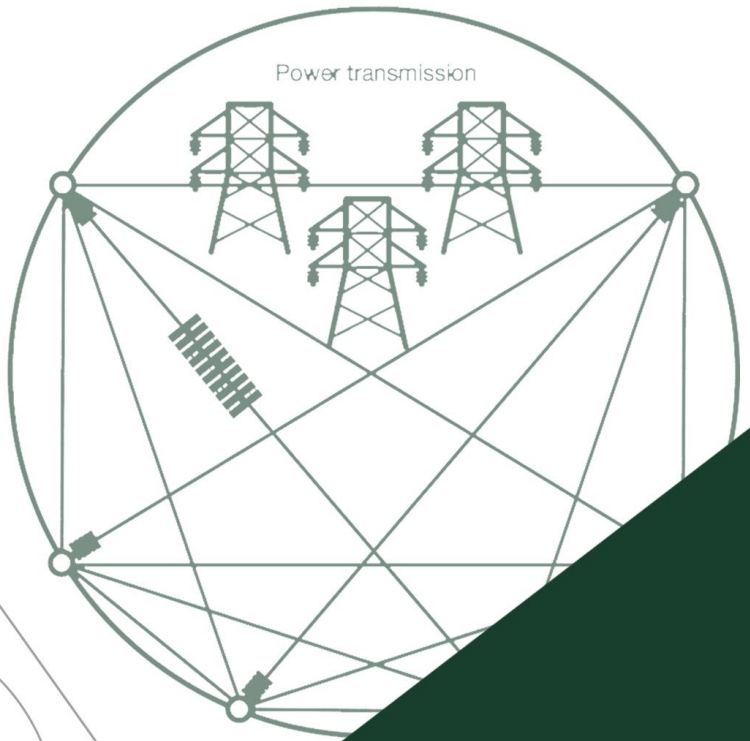
SECURITY NSFOCUS

NSFOCUS

2014 ICS SECURITY REPORT

2014 绿盟科技工控系统安全态势报告



NSFOCUS ICS SECURITY REPORT

2014 年 8 月

本报告分析了工控系统自身的脆弱性以及所面临的安全威胁发展态势，着重对工控安全产业生态环境进行了调研。

基于这些研究成果可以看到，在每个垂直领域里面，都需要工控系统厂商、信息安全厂商、科研院所以及工控系统的用户群体的深度合作，通过构建产业联盟形成利益共同体，并集成各成员单位的产品与技术优势，通过合理分工协作，形成联盟层面的安全解决方案。报告还对典型工控行业进行了安全服务推广策略的讨论，包括培训、试点、评估、建设等。

本报告可以帮助读者了解工控系统安全领域的总体发展态势，并可作为工控安全领域的主管部门、工控系统用户以及工控安全服务商在决定下一步工控安全投入时的决策参考。

分析数据分析显示近 4 年来：

- **工控漏洞快速增长** 工控系统公开漏洞数达到 549 个，2011 年之后持续保持快速增长的势头。显然这对业务连续性、实时性要求高的工业控制系统来说，造成了极大的安全威胁。
- **能源行业易受攻击** ICS-CERT 公布数据中，工控安全事件达 632 件，而且多集中能源行业（59%）和关键制造业（20%）。工控安全事件呈快速增长的趋势。
- **国家支持的黑客攻击** 2014 年 6 月，“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。这次事件表明，黑客组织（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最大安全威胁。

SECURITY

研究目标与方法

安全事件分析

分析工业控制系统自身的脆弱性及所面临的安全攻击威胁及近期安全事件。

生态环境模型

根据 2014 年初《2014 工业控制系统的安全研究与实践》[LHW2014]中提出的生态环境模型，进行展开论述。

工控行业调研

本文调查了各方当前在政策发布、技术研究、安全建设需求、产品及服务开发等多方面的进展态势；并深入研究了发电、电网等几个典型行业工控系统的安全现状、存在的问题及市场需求。

历次报告积累

第一次报告，工控安全是什么

第二次报告，工控安全存在哪些问题

第三次报告，工控安全行业需求及发展态势

第四次报告，工控安全产品及解决方案

第五次报告，……

工控安全产业生态环境模型

工业控制系统安全与传统的信息安全不同，它通常关注更多的是物理安全与功能安全，而且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战威胁的影响，工业控制系统也将从传统的仅关注物理安全、功能安全转向更为关注信息系统安全；这种转变将在国家政策的推动下对传统的工业企业产生较大的影响。确保国计民生相关的工业控制系统安全已被提升到了国家安全战略的高度，再加上工业控制系统跨学科、跨行业应用的特殊性；使其安全保障体系的建立必须在国家、行业监管部门、工业控制系统企业（用户）、工业控制系统提供商、信息安全厂商等多方面的协同努力下才能够实现。

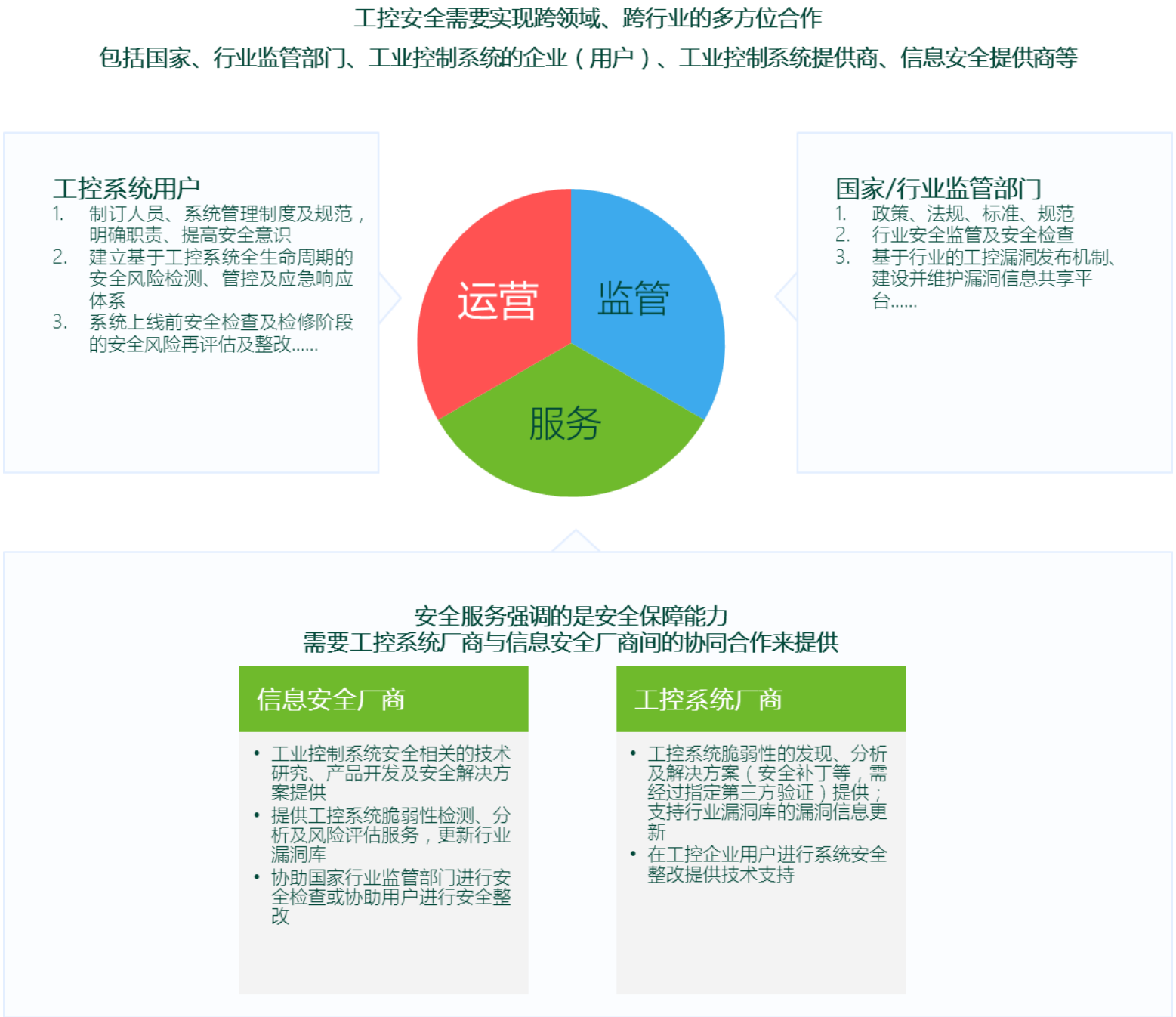


图 1.1　工控安全产业生态环境模型

目录

这里结合目录章节，对报告的主要内容提要如下：

P2 工控系统的安全威胁态势分析

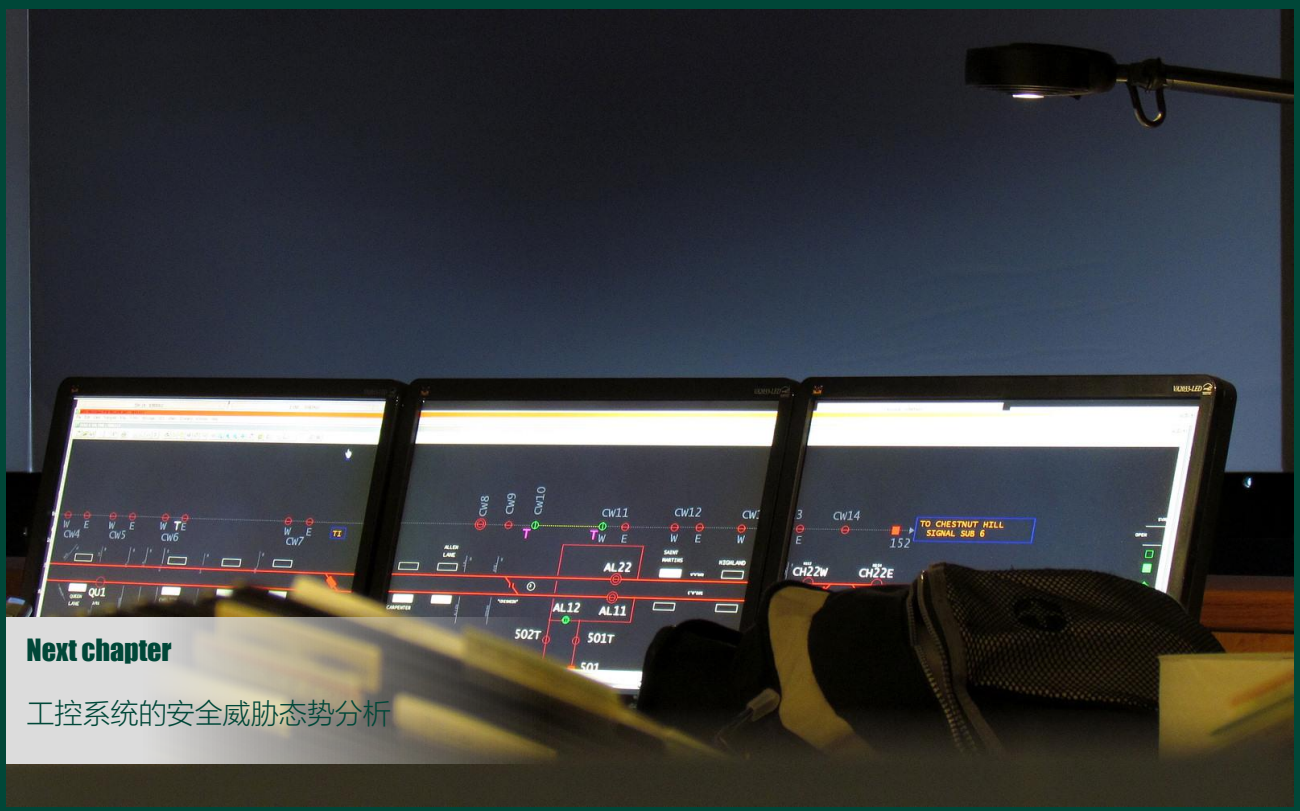
主要从近期公开的工控系统相关漏洞的统计分析结果以及对近期典型的工控安全攻击事件及新型攻击技术的分析，讨论工控系统当前所面临的安全威胁态势。

