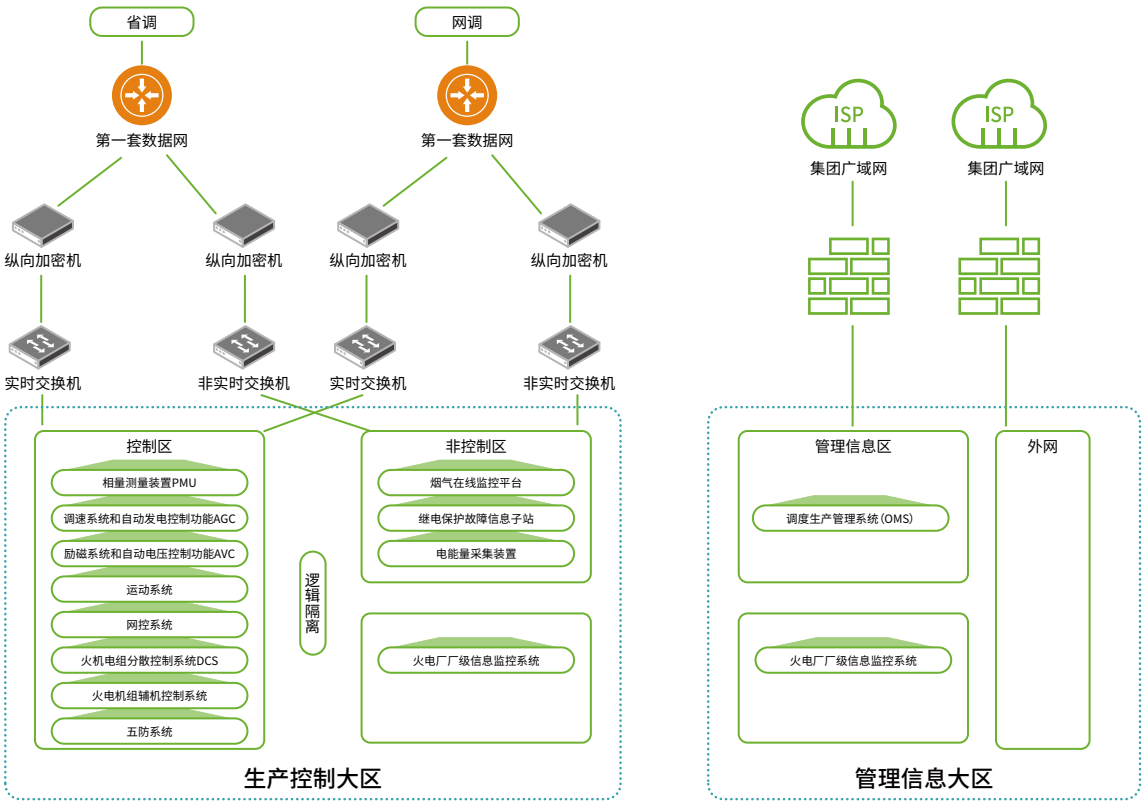


图 4.1 火电厂电力监控系统的网络架构图

上图为火电厂电力监控系统的网络架构图。电力监控系统主要与省调和网调进行外部纵向连接，并建立有第一套数据网和第二套数据网，形成了冗余结构。

4.1.1.2 系统安全防护方案

4.1.1.2.1 边界安全防护方案

- **横向边界安全防护**

  - **生产控制大区与管理信息大区横向边界防护措施**

在生产控制大区的安全 II 区和管理信息大区横向边界，根据火电厂数据交互的实际需要，部署正向安全隔离装置和反向安全隔离装置，用于支撑生产控制大区与管理信息大区的正向和反向数据流的安全防护需要。

- **控制区（安全 I 区）与非控制区（安全 II 区）边界安全防护**

在控制区与非控制区的两条网络边界处分别部署硬件防火墙，以限制安全级别低的系统对安全级别高的系统的非授权访问，为安全 II 区进入安全 I 区的数据流提供网络安全屏障。

对于和 SIS 接口机之间采用串口线进行连接的跨区连接，无法使用防火墙技术进行逻辑隔离，可将相关联的 SIS 接口机部署在控制区（安全 I 区）。对于接口服务器与 SIS 接口机未部署防火墙的，应增加工控防火墙。

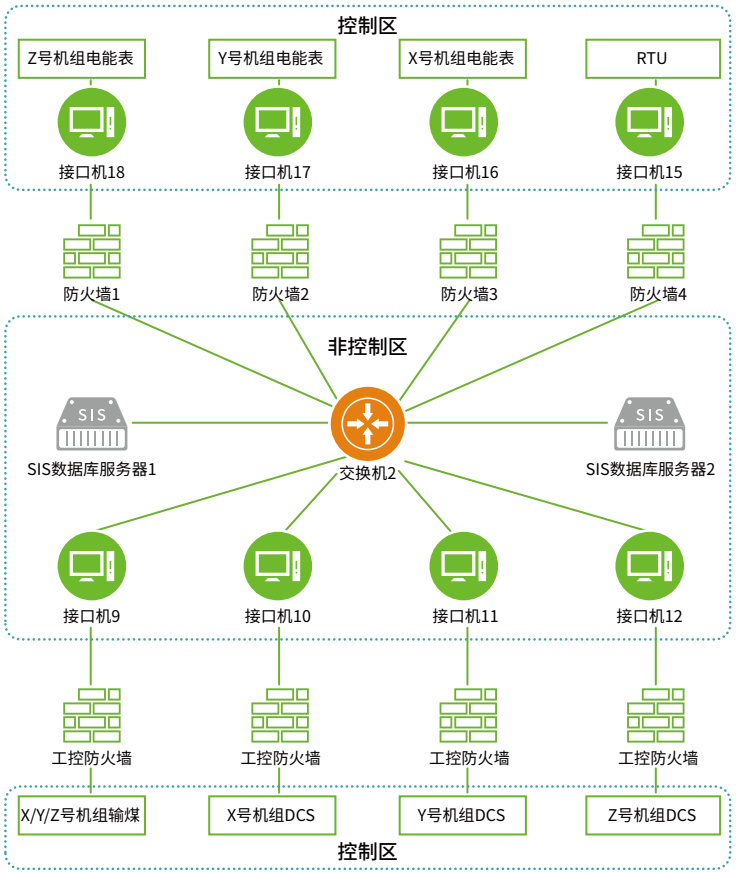


图 4.2 X/Y/Z 号机组 SIS 系统横向边界防护图

上图为 X/Y/Z 号机组 SIS 系统横向边界防护图，从图中可以看出，与 X 号机组电能表、Y 号机组电能表、Z 号机组电能表、RTU 关联的 SIS 接口机与交换机之间通过 4 台传统 IT 防火墙进行逻辑隔离，与 X/Y/

Z 号机组输煤、X 号机组 DCS、Y 号机组 DCS、Z 号机组 DCS 关联的 SIS 接口机边界处部署工控防火墙进行逻辑隔离。

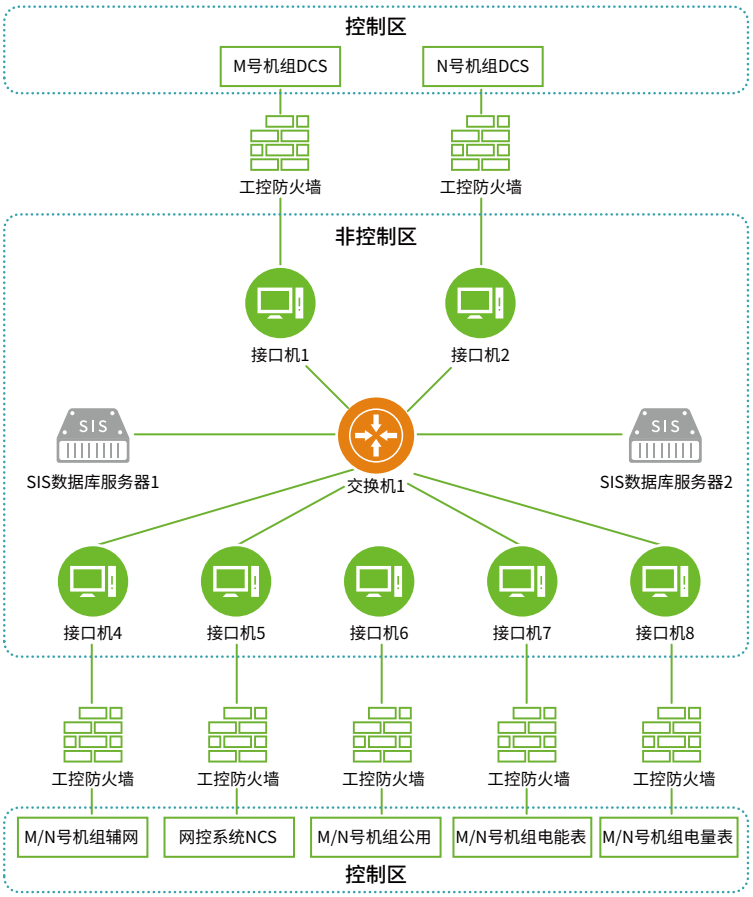


图 4.3 M/N 号机组 SIS 系统横向边界防护图

上图为 M/N 号机组 SIS 系统横向边界防护图，从图中可以看出，M 号机组 DCS、N 号机组 DCS、M/N 号机组辅网、网控系统 NCS、M/N 号机组公用、M/N 号机组电量表关联的 SIS 接口机边界处部署工控防火墙进行逻辑隔离。