P13 工控安全领域的总体发展态势分析

依据工控安全产业生态模型相关的政府主管部门、产业联盟、科研院所及国内外友商的研究及产品服务发展动态情况，讨论工控安全领域的总体发展态势。

P19 典型行业的工控安全发展态势分析

针对上半年重点调研的发电、电网等几个典型工控行业的结果，从行业政策动态，行业工控系统的安全现状、问题与需求，当前制约该行业工控安全建设发展的主要因素等多个角度来讨论各行业的工控安全发展态势；并在此基础上提出我们针对该行业的工控安全服务的推广策略。



Next chapter

工控系统的安全威胁态势分析

工控系统的安全威胁态势分析

本章将从工业控制系统公开安全漏洞的统计分析以及对近期典型的工控安全攻击事件及新型攻击技术的分析等多个方面，讨论工控系统当前所面临的安全威胁态势。

工控系统的自身脆弱性

截至 2014 年 6 月，我们以绿盟科技安全漏洞库收录的工业控制系统相关的漏洞信息为基础，综合参考了美国 CVE[CVE]、ICS-CERT 以及中国国家信息安全漏洞共享平台 所发布的漏洞信息[CNVD] [ICSMM2014]，共整理出了 549 个与工业控制系统相关的漏洞。本节将重点分析 2014 年新增漏洞的统计特征和变化趋势，主要涉及公开漏洞的总体变化趋势、漏洞的严重程度、漏洞所影响的工控系统类型、漏洞的危害等几个方面的对比分析。

公开漏洞数总体上保持快速增长的变化趋势

下图给出了截止到 2014 年 6 月之前所公开发布的工业控制系统相关漏洞按年度进行统计分析的结果。

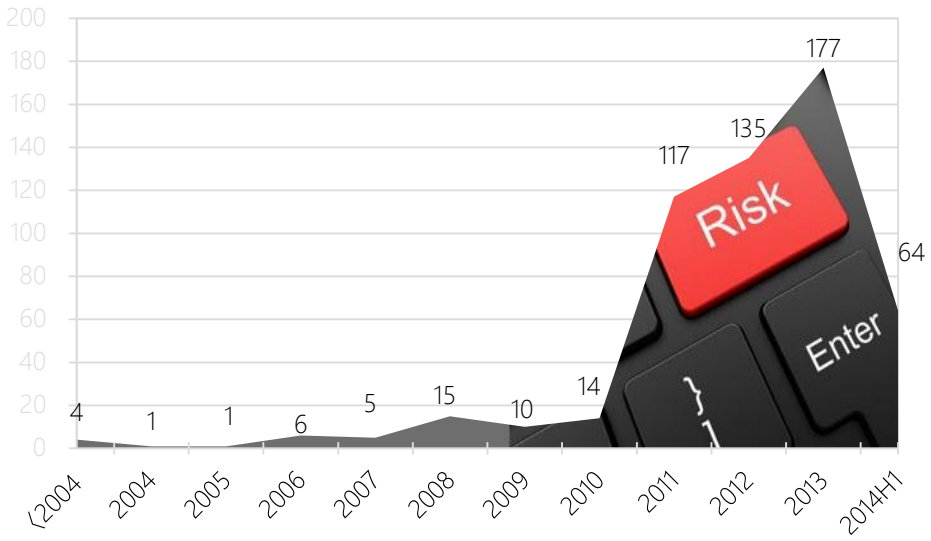


图 1.2　公开的 ICS 漏洞的年度变化趋势

在 2011 年之前，公开披露的工业控制系统相关漏洞数量相当少，但在 2011 年出现快速增长，这可能是因为 2010 年的 Stuxnet 蠕虫事件之后，人们对工业控制系统安全问题持续关注以及工业控制系统厂商分析解决历史遗留安全问题所造成的。随着各方面对工业控制系统的安全日益重视，工业控制系统的相关公开漏洞数量仍将保持一个快速增长的总体趋势。

公开漏洞涉及的工控系统厂商依然以国际厂商为主

通过对漏洞的统计分析，下图给出了公开漏洞所涉及的主要工业控制系统厂商，以及及各厂商的相关漏洞数及其占漏洞库中所有漏洞的比例情况。

分析结果表明，公开漏洞所涉及的工业控制系统厂商仍然是以国际著名的工业控制系统厂商为主，西门子（Siemens）、施耐德电气（Schneider）、研华科技（Advantech）、通用电气（GE）与罗克韦尔（Rockwell）占据漏洞数排行榜的前五名。用户的工控系统使用情况调研结果表明，这些国际著名工控系统厂商的产品在国内市场上占据优势地位，甚至某些产品在某些行业处于明显的垄断地位。这种情况必然会造成这些厂商的产品倍受系统攻防双方的重视和关注，而且也比较容易获得研究分析用户的产品，这很可能就是公开漏洞涉及到的工控系统厂商总是以国际厂商为主的主要原因。

这里需要说明的是，虽然漏洞涉及的是系统自身的脆弱性问题，但依然不能简单地通过这里的漏洞数量信息实现厂商之间产品安全性的横向对比（因为各厂商产品的漏洞数量不仅与产品自身的安全性有关，而且也和厂商的产品数量、产品的复杂度、受研究者关注程度以及工业控制系统厂商对自身系统安全性的自检力度等多种因素有关。因此，我们并不能简单地认为公开漏洞数量越多的厂商产品越不安全。），但是却可以

通过该信息评估用户工控系统所存在的安全脆弱性状况，并据此进行系统的安全加固、调整安全防护策略，来增强用户系统的整体安全防护能力。

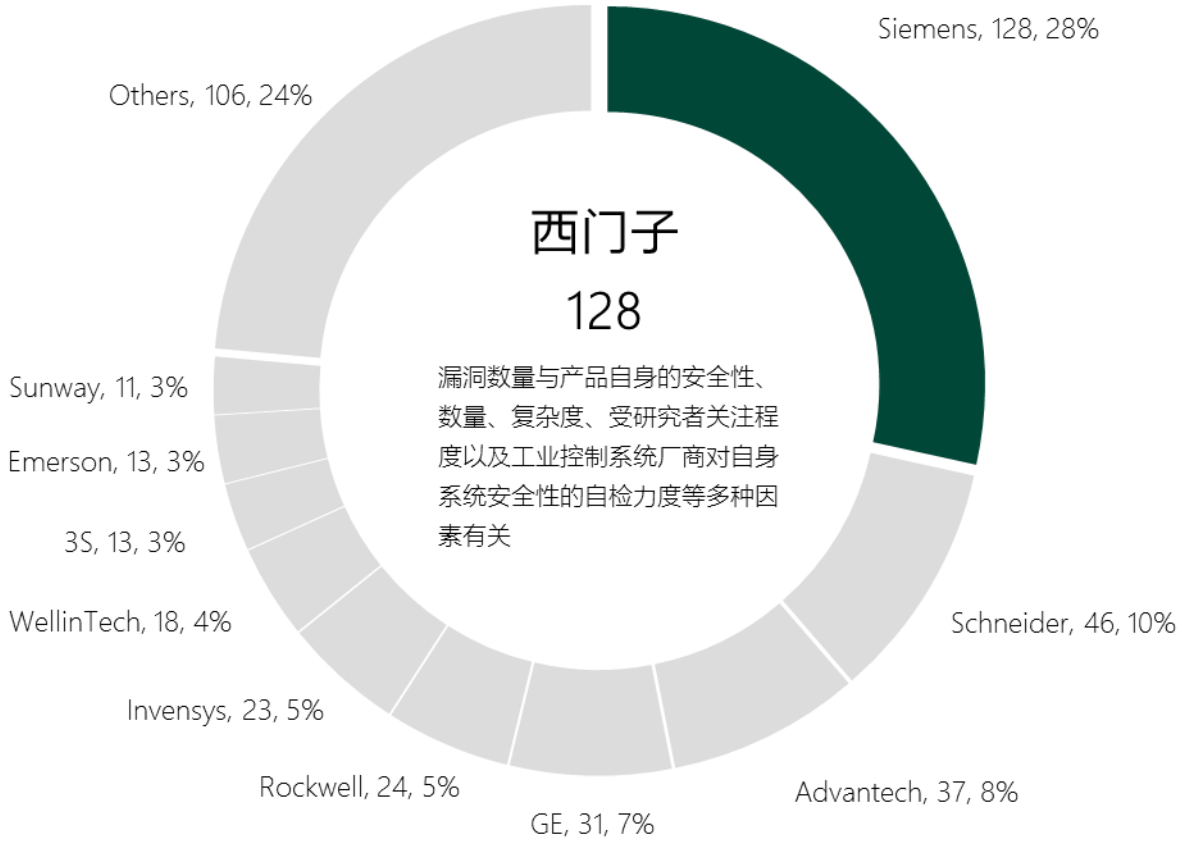


图 1.3　公开漏洞所涉及到的主要工业控制系统厂商（Top10）

图 1.4 给出了 2014 年上半年新增漏洞所涉及的工控厂商情况，与图 1.3 的总体情况相比有所变化。其中西门子以新增 25 个公开漏洞，占比 39%依然位居首位，研华科技则以新增 10 个公开漏洞，占比 15.4%而升据第二。施耐德电气则以半年新增 4 个漏洞（占比 6%）依然位列三甲之内。但需要注意的是：

1） 日本横河电机株式会社(YOKOGAWA)首次进入我们的关注视野，就以半年新增 4 个漏洞，与施耐德电气并列 2014 半年度新增漏洞的第三名。日本横河电机作为工业控制行业全球最为专业的跨国公司之一，经营领域涉及测量、控制、信息三大领域，其集散型控制系统（DCS 系统）、PLC 等工控产品在国内石油、化工等大型工厂生产过程也有较为广泛的应用。也应是我们需要重点关注研究的工控厂商之一。

2） 排名第四、第五的 Cogent、Ecava 则是两家专业的工控软件厂商，表明除了著名国际厂商之外，在工控软件某个子领域内相对领先的企业也日益受到关注。

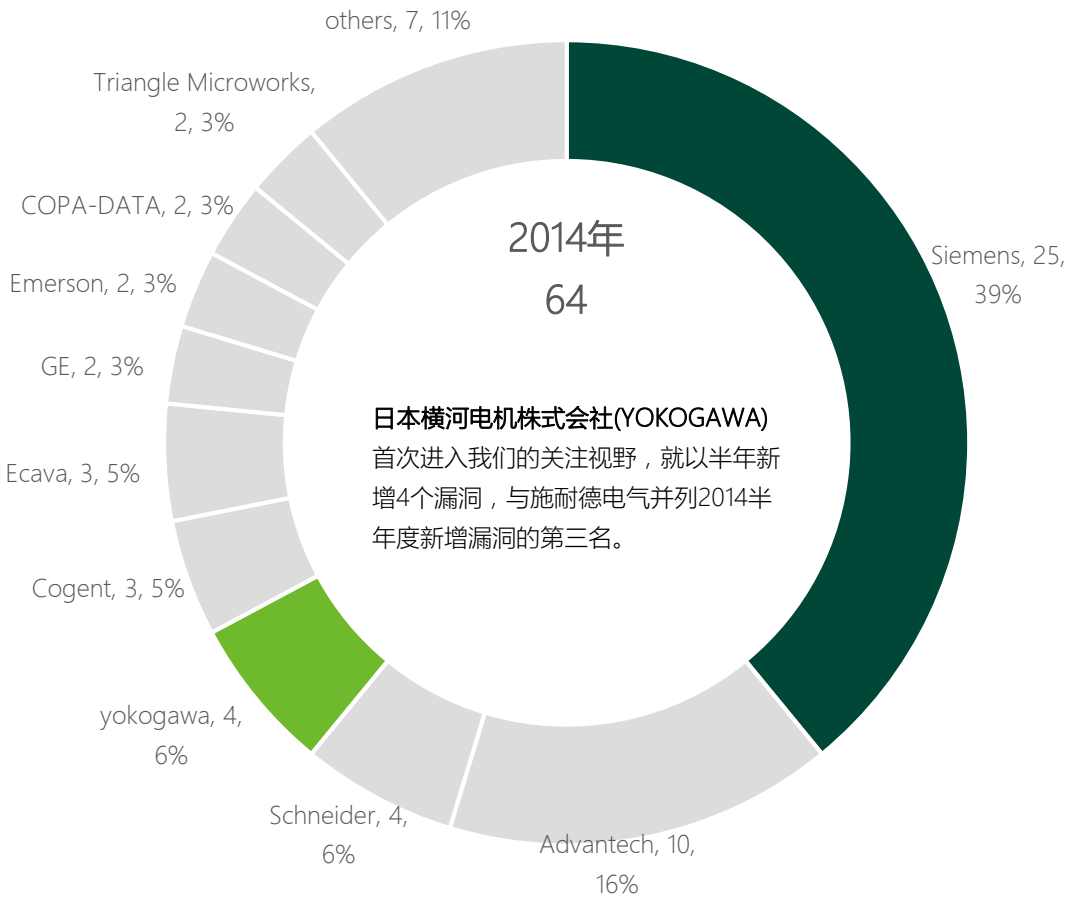


图 1.4 2014 年新增工业控制系统漏洞所涉及到的主要厂商

工控系统相关漏洞的严重性表明：工控系统存在严重的安全隐患及被攻击的威胁

因本文收集处理的公开漏洞以 CVE 收录的为主，所以本文在分析这些漏洞的严重性时，将主要根据 CVE 的 CVSS 评估值来判断，并划分为高、中、低三种情况。

根据下图的统计分析，2014 年的新增漏洞中“高危”漏洞（CVSS 值范围 7.0~10.0）超过一半（51%），且基本上都是严重性程度为“中”以上（CVSS 值大于等于 4.0）的漏洞。这也表明了当前工控系统产品存在严重的安全隐患。

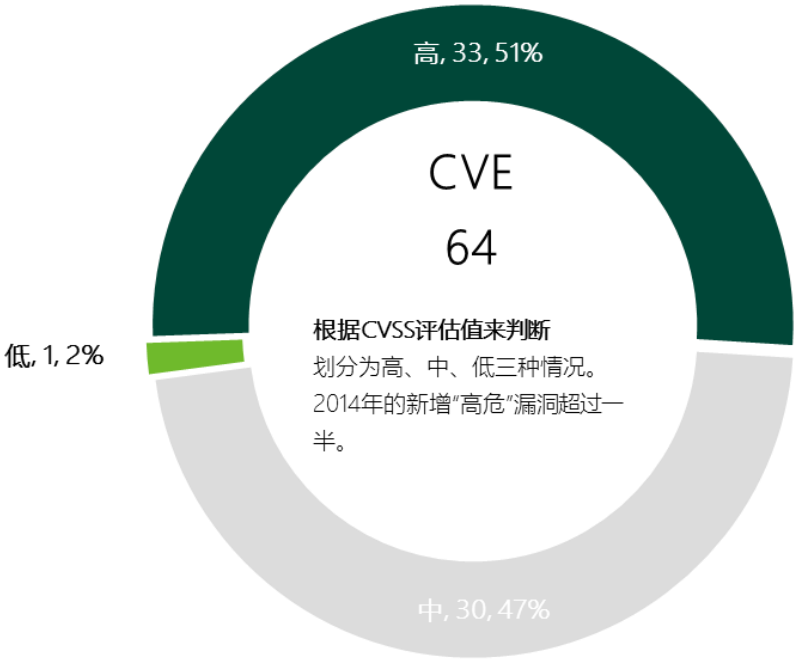


图 1.5　2014 年收录的新增漏洞按严重程度的分类情况

下图则是 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位居前五的威胁情况。从图中可知：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工控系统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%；对于当前具有规范性软件开发流程的软件企业来说，缓冲区溢出类这类软件编程不规范所造成的软件缺陷应是比较罕见的了，这也可以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，利用他们可以窃取制造企业的设计图纸、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、破坏工控系统业务的正常生产或运营活动。

显然这些漏洞所可能造成的主要威胁的分类情况也可以从侧面表明当前工控系统安全所应关注的主要安全问题。

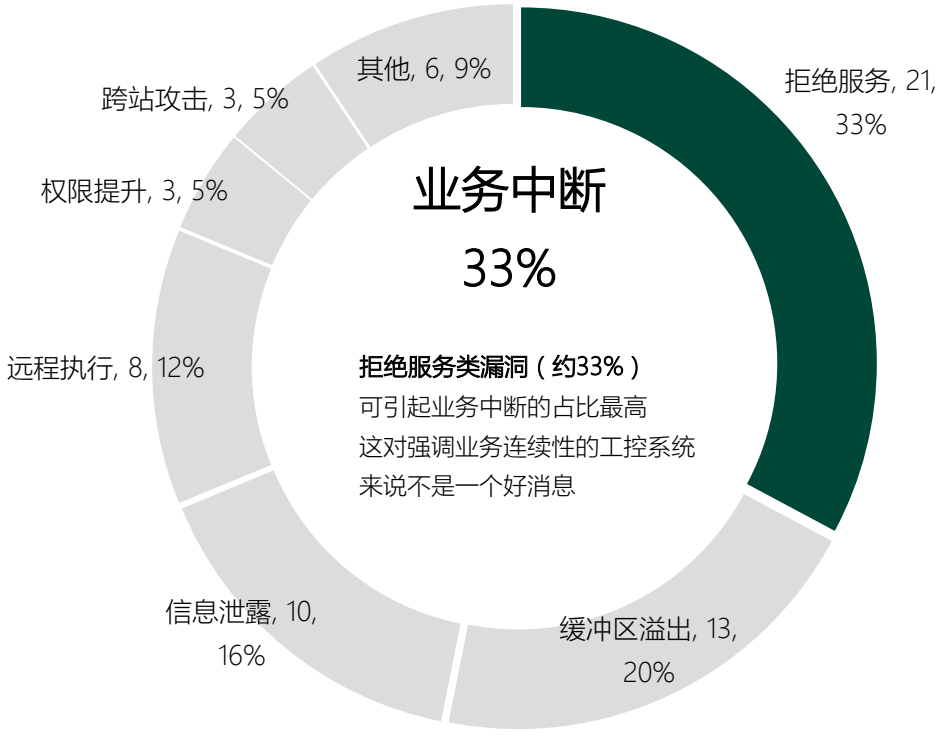


图 1.6　2014 年新增漏洞的威胁分类及占比分析

公开漏洞中以 SCADA/HMI 系统相关的漏洞为主，其占比超过 40%

公开漏洞中以 SCADA/HMI 系统相关的漏洞为主，其占比超过 40%，PLC 相关的漏洞以接近 30%的占比紧随其后。而关于集散控制系统（DCS）以及用于过程控制的 OPC 相关的漏洞也各占将近 10%的份额。这说明工控系统中攻防双方都可能把主要精力放在了工控系统的控制设备或工业控制管理软件系统的安全性分析之上了。当然，在工业控制系统的网络设备（网络交换机）及工业网络管理软件的脆弱性也受到了一定的关注，其相关的公开漏洞也有比较高的占比（合计约有 8%）。

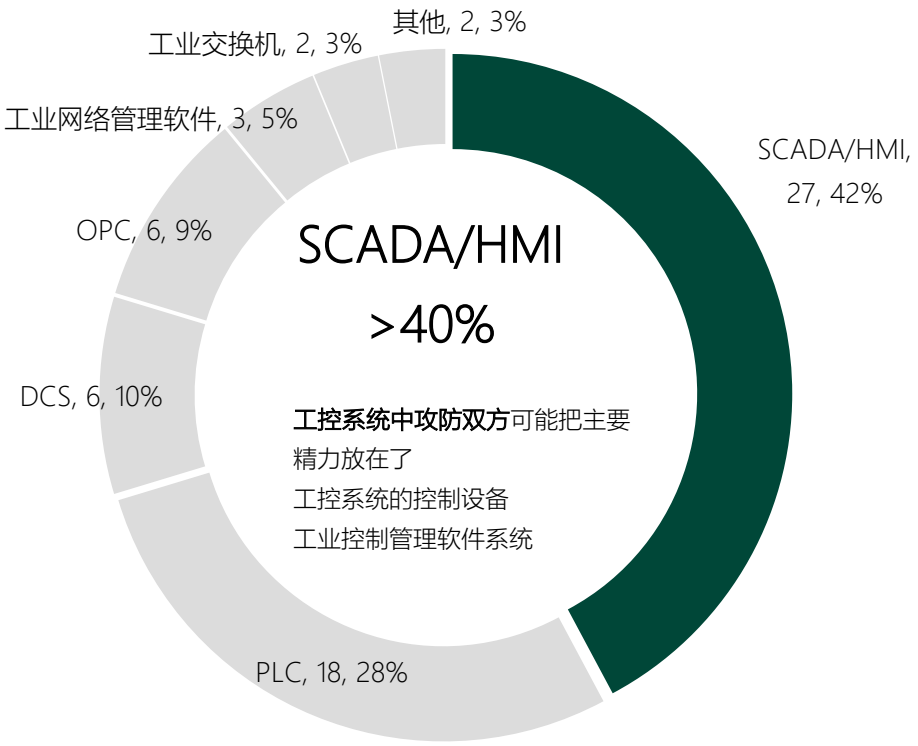


图 1.7　2014 年新增漏洞所涉及的工控产品分类分析

工控系统面临的安全威胁

工控安全事件增长快速，且主要集中在能源行业（59%）与关键制造业（20%）

结合 ICS-CERT 往年的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（如下图所示）。

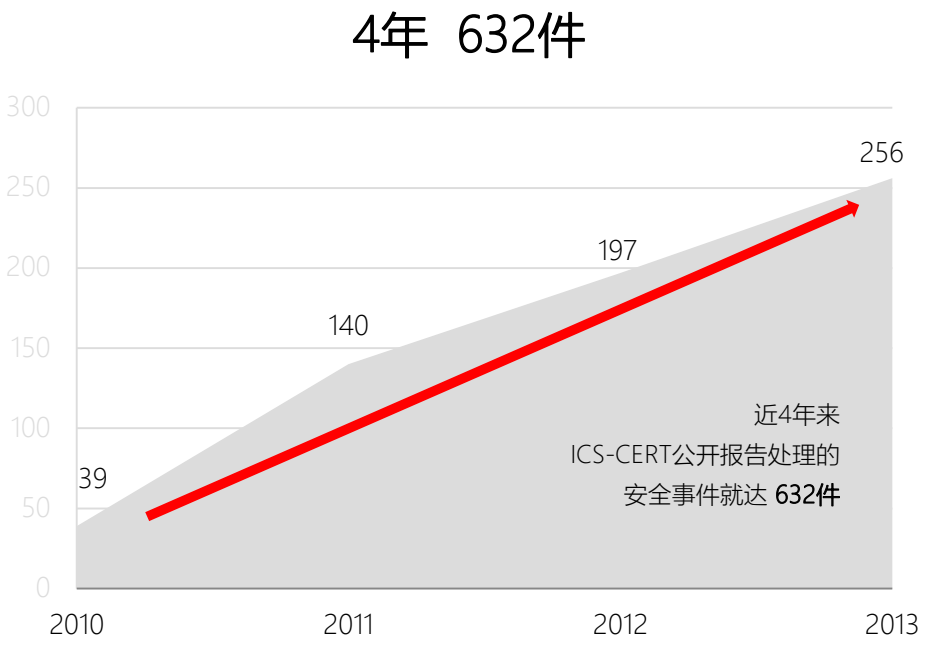


图 1.9 ICS-CERT 历年的公布工控安全事件(按财年[①]统计)统计分析

其中，2013 年度内 ICS-CERT 公开报告处理的安全事件就达 256 件[ICSMM2013]，而这些事件有多分布在能源、关键制造业、市政、交通等涉及国计民生的关键基础行业，如图 1.10 所示。从图中可知能源行业相关的安全事件则高达 151 件，接近所有事件的三分之二。这与以电力为主的能源行业对于现实社会的重要性及其工控系统的自动化程度、信息化程度较高也有相当的关系。图 1.10 关于工控安全事件所涉及的重要行业的分布图，也同时为国家主管部门以及工控系统安全厂商识别行业安全需求及安全建设投入提供相应的决策支持。从我们前期针对多个行业关于工控安全需求的调研工作中，也清晰的了解到以电力行业为主的能源行业相对于其他行业来说，具有较高的安全意识，并已在安全建设的系统安全规划、标准制定、定期的安全检查及整改方面做了不少的工作。而其他行业在工控安全方面则多处于刚刚起步阶段，市场尚待培育开发。