- **系统间安全防护**

据国家发改委 14 号令的要求，电力监控系统各子系统应该直接采用逻辑隔离技术，如 VLAN 或防火墙技术。各子系统与其他系统采用 VLAN 技术进行逻辑隔离，以满足各子系统间连接相对独立和确保

系统可用性的需求。

- **纵向边界安全防护**

火电厂与省调通信通道共部署两套互为冗余的通信设备，并在安全 I 区的接入交换机与调度的出口路由器间部署相互独立的两套纵向加密装置。

火电厂与集控中心部署纵向加密认证装置，实现厂站与集控中心之间建立加密隧道，集控中心与电厂通信均采用双网关机冗余的方式，其中每台通信网关的光纤主通道和备用通道各部署一台纵向加密认证装置。

- **第三方边界安全防护**

针对存在第三方边界（例如需要与环保部门进行连接）的火电企业，应采取电力专用隔离装置进行同等级的安全防护。

4.1.1.2.2 综合安全防护方案

- **入侵检测**

根据国家发改委 14 号令的要求，生产控制大区需要统一部署网络入侵检测系统，应当合理设置检测规则，检测发现隐藏于正常信息流中的入侵行为，分析潜在威胁。

生产控制大区部署的入侵检测系统，一方面可以满足发改委 14 号令及国能安全 36 号文有关合规的安全要求，另一方面可以检测管理大区和生产大区边界的入侵行为。针对工控网络的 APT 攻击威力巨大，甚至可能从管理网络穿透横向隔离装置流向生产网络。同时，由生产控制大区控制系统发起的流向管理大区的安全攻击也不容忽视。因此工控网络入侵检测系统需要进行双向的入侵行为检测。另外，对于 SIS 系统的交换机不支持端口镜像功能的情况，可以考虑替换为支持端口镜像的交换机或者采取外接支持端口镜像功能的交换机的形式进行端口流量的镜像。

- **主机与网络设备加固**

根据国家发改委 14 号令的要求，发电厂厂级信息监控系统等关键应用系统的主服务器，以及网络边界处的通信网关机，web 服务器等，应当使用安全加固的操作系统。加固方式包括安全配置、安全补丁、采用专门软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当先经过测试。

在火电厂电力监控系统中操作员站、工程师站、历史站、OPC 服务器、通信机、OPC 接口机、数据库服务器等关键主机上部署工控终端安全管控系统，并使用基于白名单的安全策略进行安全配置。部署的工控终端安全管控系统应与 DCS 系统原厂商进行联合实施。

- **存储器与外设管理**

根据国家发改委 14 号令的要求，火电厂应当对外部存储器，打印机等外设的使用进行严格管理，防止恶意代码通过外部存储器等传播路径摆渡进入电力监控系统。应对打印机进行严格管理，设置计算机打印身份鉴别功能，防止未授权人员使用打印机。在火电厂的生产控制大区重要控制系统（如机组主控 DCS 系统）的工程师站、操作员站和历史站部署运维管控系统，实现对外部存储器（如 U 盘）和键盘、鼠标等使用 USB 接口设备的识别，对文件进行数据加密、病毒查杀，记录交换日志、交换数据，支持查询、回溯等功能，对外部存储器的使用进行严格控制。部署的运维管控系统不能影响生产控制大区各系统的正常运行。

- **安全审计**

根据国家发改委 14 号令的要求，火电厂可通过在电力监控系统各独立子系统中部署工控安全预警平台——安全审计探针，对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等进行集中收集，在管理信息大区部署工控安全预警平台，接收安全审计探针的审计数据实现自动分析和预警。部署的工控安全监测预警平台可以作为电力监控系统防护技术的总人机接口，对所有部署在工控网络内部的信息安全产品进行管理、分析、报警及审计。工控安全预警平台以独立工作站形态接入到工业控制网络，通过工控环境主网络与工业防火墙、工业组态软件、工业交换机、系统工作站（工程师站、操作员站）、工业控制器（PLC、RTU、DPU）以及其他工控设备实现集中管理和监控，实现工控网络环境下的资产、行为、流量和协议的可视化。

- **数据备份**

根据国家发改委 14 号令的要求，应当定期对关键业务的数据进行备份，并实现历史归档数据的异地保存。火电厂应当利用存储设备（如磁带机）定期对关键业务的数据进行备份，并将备份好历史归档数据的存储介质（如磁带）放置到异地（如二级单位）进行保存。

- **恶意代码防范**

根据国家发改委 14 号令的要求，应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应

当经过测试。对于已部署防恶意代码软件的系统工作站，应严格禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。对于未部署防恶意代码软件的系统工作站，可通过结合系统原厂商实施的 DCS 安全防护系统进行恶意代码的安全防护。

4.1.2 风电场景

4.1.2.1 系统简介

风电场监控系统是以计算机、通讯设备、测控单元为基本工具，为风电场的实时数据采集、开关状态检测及远程控制提供了基础平台。它可以和检测、控制设备构成任意复杂的监控系统，在风电场监控中发挥核心作用，可以帮助企业消除孤岛、降低运作成本，提高生产效率，加快变配电过程中的反应速度。其系统架构如下图所示。

图 4.4 风电场监控系统的逻辑架构图

上图为风电场监控系统的逻辑架构图，目前电力监控系统主要与调度一平面、调度二平面以及风电场集控中心进行外部纵向连接。

风电场按照国家发改委 14 号令的要求进行安全分区，将电站网络分为生产控制大区和管理信息大

区，其中生产控制大区又根据控制实时性划分为控制区（俗称安全 I 区）和非控制区（俗称安全 II 区）。生产控制大区与调度一平面、二平面控制大区采用纵向加密认证装置实现了纵向认证加密；控制区与非控制区进行逻辑隔离，分别接入第一套数据网（一平面）和第二套数据网（二平面）。

风电场根据国家发改委 14 号令的相关划分标准，将电力监控系统中的风电场监控系统、综合自动化系统、自动发电控制功能 AGC、自动电压控制功能 AVC、相量测量装置 PMU 放置在控制区中，将功率预测系统、状态监测系统、故障录波、电能量采集装置放置在非控制区中，管理信息大区和 OMS 工作站单独组网。

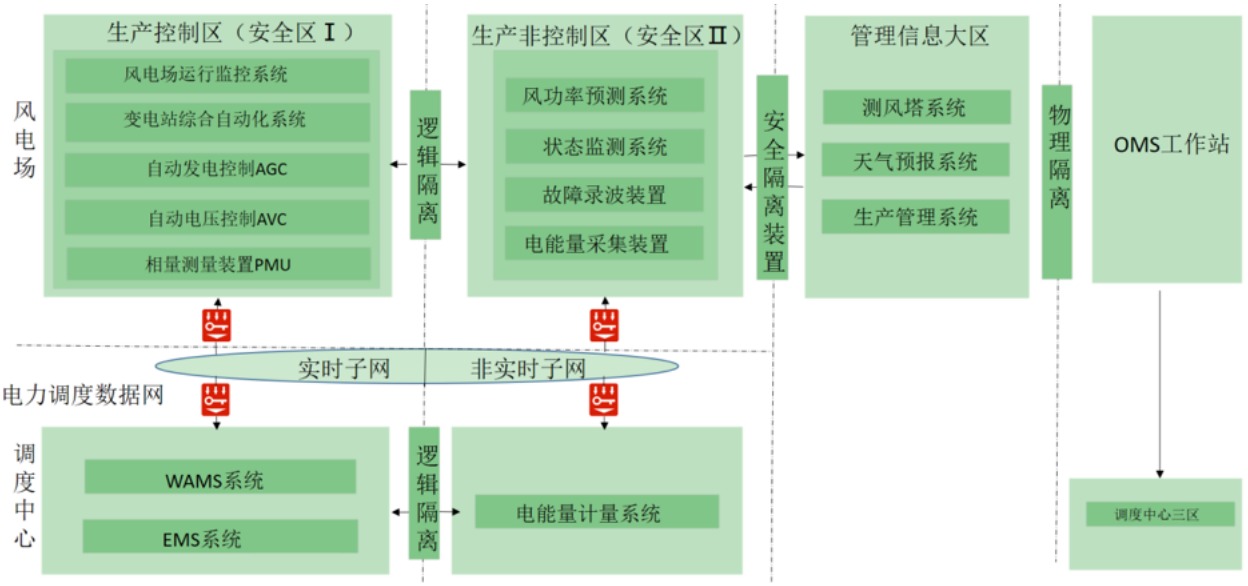


图 4.5 风电场监控系统安全分区示意图

4.1.2.2 系统安全防护方案

4.1.2.2.1 边界安全防护方案

- **横向边界安全防护**

根据国家发改委 14 号令的要求，风电场生产控制大区与管理信息大区之间通信部署电力专用横向单项安全隔离装置。控制区（安全 I 区）与非控制区（安全 II 区）边界应当采用访问控制的网络设备、硬件防火墙设备实现逻辑隔离、报文过滤、访问控制。生产控制大区与管理信息大区之间根据数据访问的方向部署正向安全隔离装置或者反向安全隔离装置。风电场监控系统各子系统之间应该采用逻辑隔离