① 这里的财年计算方法是从上一年的 10 月开始至下一年的 9 月结束。

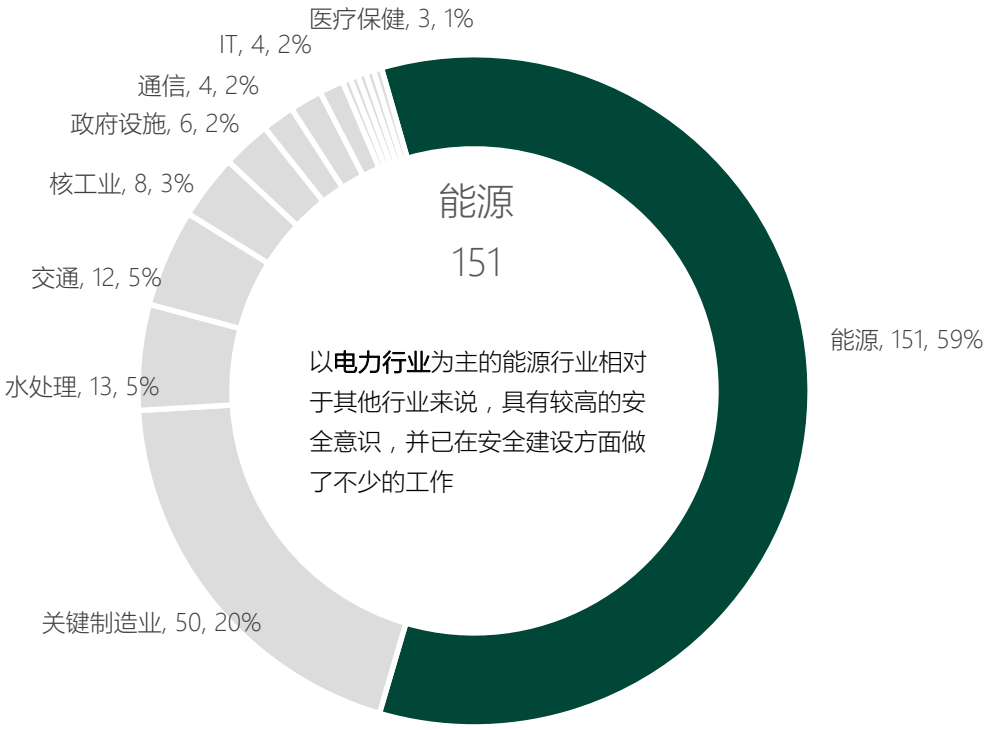


图 1.10　工控安全事件所涉及的重要行业及分布

Havex——2014 年专门针对工控系统的新型攻击

在 2014 年 6 月 25 日 ICS-CERT 发布了题为“ICS Focused Malware”的安全通告 ICS-ALERT-14-176-02[havex]中通报了一种类似震网病毒的专门针对工控系统攻击的恶意代码。安全厂商 F-Secure 首先发现了这种恶意代码并将其作为后门命名为 W32/Havex.A，F-Secure 称它是一种通用的远程访问木马（RAT，即 Remote Access Trojan）。就像著名的专门设计用来破坏伊朗核项目的 Stuxnet 蠕虫病毒一样，Havex 也是被编写来感染 SCADA 和工控系统中使用的工业控制软件，这种木马可能有能力禁用水电大坝、使核电站过载，甚至可以做到按一下键盘就能关闭一个国家的电网。

根据 ICS-CERT、F-secure、Symentec 的研究表明[Havex1~3]：网络攻击者传播 Havex 恶意软件方式有多种，除了利用工具包、钓鱼邮件、垃圾邮件、重定向到受感染的 Web 网站等传统感染方式外，还采用了“水坑式”攻击方式，即通过渗透到目标软件公司的 Web 站点，并等待目标安装那些合法 APP 的感染恶意代码的版本。ICS-CERT 的安全通告称当前至少已发现 3 个著名的工业控制系统提供商的 Web 网站已受到该恶意代码的感染。显然，这些恶意代码的传播技术使得攻击者能够获得工控系统的访问权限，并安装相应的恶意代码（后门程序或木马）。而在安装过程中，该恶意软件会释放一个叫做“mbcheck.dll”的文件，这个文件实际上就是攻击者用作后门的 Havex 恶意代码。

F-Secure 声称他们已收集和分析了 Havex RAT 的 88 个变种，并认为 Havex 及其变种多通过利用 OPC 标准 被用来从目标网络和机器获取权限并搜集大量数据[Havex2]。具体表现为：该类恶意软件会通过扫描本地网络中那些会对 OPC 请求做出响应的设备，来收集工业控制设备的操作系统信息、窃取存储在开发 Web 浏览器的密码、使用自定义协议实现不同 C&C 服务器之间的通信，然后把这些信息反馈到 C&C 服务器上（Havex 的攻击原理如下图所示）。同时 FireEye 公司的研究人员最近也声称发现了一个 Havex 的新变种[Havex3]，同样认为发现的 Havex 变种具备 OPC 服务器的扫描功能，并可以搜集有关联网工控

设备的信息，以发回到 C&C 服务器供攻击者分析使用。这表明，虽然 Havex 及其变种最可能是被用作收集工控系统情报的工具，但攻击者应该不仅仅是对这些目标公司的系统信息感兴趣，而必然会对获取那些目标公司所属的 ICS 或 SCADA 系统的控制权更感兴趣。

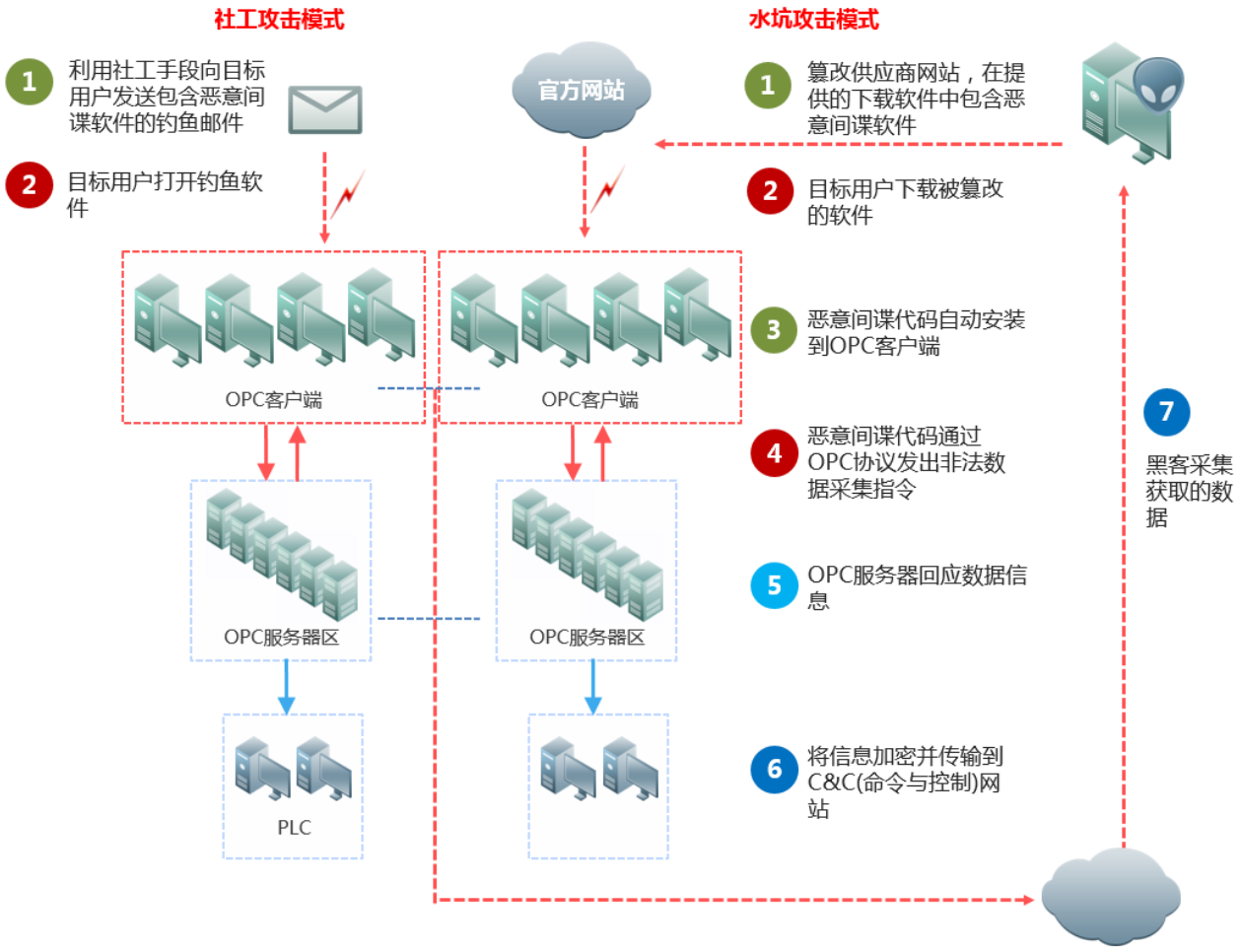


图 1.11　Havex 的攻击原理

最近多家安全公司的研究发现它多被用于从事工业间谍活动，其主要攻击对象是欧洲的许多使用和开发工业应用程序和机械设备的公司。

黑客组织是当前工控系统所面临的最大安全威胁

在 2014 年 1 月，网络安全公司 CrowdStrike[①] 曾披露了一项被称为“Energetic Bear”的网络间谍活动，在这项活动中黑客们可能试图渗透欧洲、美国和亚洲能源公司的计算机网络。据 CrowStrke 称，那些网络攻击中所用的恶意软件就是 Havex RAT 和 SYSMain RAT，该公司怀疑 Havex RAT 有可能以某种方式被俄罗斯黑客连接，或者由俄罗斯政府资助实施。赛门铁克及 F-secure 等多家安全公司在近期发布的研究报告[Dragonfly]或官方博客的博文中[havex2]也发表了类似的信息，声称近期一个称

[①] CrowdStrike 公司是一家专注于 APT 防护的新兴网络安全公司，它倡导“Active Defense”（主动防御）的安全理念，强调聚焦于提高对手的攻击成本，使防御者在战略层面上处于优势地位。其实体产品“Falcon”系统是一个基于大数据的“云服务”，可从部署了 sensors 的网络内实时收集情报以及安全事件，并坚持他们的防御理念“是在合法范围内挫败攻击者”。

为 Energetic Bear 的俄罗斯黑客组织使用一种复杂的网络武器 Havex，已经使 1000 多家欧洲和北美能源公司受损；并认为 Havex 与震网病毒（Stuxnet）相似，能使黑客们访问到能源部门的控制系统。

根据赛门铁克的研究报告[Dragonfly]称，黑客组织 Energetic Bear 也被称为“蜻蜓 Dragonfly”，这是一个至少自 2011 年起便开始活跃的东欧黑客团体。蜻蜓组织最初的攻击目标是美国和加拿大的国防和航空企业，但从 2013 年开始，蜻蜓组织的主要目标转向许多国家的石油管道运营商、发电企业和其他能源工控设备提供商，即以那些使用工控系统来管理电、水、油、气和数据系统的机构为新的攻击目标。赛门铁克专门针对“蜻蜓组织”的近期活动进行了跟踪分析与研究[Dragonfly]（如图 1.12 所示），研究认为：自 2013 年初开始，“蜻蜓组织”为达到通过远程控制木马（RAT）访问工控系统的目的，一直在使用不同的技术手段对美国和其他一些欧洲国家的能源供应商实施攻击并利用特殊编制的恶意代码感染其工业软件，这些手段包括在电子邮件、网站和第三方程序中捆绑恶意软件以及“水坑攻击”技术。并在 18 个月的时间里影响了几乎 84 个国家，但是大多数受害者机构都位于美国、西班牙、法国、意大利、德国、土耳其和波兰等国家（如图 1.13 所示）。显然，“蜻蜓组织”所使用恶意代码的破坏能力可能会造成多个欧洲国家的能源供应中断，具有极大的社会危害性。

赛门铁克、F-secure、CrowdStrike 等多家安全公司在研究后，有一个基本的判定，认为“蜻蜓黑客组织的主要目标是实施间谍活动，而且它似乎是有资源、有规模、有组织的；甚至怀疑在它最近的攻击活动背后有政府的参与”。