技术，如 VLAN 或防火墙技术。

- **纵向边界安全防护**

根据国家发改委 14 号令的要求，风电场监控系统进行远程通信时应部署电力专用纵向加密认证装置，实现双向身份认证、数据加密和访问控制。

- **第三方边界安全防护**

根据国家发改委 14 号令的要求，风电场监控系统管理大区与外部网络之间应部署防火墙，保证边界与数据传输的安全。在信息管理大区与外网边界部署安全网关（防火墙），在 OMS 工作站与调度三区边界处部署安全网关（防火墙）。

4.1.2.2.2 综合安全防护方案

- **入侵检测**

根据国家发改委 14 号令的要求，在生产控制大区控制区（安全 I 区）与非控制区（安全 II 区）和 OMS 工作站汇聚交换机分别部署入侵监测系统，合理设置检测规则，检测发现隐藏于流经网络边界正常信息流中的入侵行为，分析潜在威胁并进行安全审计。入侵检测系统为旁路部署，仅接受并分析交换机镜像过来的数据，不参与数据的转发工作。

- **主机设备与网络配置安全加固**

根据国家发改委 14 号令的要求，风电厂厂级信息监控系统等关键应用系统的主服务器，网络边界处的通信网关机，web 服务器等，应当使用安全加固的操作系统。加固方式包括：安全配置、安全补丁、采用专门软件强化操作系统访问控制能力以及配置安全的应用程序，其中配置的更改和补丁的安装应当经过测试。在风电场监控系统中进行加固时使用主机安全加固软件进行加固，需要的加固软件的版本包括 Windows 版、Linux 版。

- **存储器与外设管理**

根据国家发改委 14 号令的要求，应当对外部存储器，打印机等外设的使用进行严格管理。通过对外部存储器，打印机等外设进行严格管理，防止恶意软件通过外部存储器进入风电场监控系统。通过部署的主机安全加固软件实现对外部存储器（如 U 盘）和键盘、鼠标等使用 USB 接口设备的识别，对外部存储器的使用进行严格控制。

- **安全审计**

根据国家发改委 14 号令的要求，生产控制大区的监控系统应当具备安全审计功能，能够对操作系统、数据库、业务应用的重要操作进行记录、分析，及时发现各种违规行为以及病毒和黑客的攻击行为。对于用户登录到系统中的操作行为进行严格的安全审计，对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等进行集中收集、自动分析。

- **数据备份**

根据国家发改委 14 号令的要求，应当定期对关键业务的数据进行备份，并实现历史归档数据的异地保存。风电场监控系统建议通过管理制度将关键的程序、软件、配置文件等定期进行备份。

- **恶意代码防范**

根据国家发改委 14 号令的要求，应当及时更新特征码，查看查杀记录。恶意代码更新文件的安装应当经过测试。禁止生产控制大区与管理信息大区共用一套防恶意代码管理服务器。风电场在生产控制大区部署防病毒管理服务器，在生产控制大区 linux、Windows 主机部署防病毒软件，通过防病毒管理服务器集中管理及升级防病毒软件。

4.1.3 水电场景

4.1.3.1 系统简介

水电厂的计算机监控系统采用全计算机控制的分层分布开放式系统结构，由按功能分布的主控层及按对象分布的现地单元层组成。主控层设备包括操作员站、数据服务器站、厂外通信站、厂内通信站、工程师站、语音报警站、GPS 时钟同步系统、UPS 电源及网络设备等。

主控层从 LCU 实时采集反映全厂主要设备运行状态和参数的各类数据，如通信量、模拟量、脉冲量、交流量、扫查开关量和中断开关量等，并对全厂主要设备进行集中监控管理，主要包括设备调节控制、工况转换及参数设置、防误操作输出闭锁、报警记录及历史查询、事件顺序记录、事故追忆、温度趋势报警与分析、事故语音报警、画面软拷贝、生产统计报表生成、系统数据库管理等功能，实现自动发电控制 (AGC) 和自动电压控制 (AVC) 等高级应用。

LCU 作为监控系统的底层控制设备，主要是完成各类数据的采集与预处理，并向主控级发送采集的数据和各类报警信息，同时接受主控级的控制命令，进行有效性检查并核对后执行。而当主控级出现故

障或退出运行时，LCU 仍能正常运行并就地实现对设备的基本监控功能，如：数据采集、处理和设备运行监视；设备调节控制、工况转换及参数设置等操作；事件顺序记录；硬件自诊断功能，并进行在线诊断报警。

4.1.3.2 水电厂风险分析

1. 网络安全风险

① 网络边界防护力度不足。虽然水电厂的生产控制大区与管理信息大区之间不存在直接的物理网络连接，但是在生产控制大区中的实时区与非实时区各系统之间的边界防护措施不太完善，缺乏对工业协议的支持以及对工业病毒的防护。

② 接入区缺乏保护。电厂电力生产工控系统中，处于非实时区的水情系统的后端与前端测控站之间通过微波进行无线通信，在接收端缺乏安全防护设备对数据的无线输入进行安全防护。

③ 缺乏入侵检测防护管理机制。水电厂的生产管理区、实时区、非实时区的关键网络节点处入侵检测设备不完善，导致无法有效的检测、阻止或限制从内 / 外部发起的网络攻击行为，无法对网络行为进行分析。

2. 主机安全风险

恶意代码 / 病毒防范机制缺失。电力监控系统中的主机暂未部署恶意代码防范平台，也没有采取其他补偿机制对恶意代码进行控制管理。

3. 应用安全风险

账号管理及认证缺失，水电厂目前针对各系统根据岗位和级别分别设置了相应权限级别的账号，但缺少必要的应用安全控制策略对用户登录应用系统、访问系统资源等操作进行身份认证、访问控制和安全审计。

4. 系统运维安全风险

① 缺乏对移动介质的安全管控。电力监控系统各设备的 USB 接口未通过部署管控平台进行控制。

② 缺少对信息系统的监测审计。目前水电厂实现了对电力监控系统的监控，但缺少针对上位机、服务器、操作系统、数据库等的监测审计能力，更无法实现对电力监控系统安全设备的监管。

③ 缺乏针对重要控制设备的防护。水电厂目前暂未在各控制系统 PLC 前端部署具备工业协议深度包检测功能的防护设备，限制违法操作和针对控制器的入侵行为。

4.1.3.3 水电厂安全防护方案

1. 用工业防火墙代替现有的常规防火墙，在机组 LCU 交换机至监控系统上位机核心交换机之间部署智能保护设备，在水情系统接收遥测数据的链路上部署单向隔离装置，在管理信息大区与互联网入口前部署入侵防御装置和漏洞扫描装置。
2. 工控系统上位机主机加固建设，在监控系统上位机、水情系统上位机、闸门监控系统上位机、工业电视工作站、电能计量小子站上部署工控终端保护软件，用终端管控平台进行统一管理，在监控系统工程师站、水情工程师站、闸门监控系统工程师站等上位机上部署 USB 保护设备。
3. 部署监测审计设备，建立专门针对水电厂的在线全网监控审计平台。将监测审计设备以旁路模式分别部署在生产控制大区监控层核心交换设备一侧，可对生产控制操作与威胁流量进行审计和监测。它可以提供整个控制网络的总体运行情况，自动识别网络设备，显示网络设备当前状态，进行网络性能综合分析；监测所有通过工业控制系统重要的网络节点或区域的数据包；对数据包进行深度解析，发现异常或非法操作的数据包，分析是否有外界入侵或人员误操作；对所有异常情况发出报警，提醒现场操作人员。