自从 2010 年震网病毒、Flame、Duqu 之后，2014 年“蜻蜓组织”相关的可能大规模影响欧洲能源企业 SCADA 系统的安全事件（伴随着最新型的专门针对工控系统的恶意代码 Havex 及其近百的变种的发现）对工业界的影响巨大，这表明随着攻击者对工控系统研究的深入，针对工控系统攻击的恶意代码也将会层出不穷，而且还可能在攻击活动的背后具有国家支持的潜在因素。因而，面对攻击技术与手段日益先进、复杂、成熟的针对工控系统进行攻击的黑客组织，工控系统所面临的安全威胁也将日益严峻。

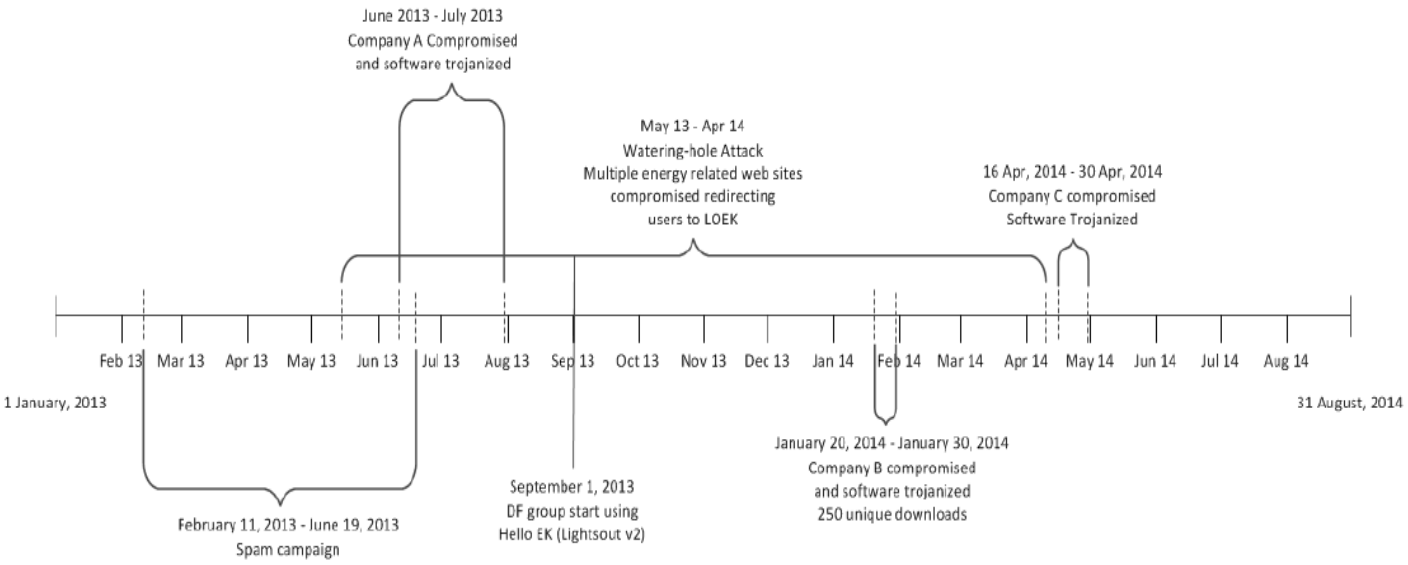


图 1.12　赛门铁克公司关于“蜻蜓组织”近期活动的时序分析[Dragonfly]

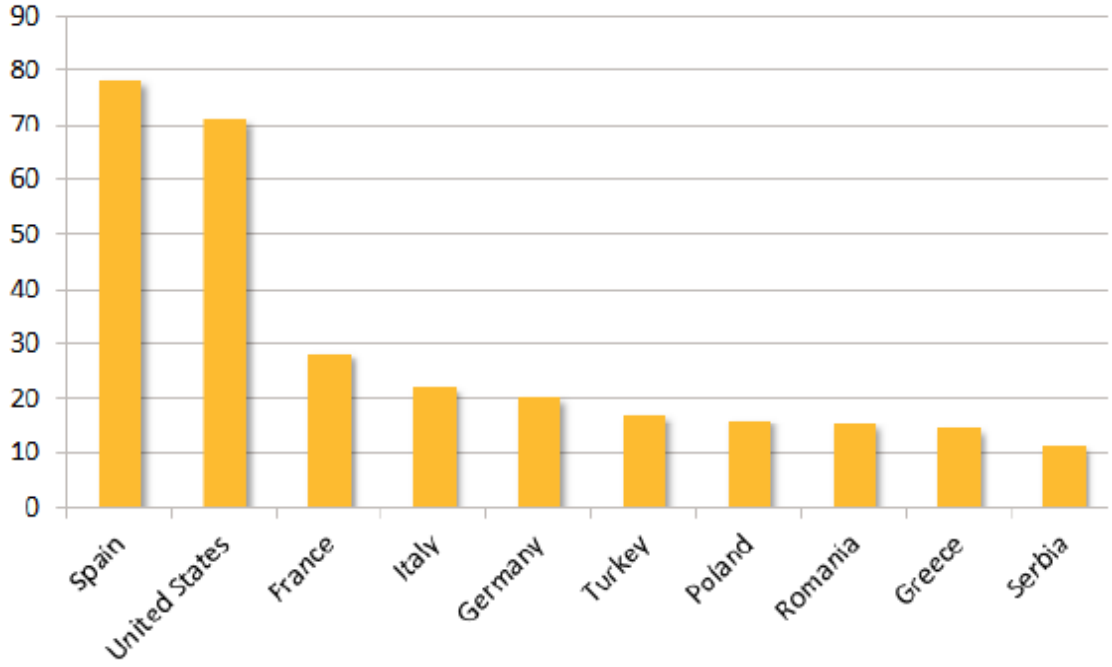


图 1.13　受蜻蜓组织近期攻击活动影响较大的国家（Top Ten）[Dragonfly]

工控安全领域的总体发展态势分析

本章则依据工控安全产业生态模型相关的政府主管部门、产业联盟、科研院所及国内外友商的研究及产品服务发展动态情况，主要讨论国内工控安全领域的总体发展态势，并结合绿盟科技的优势提出在工控领域的发展建议，以及在业内的初步合作建议。

国外发展动态概述

自从 2010 年震网事件之后，世界各国对工控系统的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[LYHC2012]。最近工业控制系统安全更成为备受工业和信息安全领域研究机构关注的研究热点。

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相应小组（ICS-CERT），专注于工业控制系统相关的安全事故监控、分析执行漏洞和恶意代码、为事故响应和取证分析提供现场支持；通过信息产品、安全通告以及漏洞及威胁信息的共享提供工业控制系统安全事件监控及行业安全态势分析，并以季度报告的方式公开发布[ICSCERT1] [ICSCERT2]。而且美国国土安全部（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[DHS2011]，来实施针对工业控制系统产品的脆弱性分析与验证工作。而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，并总体上处于领先的地位。

在欧洲则以德国西门子、法国施耐德电气为代表的工业控制系统提供商为主，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（@CT China），可提供安全咨询服务、培训、漏洞及补丁的发布 www.siemens.com/industrialsecurity 。产品方面则有工控防火墙及相应的工控安全解决方案。而在国内西门子的工作则主要侧重西门子工控系统的漏洞修补，应从属于其工控系统业务 。同样施耐德电气公司在国内也多是配合客户的安全整改工作，修补其产品漏洞并结合其工控安全防火墙为用户提供必要的工控安全解决方案。但是在工控系统领域的许多行业，来自欧洲的西门子、施耐德电气多具有绝对的技术与市场优势，而工控系统的信息化、智能化以及所带来安全问题的解决离不开工控厂商的支持，自然西门子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）http://www.tofinosecurity.com.cn/ 公司曾以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，除了美国 NIST 的 NIST800-82 之外，IEC62443 标准也是工控安全研究者最为关注的工控安全标准，需要与 NIST800-82 的内容相对照，并结合企业自身的业务特点进行综合考虑的基础上，制定工控企业实用的工控安全防护方案。

国内政策法规动态

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
  - 工信部关于工控安全的 451 号文
  - 电监会的《电力二次系统安全防护规定》
  - 电监会 2013 年 50 号文，《电力工控信息安全专项监管工作方案》
  - 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
- 标准草案

这两年在信安标委的指导下，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》

另外，其他主管部门牵头制定的标准还有：

- 《工业控制系统信息安全等级保护设计技术指南》
- ……

国内产业联盟动态

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迅速有效地取得积极成效而搭建一个交流平台。

工业控制系统信息安全产业联盟成立以来的主要工作如下：

- 开通联盟网站 http://www.icsisia.com/ ，拟建立成员单位通信员制度，并定期提供电子月讯，实现联盟成员间的信息交互并展示联盟成员成果动态信息。

- 2014 年 5 月 22 日，在上海举办“2014 工业控制系统信息安全年”大型主题系列活动首站上海站活动及第三届工业控制系统信息安全峰会（绿盟科技李鸿培博士作为联盟专家委员会成员主持下午的技术大会）。
  - 会议资料下载地址： http://huodong.kongzhi.net/2014ICSIS-1/zhibo.html
- 2014 年 7 月 1 日，组织联盟成员参观工控安全企业和利时集团，并就工控系统的安全问题进行技术交流。
- 2014 年 7 月，组织联盟成员和行业用户合作申报“2014 年度中关村产业技术联盟重大应用示范项目”
- 2014 年 8 月 1 日，工业控制系统信息安全产业联盟（ICSISIA)协办 “中国自动化学会专家咨询工作委员会（ECC）2014 年会暨第四届全国自动化企业发展战略论坛”（会议主题：环保与安全）大会。
- 借助联盟成员工信部四院，促进行业标准的制订和落实。
- ……

绿盟科技作为“工业控制系统信息安全产业联盟”的发起单位之一，积极参与了联盟成立以来的各种活动，并依托联盟与联盟的主要成员单位工信部电子科学技术情报研究所（电子一所）、工信部电子四院、中国电科院、力控华康、和利时等单位进行了相对深入的合作与技术交流。

国内工控安全厂商动态

由于工控系统被广泛应用到电力、石化、交通、市政以及关键制造业等涉及国计民生的重要行业中，如遭受攻击，受到影响的将不仅是相关企业的经济损失，甚至会引起相应的社会问题，其重要性不言而喻。因此，工控安全问题已成为当前世界各国最为重视的安全问题，在国内已被上升到国家安全战略的高度，国家的政策、标准也正在逐步的制定、完善的过程中。虽然国内工控安全市场目前也仅仅是处在刚起步、培育市场的前期阶段，但其未来市场潜力巨大 ，而且在国家层面，包括发改委、工信部等主管部委也通过设立专项基金，以资助国内科研院所、企业的工控安全技术研究及工控安全产品研发及产业化。

在此背景下，国内的科研院所、工控系统厂商、信息安全厂商以及一些专注做工控安全的新兴企业都将一定的研发力量投入工控安全的研究及产品研发领域，并力争在工控安全领域获得先发优势。

■ 不同背景的两大企业阵营

但要为工控行业的用户提供工控系统安全服务，不仅需要熟悉工控系统，而且还要具备信息安全服务及网络攻防的能力。从这个角度来看，工控系统、信息安全背景的企业各具有优势，但都缺乏对方所具有的能力和人才储备。这可能会在未来的一段时间内，工控安全领域会保持两个明显背景不同的两大企业阵营[①]：

（1） 工控系统背景的厂商

代表性企业有和利时、浙大中控、四方继保、南京自动化、三维力控、北京亚控等，虽然因攻防人才储备的角度，他们短期内难以大幅度提升其工控系统的攻防实力；虽然可以通过企业并购的方式，但在国内整个工控安全市场刚刚起步，尚没有明显具有竞争优势的企业或产品的时候，这种可能不是太大。但他们将会基于对工控系统及行业业务流程熟悉的优势，利

[①] 因工控安全在很多行业涉及到国计民生的安全，虽然国际性著名的工控系统提供商西门子、施耐德电气、GE、罗克韦尔、日本横河等在国内很多行业都在应用其工控安全产品，甚至是拥有垄断的市场地位；同时他们在工控安全研究方面也拥有先天的优势。但从国家安全的角度，工控系统的安全产品的自主可控要远比工控系统的自主可控要重要的多，因此目前这些国际性工控系统厂商并不是国内工控安全企业的潜在竞争对手，甚至他们的产品在国内销售因要符合国内的安全监管需求而需要配合国内厂商的工作。所以本节主要讨论国内厂商的竞争态势。

用其已有的行业用户群资源，采用系统集成的方案整合其工控系统的功能安全类产品、自研或友商的信息安全类产品，通过提供整体安全解决方案，实现在现有业务上的信息安全增值服务。

工控系统技术、产品、方案以及行业用户群，将可能使这类企业在寻求信息安全厂商进行战略合作时占据相对优势的地位。

（2） 信息安全背景的厂商

代表性企业有绿盟科技、启明星辰、天融信、中科网威等这些传统的信息安全厂商，他们的优势在于多年的信息攻防、安全服务经验的积累以及完善的信息安全产品线。当工控系统面对来自系统、网络层面的黑客攻击时，相对于工控系统背景的厂商来说，其优势自然是不言而喻的。但因工业控制系统行业并非是信息安全背景的厂商的传统关注对象，对工控系统相关技术与人才的储备也是从事工控安全研究及产品产业化的最大短板。

因工控行业是一个大行业，面对的客户群体又有很多不同的垂直细分行业，而且工控系统主要关注系统功能的实现，从而造成行业间的标准化不足，系统通用性比较差，而且各细分行业的业务运营模式都有很大不同，在讨论起安全性时也将有很多的个性化因素在里面。比如，在调度相关的工控系统中需要重点关注系统的实时、授权控制；而在关键的制造业则可能是要保证生产流程的连续性及敏感生产数据的防泄密等问题。个性化的工控系统及业务层面的设计使得信息安全厂商将会面临很多个性化的定制服务需求，这使得信息安全厂商难以通过像互联网安全行业那样的通用化服务或产品来提高其安全服务的投入产出比。虽然国内在工控信息安全服务及产品方面的标准化工作正在进行，但这需要工控行业厂商、行业用户以及信息安全厂商共同参与，形成分行业的标准化安全解决方案及相应的安全产品相关标准，共同培育行业性的工控安全市场。只有在具备了标准化的行业安全解决方案及相应的安全产品标准后，信息安全厂商才可能独立地提供行业通用性的工控安全防护类产品，实现产品的规模化与产业化。

当然，国内还有一些专注于工控安全的新兴公司，诸如力控华康、海天伟业、中京天裕、匡恩科技等。这些公司目前规模较小，但拥有一定的工控行业背景且因进入工控安全领域较早，多声称拥有自主工控安全产品（工控防火墙、工控系统隔离设备）和安全解决方案。因此，我们原则先把这些新型企业视为具有工控系统背景的厂商。随着工控安全市场的成熟，当前这种工控安全提供商明显划分为两大阵营的情况会逐步淡化，那时主导这个工控安全行业的将是专注于工控安全的“工控安全厂商”。

而国内的科研机构，比如工信部一所、四所、中国电科院、中科院信工所、沈阳自动化所等，因他们多侧重于政策、标准、验证环境建设及技术、方案方面的研究工作，他们的研究成果的应用及产业化则可能需要通过与上述两类涉及工控安全领域的厂商进行合作。

■ **国内工控安全厂商动态**

这里初步介绍我们所了解的一些国内从事工控安全研究厂商的进展情况，为大家进一步讨论国内工控安全市场的竞争态势提供参考。

我们首先来讨论具有工控系统研发背景的厂商情况。

（1） 中国电子信息产业集团

中国电子信息产业集团的华北计算机系统工程研究所（原电子部六所）近几年比较重视工控安全研究及产品开发方面的工作，并把工控安全作为其在信息安全领域的重要研究方向之一。已建立了工控安全实验室，并正在进行工控防火墙等产品的开发。

（2） 和利时

和利时为国内具有较高技术水平和实力的工控系统厂商，在北京亦庄拥有自己的工业园区，年产值约 40~50 亿元，其工控系统产品主要覆盖的行业有：轨道交通、市政、煤炭、医药制造等行业。今年来在工控系统安全方面因用户需求的驱动，

也有较大的投入。建立了专门的工控安全团队，加入工业控制系统信息安全产业联盟，并成为副理事长单位。除了其传统的功能安全，积极参与工控安全相关国家标准的制定工作，并期望与联盟成员协同合作，通过整合各家的优势产品形成联盟级的工控系统信息安全解决方案。

（3） 浙大中控集团

浙大中控集团是中国领先的自动化与信息化技术、产品与解决方案提供商，2013 年经国家发改委批准成立了“浙江大学工业控制系统安全技术国家工程实验室”。该实验室的重点工作是，针对炼油、化工、电力、水厂、交通等基础设施工业控制系统漏洞暴露的问题及用户的实际安全需求，建设工业控制系统安全技术研发与工程化平台，开展工业控制系统安全脆弱性分析、安全防护、安全评估、安全渗透与对抗等关键技术、产品的研发及产业化。同时浙大中控集团也参与或主持了多项工控安全相关国家标准的制定工作。

（4） 力控华康

北京力控华康科技有限公司（简称力控华康）成立于 2009 年，是专业从事工业网络及安全产品研发，提供整体安全解决方案。该公司具有一定的工业领域行业经验，拥有工控行业监控软件和工业协议分析处理的相关技术。其工控安全相关产品主要有，适用于工业控制系统的工业隔离网关 pSafetyLink®、工业通信网关 pFieldComm®和工业防火墙 HC-ISG®等系列产品。目前在冶金、石化等行业有一定的用户群。此外，该公司也是工业控制系统信息安全产业联盟的成员单位，也曾承担过 2012 年的国家发改委安全专项课题——工控防火墙项目的研发工作。

此外，诸如中国电科院、南瑞、南自等行业内企业，他们一般拥有行业内的优势市场地位，并在工控系统及工控安全研究及解决方案提供方面拥有强势的资源和影响力，应是我们争取合作的战略伙伴，这里不作为竞争厂商进行分析。

其次我们介绍具有信息安全背景的工控安全厂商的情况。

（1） 绿盟科技

北京神州绿盟科技股份有限公司，是国内著名的信息安全厂商，国内上市企业，工控系统信息安全产业联盟的主要成员之一。拥有完善的信息安全产品线和强大的技术服务能力。在工控安全研究及产品化方面，不仅在 2012 年承担国家发改委的安全专项——工控审计系统的研发及产业化项目，而且公开发布针对工控安全的综合性研究报告、实施多项电力、石化、烟草等行业的安全风险评估项目，成功开发了工控漏洞扫描系统、工控安全审计系统等两款专业化的工控安全产品，在多家战略合作伙伴的工控系统仿真试验环境中进行测试验证的同时，也在部分客户的环境中得到了试用。同时，绿盟科技这两年也参与多项关于工控系统安全的国家标准的起草与制定工作。

（2） 启明星辰

启明星辰，也是国内著名的信息安全厂商之一，国内上市公司，工控系统信息安全产业联盟的主要成员之一。近年来在公司内部成立专门的工控安全研究团队，参与了工控安全相关的多项国家标准的起草与制定工作。在烟草、电力、化工等方面也有相应的项目实践经验。

（3） 中科网威

中科网威，也是国内比较早的信息安全厂商之一，未来希望专注于工控安全领域。目前成立有“网威工业控制系统网络安全实验室”，主要工作是开展面向工业控制系统领域的网络脆弱性研究，同时为研发中心提供技术指引；目前实验室主要承担企业内部的技术研究。

中科网威关于工控安全的主要产品包括工控防火墙（NP-ISG6000/4000/2000）、工控网络安全日志服务器产品、工控网络资产安全风险监测产品、工控网络异常检测系统等。

此外，30 所卫士通、天融信、网御神州等公司也在重视和关注工控安全领域的新业务拓展，其中，卫士通在国家标准制订、工控系统安全风险评估指标体系设计等方面做了不少的工作，天融信推出了相关的工控系统安全隔离设备，网御神州也曾承担 2012 年国家发改委的工控安全专项基金项目，与有关单位合作研制工控防火墙。

总的来说，工控安全市场目前仍是一个大家都意识到其重要性，但缺乏指导性的行业标准和行业实践的新兴市场，各厂商的工作多处在前期技术研究、产品原型开发以及用户需求挖掘的市场培育阶段。至少在目前，业内尚没有占据市场优势的产品或公司。

合作策略及建议

因为工控行业是一个大行业，面对的客户群体有不同的垂直细分行业，每个行业的工控系统的业务不同、所关心的安全问题和具体的安全需求也有较大的差异。因此，在每个垂直领域里面，都需要工控系统厂商、信息安全厂商、科研院所以及工控系统的用户群体的深度合作，通过构建产业联盟形成利益共同体，并集成各成员单位的产品与技术优势，通过合理分工协作，形成联盟层面的安全解决方案。在此基础上，建设行业应用的示范工程项目，通过总结成功案例的经验教训，在国家主管部门的指导下，制定出针对行业的工控系统信息安全建设的行业标准或国标。只有建立起行业或国家标准，该行业工控系统安全产业链上的相关各方才能够找到自己的定位。另外，还要完善工控安全方案及产品的测评体系、规范测评机构、完善测评标准，这样才能保证产品提供商为用户提供安全、可靠的工控安全产品。

由于目前整个工控安全行业总体上仍处在一个刚起步、需要培育市场的初级阶段，因此在现阶段我们需要与国家主管部门、科研院所、工控系统厂商、行业专家加强合作，甚至与工控安全厂商这些潜在的竞争对手也要求同存异，在共同开拓、培育市场方面进行合作。也就是说，即使是以前的竞争对手，在现阶段也将会存在“合作大于竞争”的可能。

典型行业的工控安全发展态势分析

发电行业的工控安全发展态势

行业政策动态

■ **能源局**

（1）PLC 安全整改

2010 年爆发的伊朗布什尔核电站震网病毒事件，对于整个工业企业控制系统的安全敲响了警钟。2013 年国家能源局以国能综安全[2013]387 号文发出通知，决定对经检验存在信息安全风险的电力工控 PLC 设备开展隐患排查及漏洞整改工作。整改的范围主要是：发电厂计算机监控系统、辅助设备控制系统等电力工控系统中所使用的 PLC 设备。整改的主要内容：隐患排查：要对本企业发电厂计算机监控系统、辅助设备控制系统等电力工控系统中所使用的 PLC 设备进行细致排查和梳理，并填写本单位《电力工控 PLC 设备生产厂商及型号统计表》，报送能源局电力电力安全监管司。漏洞整改各有关单位要根据企业实际，结合厂站设备检修等工作计划，在确保发电厂安全稳定运行的前提下，积极稳妥地做好对存在信息安全漏洞的电力工控 PLC 设备的整改工作。对于目前经检测存在信息安全漏洞的施耐德电气 PLC，各有关单位应按要求开展漏洞整改工作。其中总装机容量 100 万千瓦以上的水电厂应于 2013 年 12 月 30 日前完成整改工作，由省级以上调度机构统一调度的其他电厂应于 2014 年 12 月 30 日前完成整改工作。

（2）电力企业网络与信息安全驻点

为进一步加强电力企业网络与信息安全监督管理工作，提高电力企业重要信息系统（尤其是生产控制大区信息系统）抵御恶意信息攻击的能力，根据《国家能源局 关于近期重点专项监管工作的通知》（国能监管〔2013〕432 号）要求，国家能源局 2014 年组织对辽宁省电力企业网络与信息安全工作开展了专项驻点监管。根据驻点监管情况，编制形成《电力企业网络与信息安全驻点辽宁监管报告》。根据实地调查摸清了辽宁电力企业的分布情况，也发现了电力企业存在的一些突出的问题，主要集中在：

管理不足：部分电力企业网络与信息安全工作多头管理，职能交叉，缺乏统一领导和沟通协调；信息安全工作人员配备不足，甚至身兼数职，不利于信息安全工作的落实。部分电力企业对网络与信息安全的应急处置工作重视不足，应急预案针对性、可操作性不足，应急演练形式大于内容，起不到发现问题、解决问题的作用。部分电力企业对信息安全等级保护工作重视不够，定级、备案、测评、整改等环节的各项要求落实不严。