4.1.4 核电场景

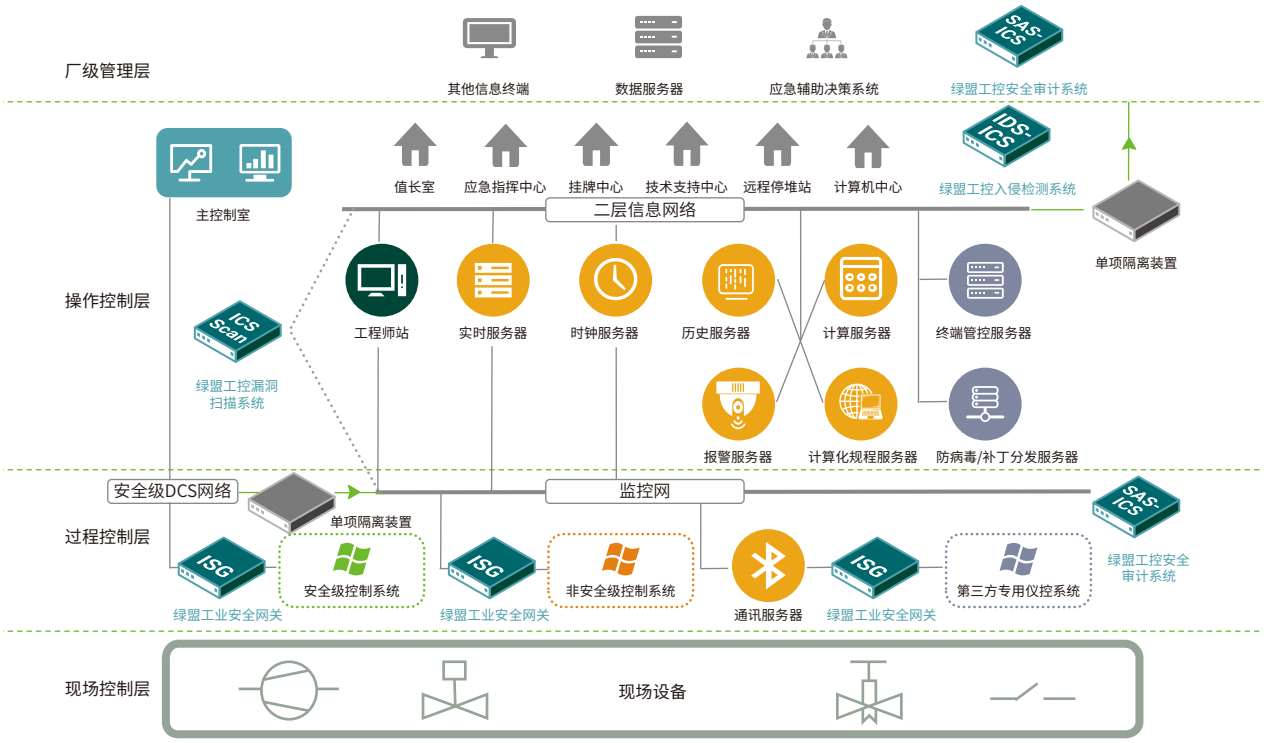


图 4.6 核电站安全防护图

核电与火电的安全场景类似，具体的场景与保障框架可以参考火电的场景。概括说来主要分为以下几个部分：

安全威胁检测：部署工控漏洞扫描系统对上下位机操作系统和应用软件进行漏洞扫描，对工控资产进行风险评估和验证漏洞修复情况；

网络边界防护：在二层信息网和厂级管理层之间、安全级控制系统和非安全级控制系统之间部署单向隔离装置实现数据单向传输；在监控网和现场控制层之间、监控网和第三方专用仪控系统之间部署工业安全网关阻断来自监控网的病毒传播、黑客攻击等行为，限制非法操作，避免其对控制网络的影响和对生产流程的破坏；

内部网络监测：在二层信息网和监控网分别旁路部署工控入侵监测系统和工控异常行为审计系统，准确监测网络异常流量，通过对相关工控协议进行深度解析，及时发现潜在的网络攻击和异常行为，并在第一时间告警；

主机安全加固：对主机终端进行安全加固，实现对账号权限、口令策略、系统服务、补丁更新、日志管理等方面的安全配置，结合核电业务需求和相关信息安全标准规范制定各类主机资产安全配置基线，并部署工控安全配置核查系统定期进行安全配置审计；

终端综合管控：在主机终端部署工控终端管控系统对外设进行严格的访问控制、状态监控、进程监控、病毒防护、补丁升级、恶意代码监测、操作行为审计、基于白名单机制的应用程序管控等。

4.2 制造业工控典型安全解决方案

4.2.1 烟草行业

4.2.1.1 系统简介

4.2.1.1.1 卷烟厂网络架构

卷烟厂的网络架构由生产网和管理网两部分构成。如图所示。

典型工业场景安全构建

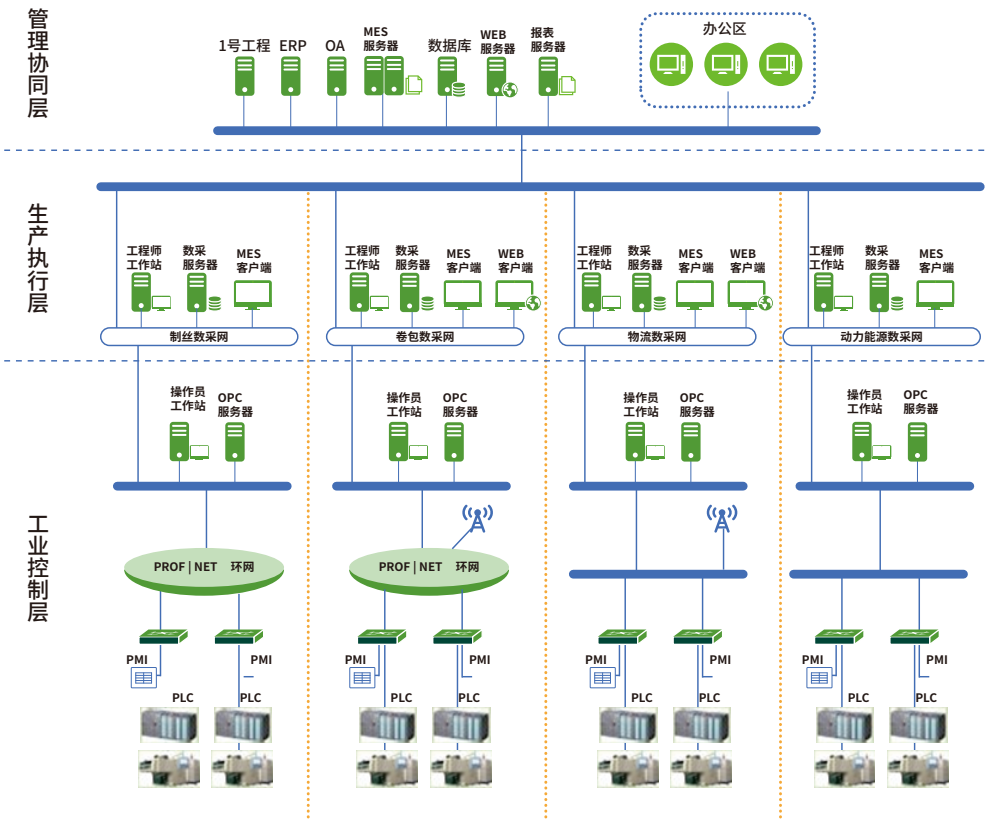


图 4.7 卷烟厂网络架构图

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，管理信息系统融合信息服务、决策支持于一体。

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是管理执行，对下层生产控制系统是调度指挥，

在管理协同层和工业控制层数据双向通道中起到核心作用。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。

工业控制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、卷包机组、动力能源中心、物流中心等生产系统。主要完成加工作业、检测和操控作业、作业管理等功能。

4.2.1.1.2 卷烟厂面临的安全问题

卷烟厂所面临的安全问题包括两个层面：网络与通信层面和控制器、主机及应用层面。以下进行分别介绍。

- 网络与通信层面的安全问题：

1. 生产网与管理网之间安全隔离机制不合理。

目前生产网与管理网之间的安全隔离机制主要有以下几种。

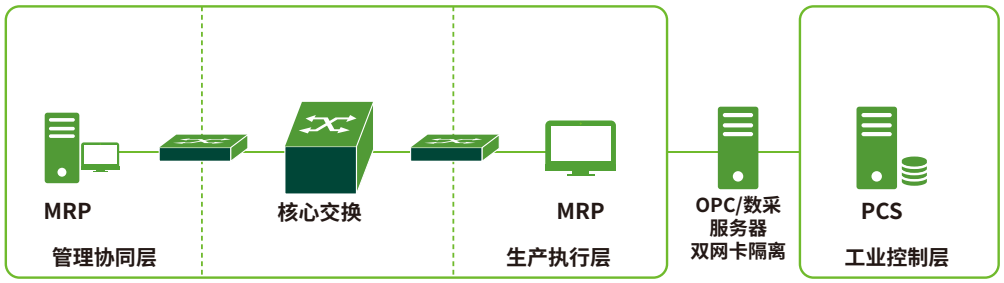


图 4.8 数据采集服务器或 OPC 服务器双网卡隔离

如图所示，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被病毒感染，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。

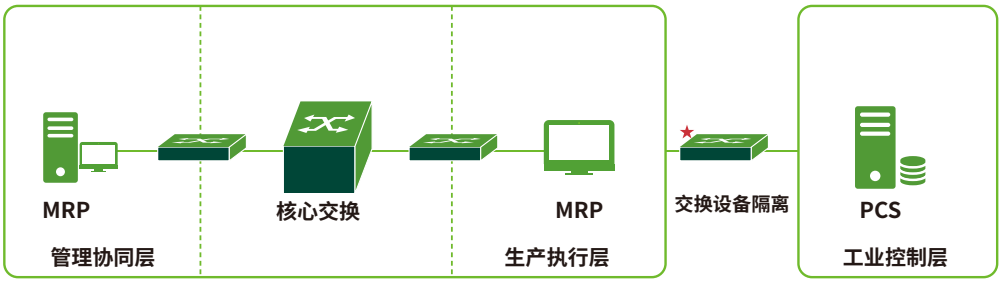


图 4.9 交换设备隔离

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。

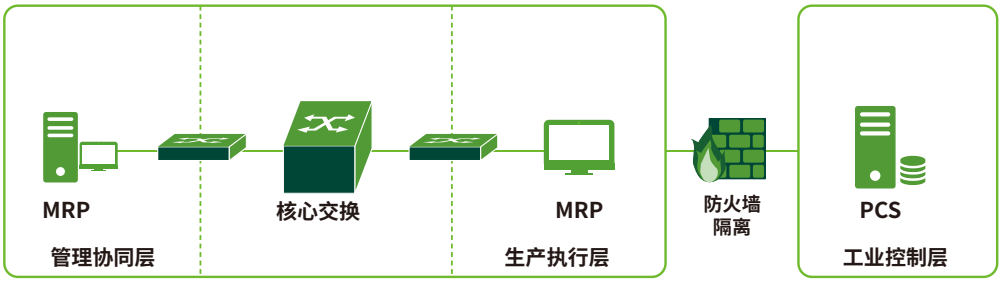


图 4.10 防火墙隔离

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。

2. 控制指令数据通信明文传输

主要传输的数据包括管理网内部数据通讯和工业控制指令（如 ProfiNet/ProfiBus、ModBus、DNP3 等）。

3. 生产网无线网络管控机制缺失或不完善

如 AGV 无线引导小车。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（WiFi）。

4. 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。

5. 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的根本原因，最终无法对事件进行定性分析。

- 主机及应用层面的安全问题：

1. 工业控制系统自身存在大量漏洞

目前烟草行业工业控制系统使用的比较主流的品牌是 Siemens S7 系列 PLC、Rockwell AB PLC 以及 GE PLC。这些设备中普遍存在着安全漏洞。这些漏洞包括拒绝服务漏洞，缓冲区溢出漏洞，可能造成信息泄露、远程控制及权限提升类的漏洞等。这些漏洞一旦被利用可以造成卷烟厂的业务中断，卷烟生产企业的生产计划、工艺流程等敏感信息被窃取，甚至可以获得工控系统的控制权，干扰、破坏卷烟厂的正常生产或运营活动。