技术不足：部分企业生产环境与企业信息网之间缺乏有效的安全隔离；部分企业电力二次系统安全防护设备运行维护不及时、安全配置不完整。

针对存在的问题，能源局提出了如下的监管意见：

1) 强化组织保障体系建设。各电力企业要梳理网络与信息安全管理涉及的部门、岗位和人员，进一步明确各相关部门，特别是牵头管理部门的权利、责任和义务，明确部门间的工作协调机制，各部门要设立信息安全管理专职岗位，责任到人，强化信息安全组织保障体系。

2) 建立健全常态化工作机制。各电力企业要深刻认识到电力信息安全与电力生产安全同等重要。要根据国家和行业监管部门有关要求，落实专项资金、制定工作计划，定期对电力二次系统开展安全评估、等级保护测评，形成常态化工作机制。对评估、测评中发现的问题，要安排资金，及时整改，消除安全隐患。

3) 统筹做好电力工控 PLC 设备安全整改工作。各电力企业要按照《关于开展电力工控 PLC 设备信息安全隐患排查及漏洞整改工作的通知》（国能综安全〔2013〕387 号）的有关要求，根据实际情况，统筹安排，采取召回、固件升级、老旧设备更新等方式分批分期开展电力工控 PLC 设备的整改加固工作。新建系统中要选用安全、可靠、可控的 PLC 等工控设备。

4) 强化信息安全人才队伍建设。各电力企业要面向公司领导、相关部门主要负责人和企业员工，定期组织开展信息安全政策宣贯培训，提高领导层的认识，提高员工信息安全防范意识。同时要制定培训计划，派送技术人员参加行业和其它专业机构举办的信息安全培训，提高信息安全从业人员的专业技术水平。

5) 加大科技支撑力度。各电力企业要进一步加大科技投入，针对电力行业重要信息系统（尤其是生产监控系统）的实际特点及技术发展情况，充分发挥科研院所、高等院校的科研创新能力，深入开展基于可信计算的系统安全免疫、电力工控设备信息安全漏洞的监测/检测、信息系统安全审计等内容研究，切实保证电力企业重要信息系统的安全可靠运行。

■ 工信部

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》（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 6 个方面要求工业企业加强对于工业控制系统安全的管理。基于 451 号文件，工信部形成了一套针对工业企业工业控制系统的安全检查规范，因为工信部不是电力企业的主要监管单位，从 2012 年开始基于检查规范在一些发电集团的个别电厂进行了试点性的安全检查试用，并未在发电行业中进行大规模的推广。

■ 发电集团内部

从国家出台的针对工控安全的政策开始，各个发电集团已经开始考虑如何来有效的开展工控安全的建设。受能源局委托华能在 2012 年和 2013 年陆续对一些电厂的控制设备进行了漏洞整改，从整改的过程中也积累了大量的工控系统安全建设的经验。利用已有的工控安全建设的经验，通过与现有的工控安全技术进行有效结合，来加强在工控安全方面的建设，现阶段是华能和各个发电集团在未来工控安全建设方面的一个重要的方向。

各个发电集团在日常的安全考核中，已经把工控安全列入到日常的安全考核项目中。一些发电集团已经开始着手针对工控安全从整个集团的角度来考虑如何构建起一套行之有效的管控措施。一些省级电力公司已经开始在一些电厂尝试引入一些新的方法和思路来构建工业控制系统安全，如在 SIS 系统的边界处，通过监听等方式结合数据分析平台，制定相关的工控系统安全考核基线，形成一整套针对工控系统的安全预警机制。

行业工控系统的安全现状及问题

■ 电厂工控系统简介

整个电力系统是由发电、输电、变电、配电、用电和调度组成。其中发电企业是整个电力系统中起始环节，是整个能源闭环系统中最主要的生产环节。我国发电企业通常情况下，主要的发电形式为火力发电、水利发电和核能发电。其中火力发电占据整个发电企业发电量的比重最高。整个发电控制系统多是以 DCS 系统为核心辅以 PLC 作为辅机控制，形成对发电机组的任务下达和停机等控制，同时通过 DCS 与 PLC 反馈的数据了解机组整体运行状况。通过仪器仪表安全系统，如继电保护、故障录波等实现对机制安全运行的监控。

下图是一个火电厂控制系统的示例图，发电控制系统主要是由控制中心（操作员站和工程师站组成）、DPU、继电保护、故障录波、AGC 和 AVC 等组成，其中 DCS 对主发电机组的运行进行监控，PLC 作为辅机系统主要控制组件，辅机系统主要完成如除尘、脱硫等工作。电网的调度主站监控发电机组对电网下达的生产任务的执行情况，为了便于电厂发电与电网的有效阶段，通过部署在电网与电厂之间的关口电表实现对电量信息的统计和核算。

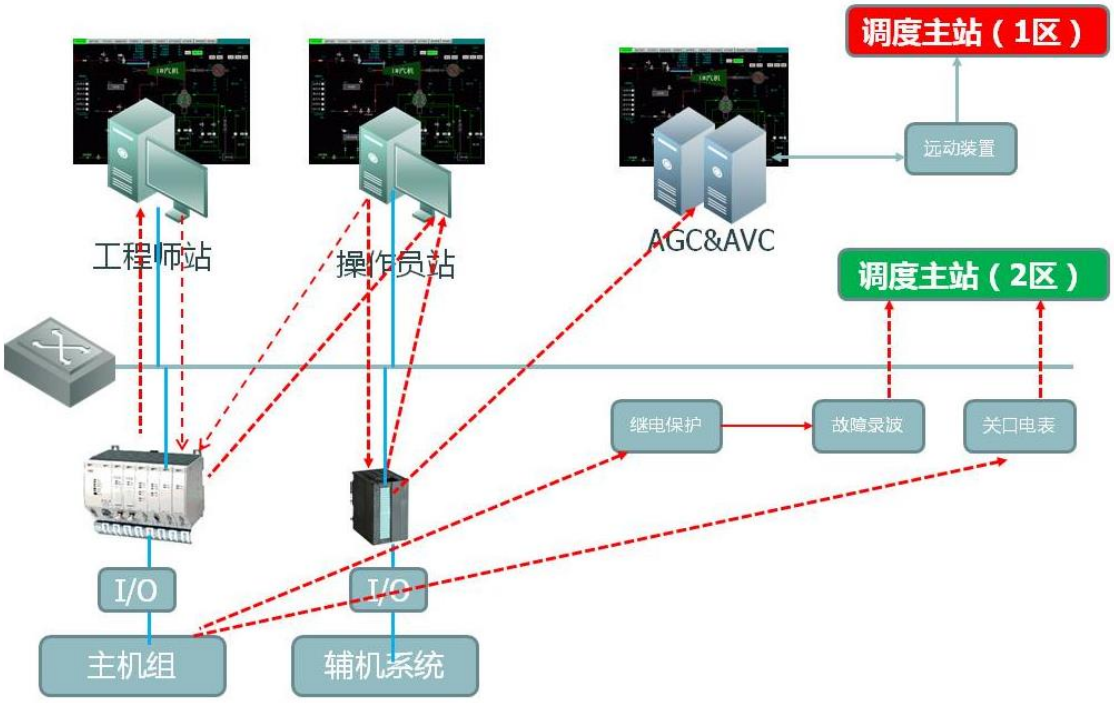


图 1.14　火电厂控制系统的示例图

■ **现有的安全措施**

（1）电力二次系统安全防护

根据电监会 5 号令的要求，发电集团从 2005 年就开始了针对电力二次系统安全防护的建设。依据电力二次系统安全防护的要求，主要是要建立发电厂二次系统的安全区，实现在不同安全区域之间的横向安全隔离以及与调度中心通信的纵向加密认证。下图为发电厂二次系统安全区域示意图（以火电厂为例）。

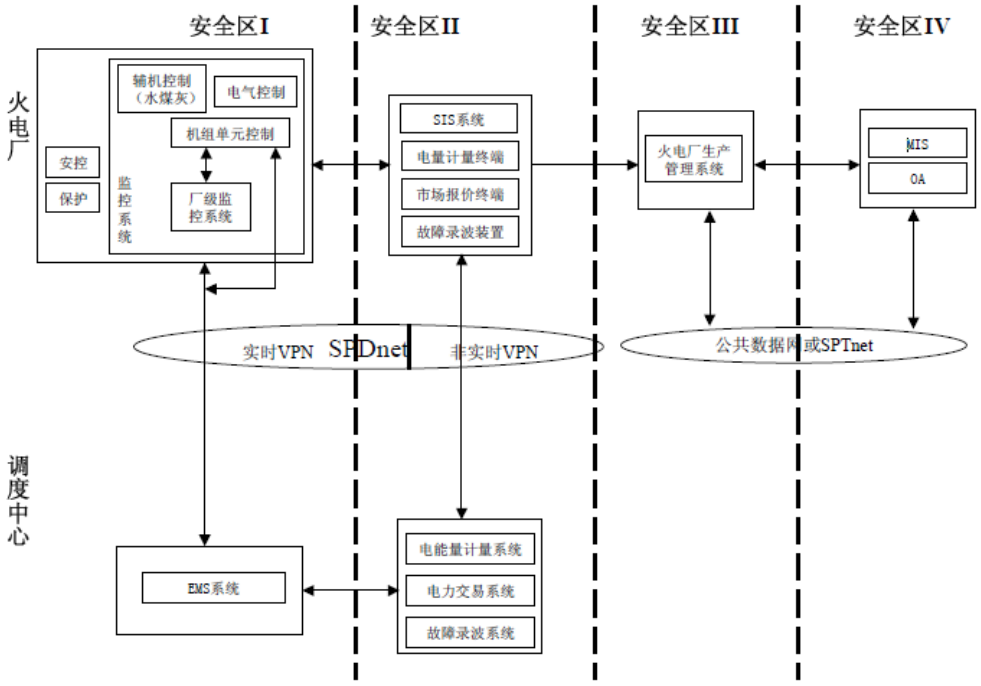


图 1.15　以火电厂为例的发电厂二次系统安全区域示意图

因为电监会 5 号令是专门针对电力二次系统安全防护的指导性文件，并且电监会（现电监会职能已经并入能源局）是定期对相关发电企业进行安全检查，对于严重违背电监会 5 号令精神的企业要求限期整改，并从调度侧严格规范发电企业执行电监会 5 号令，如果出现限期整改仍然无法达标的企业，要限制上网，所以，从发电企业自身的业务需求出发，发电企业对二次系统安全防护很重要，并且都按照 5 号令的要求来执行。整体上看，从边界要求方面发电企业已经建立相对完善的防护体系。

（2）电力等保要求

电监会于 2007 年发布关于开展电力行业管理信息安全等级保护定级工作的通知，要求在电力企业中开展等级保护，要求按照电力行业定义的不同等级的系统进行定级工作。定级指导如下表所示：

表格 3.1　发电行业电力二次系统等保的定级指导

类别	定级对象	系统级别		
		总部	区域（省）	地市
电力二次系统	火电机组控制系统 DCS（含辅机控制系统）	单机容量 300MW 以上为 3 级，以下为 2 级		
	水电厂监控系统	总装机 1000MW 以上为 3 级，以下为 2 级		
	电能量计量系统	3		2

从发电企业实际的情况看，大部分的重点电厂已经完成了等保定级和相关的安全建设，就整个发电企业现状看，对于等保的执行在各地区之间在信息化建设水平的不同，专项资金支持方面存在一定的差异，导致最终在建设方面各地方参差不齐。

- **安全措施的不足**

（1）技术方面面临的问题

- 发电企业对于电力二次系统的安全防护要求的执行，普遍集中在专用装置的部署上，在边界的入侵检测等技术手段上普遍存在不足。
- 对于发生的安全事件，往往缺乏相关的审计手段，无法在事件发生后对事件进行及时定位；往往在事件发生后，无法找到根本原因，最终无法对事件进行定性分析。
- 操作员和工程师站的权限没有相关的管理，普遍存在弱口令等配置脆弱性等问题。对于外部的介质连接等尽管已经从管理角度制定的相关要求，但因缺乏相关的安全技术手段，无法进行有效监控，造成对介质传递的信息无法管理，造成很多的恶意软件直接进入系统中，对系统产生影响。
- 缺乏统一的安全管理中心，所有的安全都是单点的，无法针对已检测到相关潜在安全威胁进行深度分析和定位。
- 缺乏真正意义上的安全域的划分，控制系统内不同区域之间的安全防御没有建立起来，造成某一子系统一旦遭受到攻击很快就会扩散到整个系统中。
- 相关设备通信缺乏有效的安全认证机制。