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 的前端现场操控触摸屏 HMI 的登陆身份认证机制不完善，弱口令现象普遍存在，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，系统存在的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，导致存在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。

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，因此不安装防病毒软件，这就给病毒与恶意代码的感染与扩散留下了空间。而对于数采服务器和 Web 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。

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。这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。这相当于对车间 PLC 控制器可以随意操作，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。

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、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权限，或者登录账号和初始密码都是默认的，并且没有设置密码保护策略。攻击者可获得数据库权限，并任意破坏、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存储与备份机制，无法应对偶然事故的发生，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。

4.2.1.2 系统安全防护方案

4.2.1.2.1 边界安全防护方案

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。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：

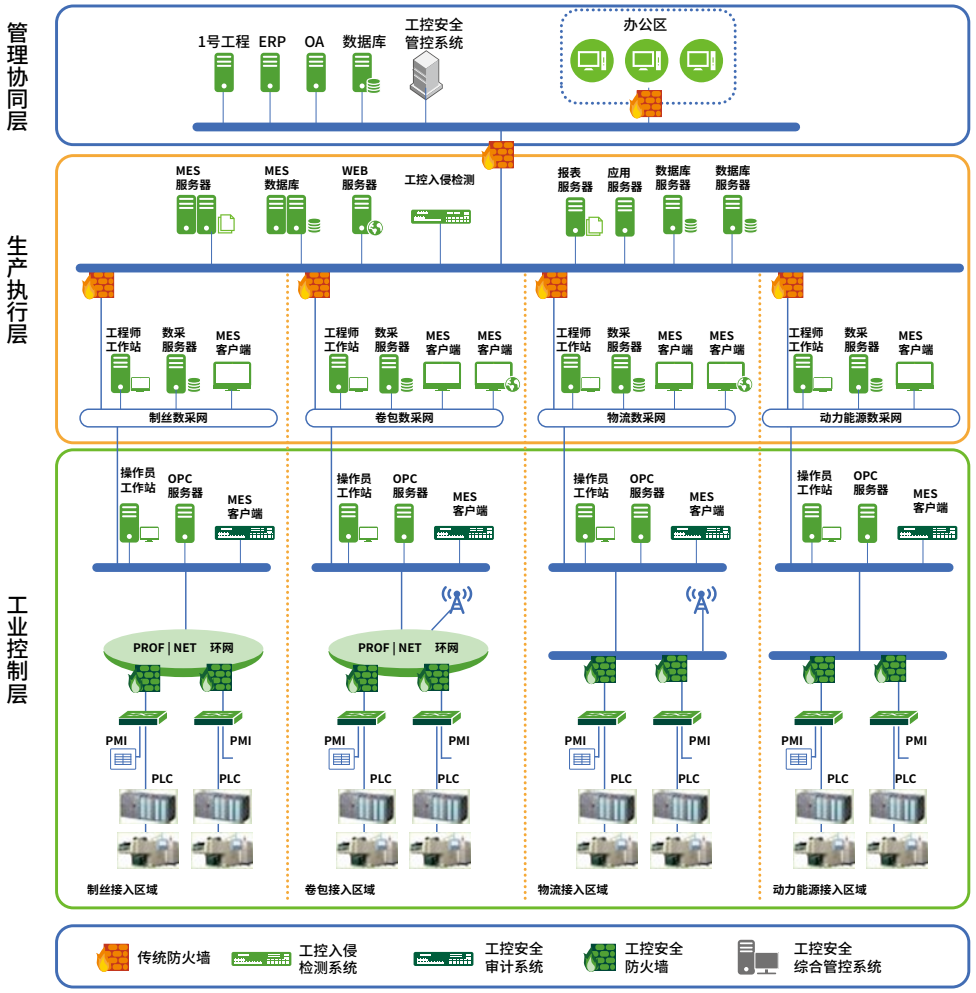


图 4.11 卷烟厂安全防护图

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，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）的数据包进行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生产业务的影响。

4.2.1.2.2 综合安全防护方案

- 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传输的指令信息进行有效审计，检测其中的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指令的下发，审计设备可以进行及时的告警。并且在对异常操作的追诉过程中，审计设备可以实现对恶意事件和行为的事后追查稽核，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。

- 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。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的监控并生成告警信息。各车间系统运维人员可以通过对监控告警的设置、筛选、分析完成对威胁的监视、分析、诊断的工作。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，并对各类事件的统计结果和发展态势进行呈现。

- 系统上线前安全评估

目前在卷烟生产企业中，工业控制设备（PLC）的入网与上线管理机制比较欠缺。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和相应的工控设备与系统提供商进行联系，获取相关的漏洞解决方案。漏洞的检测主要包括对已知漏洞的漏洞扫描技术和主动漏洞挖掘技术（FUZZ 技术）等。

4.2.2 汽车制造业

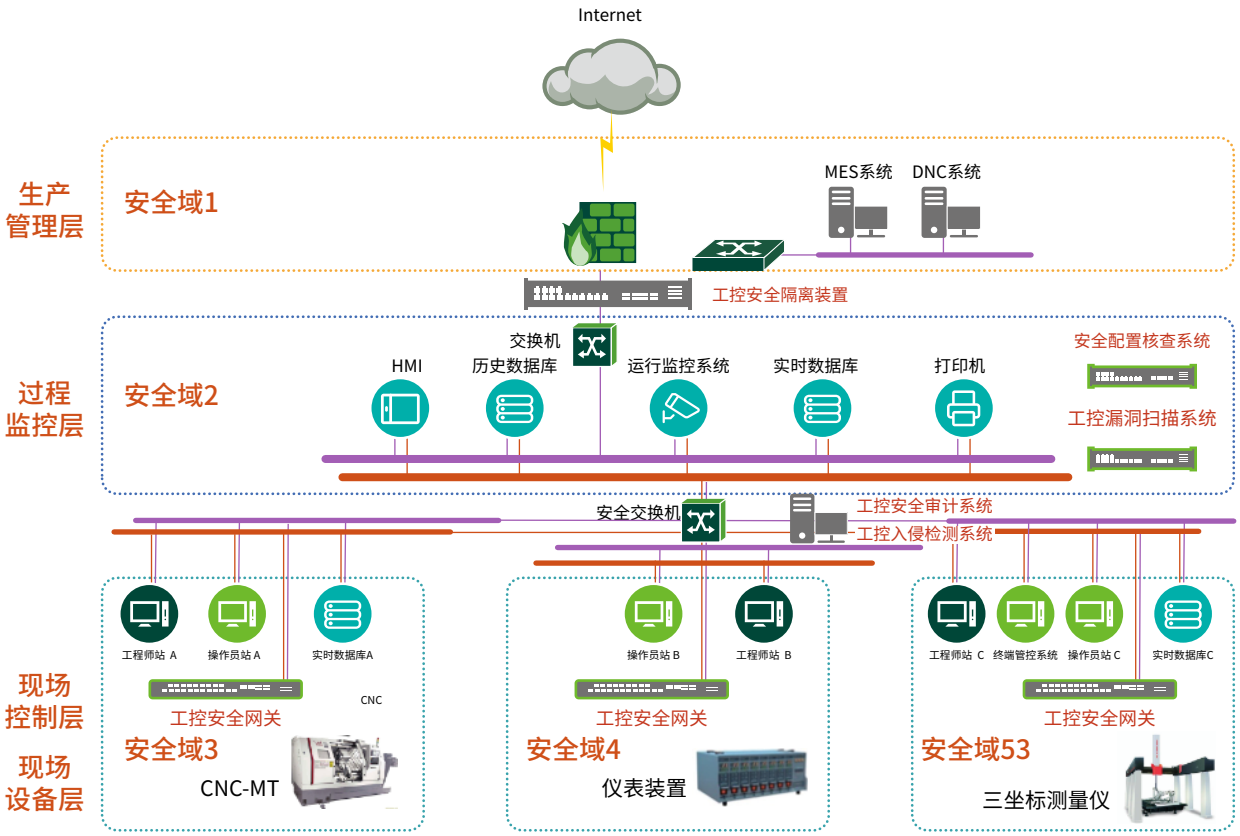


图 4.12 车厂安全防护图

- 外部边界隔离和监测。外部边界为 ICS 区域与 IT 区域的边界，即安全域划分示意图中安全域 1 与安全域 2 之间的边界，部署工控安全网关，作为外部威胁进入 ICS 环境的第一道边界防护；
- 工控环境中的细分安全域边界之间部署工控安全网关，形成纵深防御的结构，对通信行为进行严格控制。对应图中的安全域 3、安全域 4、安全域 5 与安全域 2 之间的边界分别部署控制设备；
- 在安全域 2 中部署工控安全审计系统，对流量和操作进行审计，并对工控环境中分布式部署的所有工控设备的运行状态和日志进行集中监控；
- 在安全域 2 中部署工控漏洞扫描和工控安全配置核查系统，辅助运维过程中的脆弱性管理；

- 在工控环境中所有安全域中的 IT 服务器和 PC 设备部署终端管控系统，实施外设管控、进程管控和恶意代码防范；
- 如果在工业网中存在自动化设备厂商远程运维的情况，需要在网络中部署 VPN 或者 CA 认证系统，用以识别远程运维人员的身份，提高工业网远程接入的可信化认证能力。

4.3 市政工控典型安全解决方案

4.3.1 水务场景

4.3.1.1 水务 SCADA 系统架构

水务的 SCADA 系统主要由操作员站，工程师站，取水泵房 SCADA 系统，加药间 SCADA 系统，反冲洗 SCADA 系统，送水泵房 SCADA 系统，脱水泵房 SCADA 系统等构成。其具体的结构图如图所示。

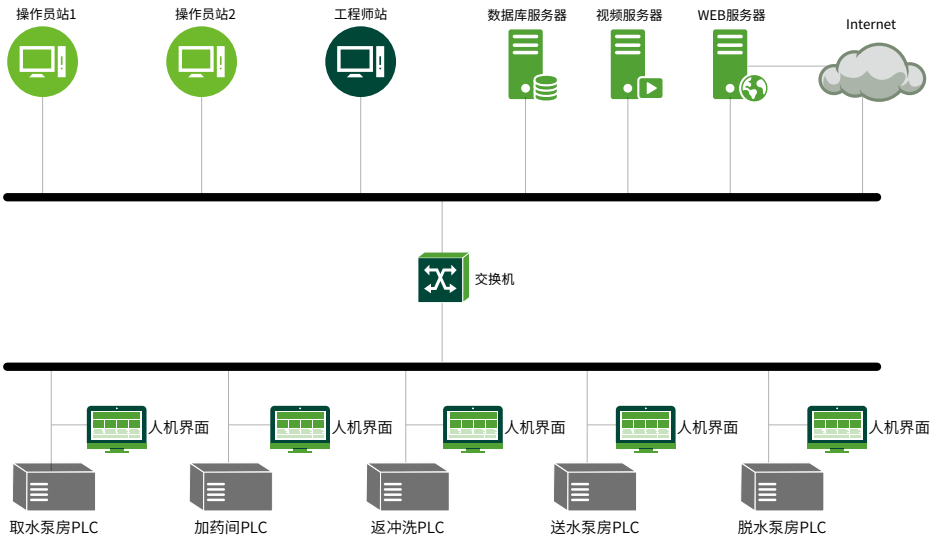


图 4.13 自来水厂安全防护图

4.3.1.2 安全需求分析

1. 门户网站安全分析

水务系统门户网站可以从外网直接访问，因此访问群体较复杂，聚集了大量的国内外访问流量，也容易引起黑客的关注。其所面临的安全威胁主要有：

① 黑客通过 SQL 注入、跨站脚本等攻击方式，可以轻松的拿到门户网站的管理权限，进而篡改网页代码；攻击者有可能将门户网站替换成钓鱼网站或者黄色网站，或者在主页上发布敏感言论，对企业造成极其恶劣的负面影响。

② 入侵者成功获取 WEB 服务器的控制权限后，可以以该服务器为跳板，对内网进行渗透、探测扫描，发起攻击，对企业内部敏感数据造成威胁。而从当前主机安全评估结果来看，黑客进入内网后，可以轻而易举攻陷其他服务器。

传统的边界防护设备，如防火墙和入侵防护系统，作为整体安全策略中不可缺少的重要模块，局限于自身的产品定位和防护深度，不能有效的针对 Web 应用攻击提供完善的防御能力。因此，有必要采用专业的 WEB 防护系统，有效防护各类攻击、降低网站安全风险。

2. 网络边界安全分析

计算机网络本身具有一定的脆弱性，随时都有可能遭受来自各方面的袭击和破坏，有些甚至是毁灭性的。网络不安全的主要因素如下：

① 网络协议的自身并不安全。网络是一个开放式的信息系统，可以与 Internet 相联，与网络中任何一台计算机进行信息交互。由于 TCP/IP 协议自身存在脆弱性，网络处于危险之中。

② 病毒蠕虫的快速传播。水务系统内网一旦遭受了病毒和蠕虫的侵袭，不仅会造成网络和系统处理性能的下降，同时也会对核心敏感的数据造成严重的威胁，甚至造成网络的拥塞，导致业务的中断。

③ 现有防火墙解决方案的不足。在网络应用层出不穷、新型威胁不断涌现的背景下，无论是传统防火墙、统一威胁管理设备（UTM）还是“下一代防火墙（NF）”，均已远远不能满足用户对自身网络的安全防护诉求，主要体现在传统防火墙不能对网络应用、用户进行有效识别和控制，现有的基于 IP 地址的访问控制已经不可靠。

3 业务系统安全分析

随着网络环境的不断发展和完善，水务系统中不仅各项业务工作如订单管理、文件分发等由计算机替代，而且信息存储及信息提供也转变为数字方式。业务系统不安全的主要因素如下：

① 系统漏洞给业务系统造成极大的威胁。恶意入侵者可以利用系统的漏洞，通过发起恶意扫描和远程溢出等攻击，进入业务系统后台，获取、篡改甚至破坏敏感的数据，乃至破坏整个网络的正常运行。

② 网络安全审计问题尤为突出。防火墙、入侵检测等传统网络安全手段可实现对网络异常行为的管理和监测，如控制网络连接和访问的合法性、监测网络攻击事件等，但是不能监控网络内容和已经授权的正常内部网络访问的行为，因此对由于正常网络访问行为导致的信息泄漏事件、网络资源滥用行为（即时通讯、论坛、在线视频、P2P 下载、网络游戏等）无能为力，也难以实现针对内容、行为的监控管理及安全事件的追查取证。因此，迫切需要一种安全手段对上述问题进行有效监控和管理。因此对于任何一个安全体系来说，审计追查手段都是必不可少的。

③ 人为失误及业务权限管理问题，如弱口令，不正确的共享、应用系统的错误使用等，内部人员对业务应用系统的越权访问、违规操作，或者操作人员直接的错误输入导致系统宕机等。

4.3.1.3 安全解决方案

1. 门户网站防护

采用 web 应用防护系统来确保 web 应用系统安全。Web 应用防护系统需要具备针对“攻击事件”提供事前预防、事中防护、事后补偿的整体解决方案。作为 web 客户端和服务器端的中间人，Web 应用防护系统可以避免 web 服务器直接暴露于互联网上，监控 HTTP/HTTPS 双向流量，对网络层、Web Server/Application 层双向数据实施检测和保护，可以降低 web 站点的安全风险，并需要能够护各类带宽及资源耗尽型拒绝服务攻击。

2. 网络边界防护

采用网络入侵防护系统实现网络边界的安全防护。网络边界的安全防护系统具有智能协议识别和分析，协议异常检测，流量异常检测的功能，有效发现绑定在任意端口的各种木马、后门，发现未知的溢出攻击、零日攻击以及拒绝服务攻击，并可以有效抵御分布式拒绝服务攻击 (DDOS)、未知的蠕虫、流氓流量的攻击。

3. 网络安全审计

水务系统中需要部署安全审计设备，主要完成以下功能：

① 内容审计。提供深入的内容审计功能，可对网站访问、邮件收发、远程终端访问、数据库访问、数据传输、文件共享等提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪。

② 行为审计。提供全面的网络行为审计功能，根据设定的行为审计策略，对网站访问、邮件收发、数据库访问、远程终端访问、文件上传下载、即时通讯、论坛、移动应用、在线视频、P2P 下载、网络游戏等网络应用行为进行监测，对符合行为策略的事件实时告警并记录。

③ 流量审计。提供基于协议识别的流量分析功能，实时统计出当前网络中的各种报文流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

4.3.2 城市燃气系统安全解决方案

4.3.2.1 总体概述

城市燃气系统 SCADA 系统主要由调度控制中心、储配站门站、输配站、无人站、重要用户监测点等组成。SCADA 系统主要由调度控制中心、站控系统及数据传输通讯系统三大部分组成。其特点为调度中心和子站相互配合的方式。其具体的架构如图所示。

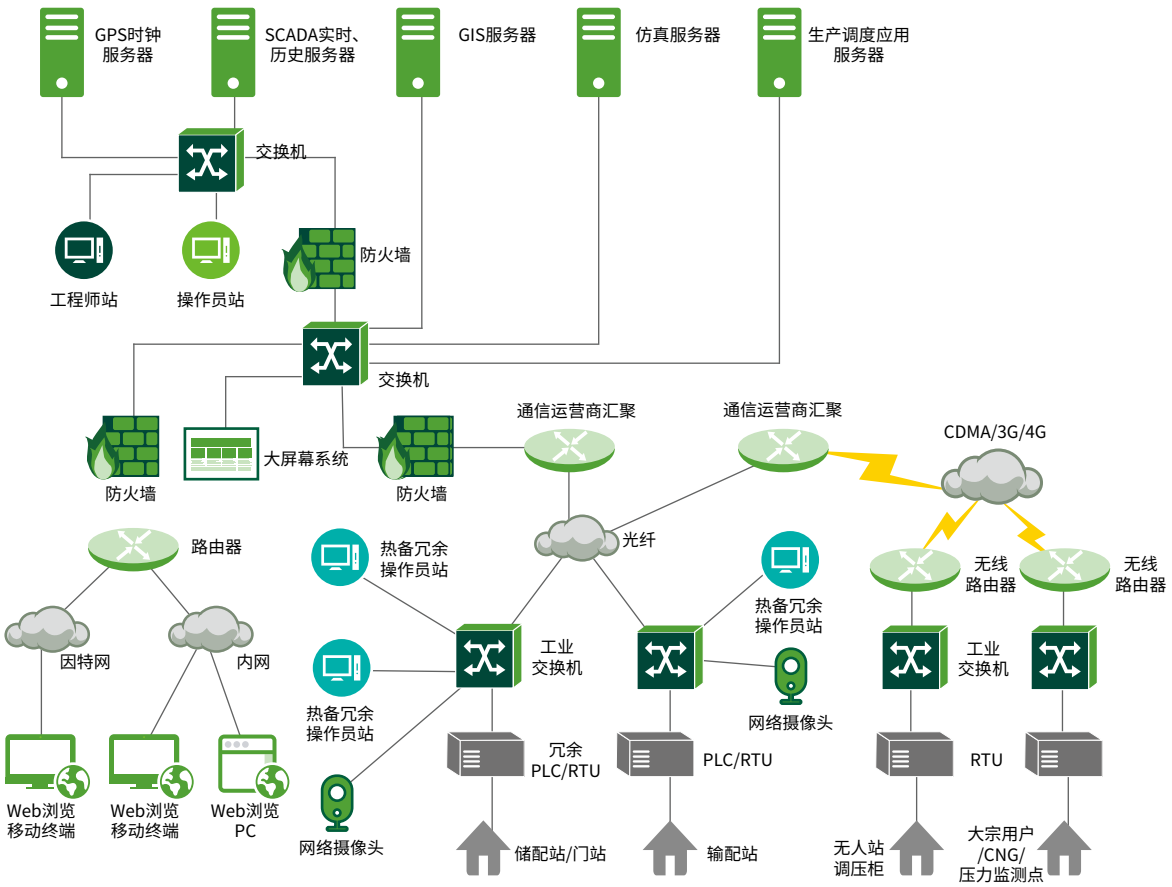


图 4.14 城市燃气安全防护图

调度控制中心：根据 SCADA 系统规模大小分为总调度控制中心、备用调度控制中心和区域调度控制中心，完成对城市高中压燃气管网各重要站场、远控截断阀室的监控，同时完成对中压管网监测点的监视，实现管网运行优化、制定输送计划、计量管理等一系列任务。

站控系统：根据管网站场分布，在门站、输配站、调压站、压力监测点等设置不同规模的站控系统。站控系统是 SCADA 系统的远程监控站，它们执行主调度控制中心指令，实现站内数据采集及处理、联锁保护、连续控制及对工艺设备运行状态的监视，并向主调度控制中心上传所采集的各种数据与信息。

4.3.2.2 安全防护方案

4.3.2.2.1 边界安全防护方案

在每个站控系统 PLC/RTU 和工业交换机之间部署工业安全网关，防止恶意流量或攻击通过门站直接进入现场站。

在 SCADA 服务器，工程师站，操作员站的网络前段部署工业防火墙，将所有流向服务器的数据进行深度解析，保护该服务器免受异常操作、非法指令恶意控制、病毒攻击等行为干扰和破坏。

4.3.2.2.2 综合安全防护方案

- 安全区域划分。对整个燃气网络系统进行安全区域划分，实现对业务系统区、访问用户、互联网出口、核心交换区之间的相互访问进行权限控制，同时 SCADA 工控系统区域也进行划分。通过安全区域划分为提升整个安全防护水准提供基础。
- 提升网络安全防护可靠性。对核心交换区、移动用户接入区、敏感数据接入区关键节点设备进行冗余架构设计，实现双机热备，保证整个安全防护体系设备的高可靠性。
- 部署数据库审计系统，数据访问职责划分清晰。通过在敏感数据区部署数据库审计系统，能够实时审计用户对数据库的操作，包括建立表格、删除、修改等行为。
- 数据保护得到加强。部署数据防泄密系统，保证单位保密数据在生产、传输、存储等环节不会被泄密，即使数据被拷贝走，也无法打开。
- 部署安全统一管理区。整个网络系统各个安全防护措施部署后，需要进行有效的管理与运维。通过部署威胁分析系统、漏洞扫描系统、堡垒机等设备，有效完成安全的统一管理；在 SCADA 中心区域部署工控漏洞扫描系统、工控安全审计、工控入侵检测系统等设备来进行整个 SCADA 工控系统的安全管理。

4.4 石油石化行业工控典型安全解决方案

4.4.1 油气采集工控系统安全解决方案

4.4.1.1 总体概述

- **系统简介**

油田开采属野外作业，流动性强，点多、分散、距离长。在油田开采过程中由于管理需要，油气管理中心与集输控制中心、气体处理厂控制中心、管道首站、现场控制层通过工业网络进行连接，所以系统都需要通过大量有线网络和无线网络进行数据传输和远程系统管理。

- **油气田分公司整体网络情况**

油气田分公司生产网核心网络一般通过自建光缆连接不同区域的二级单位。从网络冗余连接方面，各二级单位部署两台路由器作为备份，同时每台路由器分别连接 GMC 和 BGMC 的一台核心。全网运行 OSPF 协议。因此，整个生产网组成了一张高冗余的可靠架构。

从网络链路分析，油气田分公司 GMC 和 BGMC 通过石油专线连接不同区域的二级单位，核心路由器通过卫星方式作为各二级单位的备份链路。当前，有部分位置偏远无法建设有线的中心站或场站采用了卫星、无线网桥、3G/4G 等方式进行数据传输。

4.4.1.2 工控网络安全防护方案

4.4.1.2.1 边界安全防护方案

在保证系统可用性前提下，需要对生产网工业控制系统进行防护，实现“垂直分层，水平分区”。

- **安全域划分**

“垂直分层、水平分区”即对工业控制系统垂直方向化分为四层：现场设备层、现场控制层、监督控制层、生产管理层。水平分区指各工业控制系统之间应该从网络上隔离开，处于不同的安全区。

- **垂直分层**

按照工业控制系统信息安全防护思路，每一个工业控制系统应单独划分在一个区域里，具体划分如下：

1. 分公司办公网和分公司生产网各是一个独立的安全域，这两个安全域之间通过安全隔离网闸实现安全隔离；
2. 在分公司生产网安全域内又划分为分公司 GMC 安全域、输气处 DCC 安全域（分公司 BGMC 安全域）、A 区域 DCC 安全域、B 区域 DCC 安全域、C 区域 DCC 安全域、D 区域 DCC 安全域、E 区域 DCC 安全域；

3. 以如上安全域划分方式，将分公司生产网按照行政层级进行纵向安全域划分。

- **水平分区**

分公司从行政级别上分为五层，每一层又包含多个单位，在水平分区的时候，考虑同级单位的水平划分。在二级单位，按照五矿一处一厂划分为七个水平区域。在水文所级，按照每个水文所进行分区隔离。

按照基于安全域的信息安全防护思路，在同一层级将工业控制系统分为五个域，即数据服务器域、安全支撑域、核心交换域、用户接入域、分支接入域。水文所及以下单位部分安全域根据实际情况取舍。

数据服务器域主要是规划部署该层和工业控制生产相关的服务器，主要威胁来自于：内部人员越权和滥用、内部人员操作失误、软硬件故障、内部人员篡改数据、内部人员抵赖行为；主要防护手段包括：应用和业务开发维护安全、基于应用的审计、身份认证与行为审计；辅助防护手段包括：异常检测、访问控制。

安全支撑域主要是规划部署该层和工业控制生产相关的安全运维、安全检测、安全管理等设备，主要威胁来自于：网络传输泄密、非授权访问和滥用、内部人员抵赖；防护手段包括：带外管理和网络加密、身份认证和访问控制、审计和检测。

核心交换域主要是规划部署该层和工业控制生产相关的核心交换设备，主要威胁来自于：网络设备故障、网络泄密、物理环境威胁；防护手段包括：基础网络的可用性（备份、冗余）、基础网络的保密性（网络传输加密）、基础网络的完整性（基于网络的认证）。

用户接入域主要是规划部署该层和工业控制生产相关的用户终端，主要威胁来自于：内部人员的恶意行为、内部信息泄露；主要防护手段包括：终端行为管控、访问控制。

分支接入域主要是规划部署该层和工业控制生产相关的外联设备，主要威胁来自于：黑客攻击（外部入侵）、恶意代码（病毒蠕虫）、越权访问（非授权接入）；防护手段包括访问控制（工业防火墙）、入侵检测（IDS）、恶意代码防护（防病毒）。

4.4.1.2.2 边界安全防护

分公司的工业网络需要提供纵深防御的安全策略。其中边界安全防护是整个防护环节最重要的一环，既可保证各网络之间的访问得到严格控制，也可截断各类病毒、恶意代码的传输路径，使得各层级边界安全得到保障。

在分公司、输气处、二级单位，二级单位与水文所之间部署工业防火墙。通过部署适用于工业环境的专用防火墙，并配置针对工业协议的访问控制策略，同时梳理网络中原有的传统防火墙的安全策略，提升包过滤策略的粒度，将工业安全协议防护手段和传统安全策略相结合，并按照安全级别，进行整体安全区域划分，从而提升边界、区域到终端的防护能力，有效的降低网络被入侵及安全威胁迁移扩散的风险。

在整体网络业务结构方面，通过在核心网络设备上配置 ACL 访问控制列表，建立点对点、点对多、多对点的业务访问关系，强制规范业务数据流路径，从而强化业务流程管理，降低业务数据流路径上的安全风险。

4.4.1.2.3 综合安全防护方案

- **安全审计**

  - **现有设备加固**

开启设备自带系统日志、安全日志记录，实现对设备运行状况、网络流量、用户行为、事件日期、用户、事件类型等信息的记录，便于管理员充分了解设备运行状态及实现安全事件的可查、可追溯。

  - **运维人员审计（工控运维堡垒机）**

分公司及下属单位目前具备一部分运维管理相关的制度，但单纯从制度上并不能完全杜绝其中的风险，一小部分的原因是制度的落实程度不够，大部分的原因是由于各类场站值守人员大多为自动化相关专业的人员，对信息安全、数据库和相关软件知识了解不够，没有能力审计运维人员的操作，此外，在传统安全和工控安全的案例中，有相当数量的安全事件是由于运维人员或内部人员非法操作导致，故需要专业的、基于工业环境的运维审计设备进行审计。

在分公司水文所、中心站部署移动运维审计系统，用于工业控制系统中的 PLC、DCS、工业交换机、HMI、操作员站、工程师站以及历史数据库、实时数据库等设备的现场维护。

- **入侵检测**

从功能要求出发，应在网络边界处监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、IP 碎片攻击能行为，并在遇到攻击行为时，记录攻击源 IP、攻击类型，在发生严重入侵时提供报警及在线阻断。

工业控制系统采用的控制协议与传统的网络应用协议不同，往往采用专有协议。基于传统网络七层

协议进行检测的入侵检测系统不能有效完成工业控制系统的安全检测。对于工控系统，需要专有的工控协议进行解读，形成特有的工控网络检测策略，实现对各工业控制网络系统的有效入侵检测。在分公司、二级单位、水文所、站场核心网络上部署工控异常检测系统，同时通过全面的适应工业控制网络的特征库和高效的特征库匹配算法对恶意代码及病毒进行有效检测。

- **安全管理**

  - **工业控制漏洞挖掘系统**

为了有效发现、排查工业控制系统的安全隐患，需要部署工控系统漏洞扫描系统检测工业控制系统中潜在的安全缺陷或漏洞。系统基于工控系统已知的安全漏洞特征（如 SCADA/HMI 软件漏洞，PLC、DCS 控制器嵌入式软件漏洞，Modbus、Profibus 等主流现场总线漏洞、SCADA/HMI 软件漏洞等），对 SCADA、DCS、PLC 等工业控制系统中的控制设备、操作站、工程师站、服务器、数据库、中间件等多种系统进行扫描、识别，为工业控制系统提供完善的漏洞分析检测能力。

针对工控系统未知漏洞，采用基于 Fuzzing 漏洞挖掘技术通过向 SCADA/HMI 软件、DCS 系统、PLC 控制器发送预先精心设计的带有攻击性的测试数据、监视返回的结果是否异常发现被测对象的安全漏洞。

5

工控信息安全发展展望

工控信息安全发展展望

伴随着国家各个部委的政策指引，国家相关资金的支持以及各个控制系统运营企业对工控安全重视程度的提升，工控信息安全必然会迎来一个比较好的发展时期。伴随着工业部一网一库三平台的推进以及信息安全等级保护 2.0 的出台以及关键基础设施安全保护条例的出台，工业安全的发展会迎来一个比较大的发展契机。

工业企业在开展工控安全方面目前经历了三个阶段：

1. 以合规及安全事件带动的安全评估阶段；
2. 以寻求解决问题途径和方法的试点建设和经验总结阶段；
3. 以成熟模式推广的规模化应用阶段；

从目前的阶段看，监管的要求进一步加强，在各个行业中工业安全的应用已经开始了由点状的试点、示范应用向规模化推广。在一些行业中如电力行业尤其是发电行业、轨道交通行业中已经出现了区域级的规模化部署和应用。从整个工控安全的发展角度看，大规模部署和应用仍然需要一个时间周期，以试点带动安全逐步的落地是目前工控安全的一个大的趋势。

工控安全目前的核心技术还没有得到有效解决，技术的发展进入一定的瓶颈期，产品目前趋同的情况比较严重。由于技术上存在瓶颈，使得产品功能差异较小，导致厂商在狭小的空间中激烈竞争，整体市场收益较少。工控安全技术方向仍然需要新一轮的创新，工控安全在考虑引入 IT 信息安全的技术手段或者是构建在工控安全自身特性的技术上时，都需要与工控系统自身的运行特点相互匹配，需要考虑好 IT+OT 统一的安全技术手段如何有效的融入到工控安全能力中。要考虑安全技术在工业业务增效中起到的作用。技术应用上要考虑轻量化、无扰动、业务数据的采集与安全数据采集之间的关联，需要考虑各个行业领域应用的差异性，共性技术的提取与特异性技术的应用等。

另一个很重要的参与者控制器厂商对工控安全的重视程度也进一步提升，他们在自己的控制系统中加入相关的安全属性，实现“内生的安全功能”，同时也会加大与业界的安全企业合作，来联合推广适配于自身业务特点和属性的安全解决方案。

在安全能力的构建上，与业务自身管理平台相融合，实现安全与业务数据的采集融合，平台级数据交换与共享，综合性的业务故障联合诊断分析会成为未来工控安全的一个发展趋势。在构建过程中需要安全数据、业务数据的翻译与解析，形成有效的“通话机制”。安全数据内容与业务数据内容之间的桥梁和通道需要逐步打通，逐步实现业务通道给安全提供有效数据，安全为业务保证提供有效支撑的一体

化的业务保证能力。

同时，我们看到在工业信息化改造及广泛互联的大趋势下，由于互联互通的便捷性及成本优势，原有工业系统的封闭模式会逐步被打破，新业务应用形态会带来新的安全风险，如云端的安全风险、边缘侧安全风险及厂级的安全风险等。从未来角度看，工业信息安全必将是一个综合性的安全，涵盖了云安全、边界安全、控制安全、数据安全等领域，安全的价值也需要体现在对业务的实质性促进作用上，这也符合工业领域的属性和特点。

6. 附录 缩略语中英文对照

缩略语	英文全称	中文全称
AGC	Automatic Generation Control	自动发电控制
APT	Advanced Persistent Threat	高级持续性威胁
AVC	Automatic Voltage Control	自动电压控制
CPS	Cyber Physical System	信息物理系统
DCS	Distributed Control System	分布式控制系统
DOS	Denial of Service	拒绝服务
DPU	Distributed Processing Unit	分散处理单元
ERP	Enterprise Resource Planning	企业资源计划
FCS	Fieldbus Control System	现场总线控制系统
GE	General Electric Company	通用电气公司
HMI	Human Machine Interface	人机界面
ICS	Industrial control system	工业控制系统
IDS	Intrusion Detection System	入侵检测系统
IEC	International Electrotechnical Commission	国际电工委员会
MES	Manufacturing Execution System	制造执行系统
OMS	Order Management System	订单管理系统
PCS	Process Control System	过程控制系统
PLC	Programmable Logic Controller	可编程逻辑控制器
RTU	Remote Terminal Unit	远程终端单元
SCADA	Supervisory Control And Data Acquisition	监控和数据采集
SIS	Safety Instrumented System	安全仪表系统

7. 参考文献

[1] https://me-en.kaspersky.com/about/press-releases/2016_91-1--of-vulnerable-industrial-control-systems-likely-belonging-to-large-organizations

[2] https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523849948

[3] https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/

[4] https://ics-cert.us-cert.gov/advisories

[5] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

[6] ICS-CERT Annual Vulnerability Coordination Report，https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

[7] https://www.fireeye.com/blog/threat-research/2018/10/ics-tactical-security-trends-analysis-of-security-risks-observed-in-field.html

8. 作者信息

王晓鹏：绿盟科技工控安全产品总监，自动化学会信息安全专委会委员，工控安全产业联盟理事，工控安全国家工程实验室技术专家。曾参与了多个工控安全国家标准的制定，是多个工控安全国家项目的绿盟科技负责人。

吴子建：绿盟科技担任安全研究员，博士毕业于清华大学自动化系，博士期间主要做优化与系统工程方面的研究。主要研究领域为基于大数据和机器学习的网络安全，业务安全，工业系统信息安全等工作。

潘雨晨：绿盟科技格物实验室研究员，负责应急响应运营，虚拟化安全方向研究。

马　良：绿盟科技格物实验室研究员，擅长 : 嵌入式软硬件和各种搞硬件设备的手段。在进入安全行业前 , 曾有十年丰富的嵌入式开发经历目前研究领域为物联网和工控安全。曾参加 XPWN 和 GeekPWN 等黑客比赛并夺得大奖。在 2018 年的 GeekPWN 国际机器特工比赛中 , 他制作的机器人获得了国际第 2 名 , 国内第一的好成绩。

王旭辰：工控安全产品经理，主要从事工控系统评估工具和网络边界防护产品的管理工作。

THE EXPERT
BEHIND GIANTS
巨人背后的安全专家

多年以来，绿盟科技致力于安全攻防的研究，
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。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com

绿盟科技官方微信