（2）管理方面面临的问题

- 在生产环境中负责安全的人往往是兼职的，并且对安全的关注度不高，在遇到安全事件时，无法进行有效的定位和及时有效的处理。
- 在控制系统中缺乏有效的信息安全应急响应预案。
- 生产环境中人员信息安全意识淡薄。
- 人员身份与相应的权限没有建立相应的映射关系，只是基于控制系统进行权限划分，没有定位到具体人和设备。
- 安全管理制度中对于信息安全相关的制度和章程基本没有，人员入岗没有进行相关的安全培训。
- 电厂一般都 24 小时不停机状态下运行，人员的轮班一般是有相关的管理制度的，但是在相关人员的权限交接和控制方面普遍没有基于信息安全考虑，人员管理上存在一定的漏洞。

行业安全建设需求分析

■ **服务**

从服务的角度，发电企业在工控安全主要存在着安全体系规划、安全评估和应急响应体系建设 和标准制定四个方面的安全需求。

（1）安全体系规划

部分发电企业在制定安全规划中，已经把生产系统的安全列入到了整体安全保障的框架范围内，并且作为一个建设的重点方向。在建设的目标上，希望能够基于电力二次系统防护的要求，结合发电企业自身安全发展的需求，建立起一套能够保障发电生产安全的防护系统。

（2）安全评估

能源局、工信部门、公安部门定期会对发电企业进行安全检查，对于发现的问题，也希望电力企业能够在限定的时间进行整改。为了解发电企业自身安全的状况和加强防护能力，满足相关部门安全检查的考评指标；发电企业希望能够定期对自身的工控系统进行安全检查，但是前提是希望参与安全检查评估的企业能够拿出一套行之有效的评估方案，确实可以落实到系统的生产环境需求中来。

（3）应急响应体系

随着工控安全在发电企业中重视的提升，发电企业也意识到自身在应急响应方面存在较大的不足，也希望能够建立一套有效的应急响应体系。

（4）标准制定

发电企业在推进工控安全方面面临的一个比较大的问题是，缺乏相关可操作的指导性文件，一些发电企业已经意识到在标准制定方面的缺失，开始了研究相关标准的制定工作。需求主要集中在从上线前的安全验收标准到上线后的安全运维标准方面。

■ **产品**

从产品角度看，发电企业在工控安全产品需求方面主要存在如下产品的需求：

- **传统安全产品需求**
  - IDS：满足电力等保和电力二次防护方案要求
  - 加密认证装置：满足电力等保和电力二次防护方案要求
  - 隔离装置：满足电力等保和电力二次防护方案要求
  - 防火墙：满足电力等保和电力二次防护方案要求
  - 日志分析平台：满足电力等保和电力二次防护方案要求
- **新型安全需求**
  - 工控审计：基于业务行为的审计系统含异常行为审计
  - 工控终端安全产品：操作员站、工程师站防护产品，尤其是进程白名单产品
  - 工控统一管理平台：基于业务和安全的统一分析展示平台
  - 工控防火墙：可部署在工控现场的访问控制设备要求到操作指令级
  - 无线审计：可以基于工业无线的现场环境进行审计

工控安全发展的制约因素

- **国家政策层面**

一方面，工控安全是在国外发生严重工控安全事件如震网事件后而引起关注的，但是我们整体上在工控安全方面的研究起步较晚，相关行业配套设施还不足；另一方面，工控安全是一个交叉学科的领域，相关领域内的企业和人才都比较缺乏，无法形成规模化的安全建设队伍；再者，工业领域中出现的事故是直接带来经济损失和人员伤亡的，在现阶段由于工业安全事件所导致的生产问题还没有完全显现的情况下，通过新技术对运行了数年的工业生产环境进行安全改造，新技术的引入是否会影响到工业生产的正常运行，都存在较大的不确定性。

从国家已出台的工控安全方面的相关政策看，更多的是引导企业在大的框架和指导下进行工作，对于企业是否按照要求进行工作，还缺乏相关的监管机制，国家也是在逐步收集信息过程中逐步会细化相关政策，整体进度上需要一个预热到成熟的过程。

- **企业人员的安全意识**

电厂中的工控系统，通常是这样进行人员分布的，负责信息的人员，进行相关的信息系统的运维和与调度中心通信的远动系统的运维；负责热工的人员，进行主要的控制系统如 DCS 和 PLC 的运维；但在信息安全方面一般是没有固定的人员。对于信息安全问题，相关人员在意识上普遍不够重视。而且在应对突发的信息安全事件时，没有专人来负责，造成应急响应能力普遍缺乏。

- **缺乏安全检测机制**

在电厂的工控环境中普遍缺乏相关的安全检测机制，经常无法定位相关的工控安全事件或者事后分析定位时，需要耗费大量的人力和物力，实际的结果也不一定是最终的原因。在事件难以定位以及无法正确辨别是信息安全事件的前提下，发电企业在信息安全的投入上就不会有太大的主动性，他们更加愿意把发生的相关生产问题定性为功能安全事件，而实际上信息安全事件往往是通过导致功能安全问题，最终导致生产问题。

工控安全的推广策略

- **安全培训**

在发电企业工控安全意识普遍存在一定不足的情况下，安全培训是一个很好的切入点。从发电企业角度来说，因为从国家层面到企业集团层面都对工控安全提出的一些要求，企业也很希望开展相关工作，但是往往不知道可入手的着力点在那里。通过信息安全的培训，加强工控企业现场工作人员和相关管理人员对工控安全的认识，对树立起绿盟工控安全领导性企业的形象也是非常重要的。我们可以引导企业从相关的管理咨询入手，再逐步拓展到相关的工控系统的安全建设上来。

- **产品试点**

工控行业与信息安全行业之间，原来是两个相对独立的行业。信息安全产品对工控具体应用场景的适应性存在一定的不足。而且从产品实际的发展的角度来看，信息安全产品需要与具体环境进行有效结合，通过实践证明对业务没有影响，并能够有效解决工控安全问题的时候，才能得到发电企业的认可。

- **风险评估**

在工业控制系统中一直以来都非常关注功能安全，IEC 61508 的功能安全要求，在工控领域中应用比较多，基于 IEC 61508 的 HAZOP 风险评估方法在新建信息和系统安全改造中应用比较广泛，并且相关的认证也作为企业安全的一个重要方面。

IEC 61508 更加强调工控系统的本质安全和固有安全，但是，从最近发展的趋势看，信息安全也逐步在成为此标准的一个关注点。

从合规性要求看，基于电力等保和二次系统安全防护要求的安全评估对于发电企业来说还是有比较大的需求，尤其是在重大节日保电等时期前。

- **建设思路**
  - 建立工控系统的准入机制如 DCS、PLC 设备、SCADA 软件在上线前的安全检查
  - 基于业务进行安全分区，强化对边界的控制，如针对不同控制业务之间的有效隔离
  - 通信过程的加密认证
  - 基于安全监控业务行为，发现潜在的异常行为，建立起基于业务行为的安全基线
  - 主机及主机应用侧的安全管控，账户权限的最小化原则，如系统进程的白名单机制
  - 基于安全的系统运行分析，早期安全预警与态势分析

电网行业的工控安全发展态势

行业政策动态

■ **能源局要求**

（1）电监会 5 号令

2004 年 12 月 24 日电监会颁布电监会 5 号令。5 号令强调为了防范黑客及恶意代码等对电力二次系统的攻击侵害及由此引发电力系统事故，建立电力二次系统安全防护体系，保障电力系统的安全稳定运行，根据《中华人民共和国计算机信息系统安全保护条例》和国家有关规定，制定电监会 5 号令。

电监会 5 号令主要强调，电力二次系统安全防护的安全分区、网络专用、横向隔离、纵向认证的原则,保障电力监控系统和电力调度数据网络的安全。所有电力二次系统的规划设计、项目审查、工程实施、系统改造、运行管理等应当符合电监会 5 号令的要求。

电监会 5 号在具体执行层面的主要依据是 2003 年全国电力二次系统安全防护专家组和工作组编制的电力二次系统安全防护方案。电力二次系统安全防护方案中电网防护主要在电力调度系统的主站系统内的安全分区之间有效的安全隔离、区域边界的安全防护以及与厂站通信的加密处理等。

电力二次系统安全建设的示意图如下图所示：

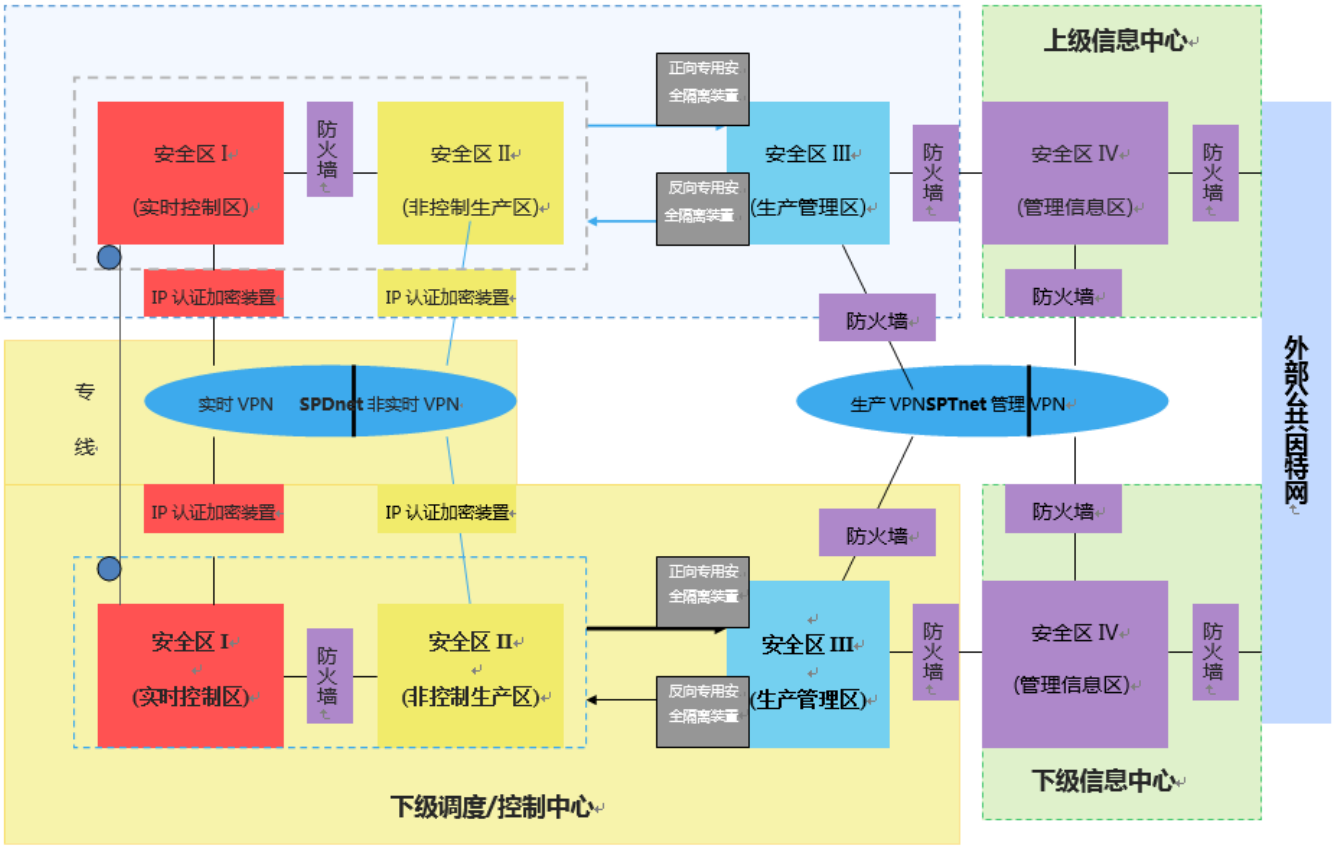


图 1.16　电力二次系统安全建设的示意图

（2）电力等保要求

电监会于 2007 年发布关于开展电力行业管理信息安全等级保护定级工作的通知，要求在电力企业中开展等级保护，要求按照电力行业定义的不同等级的系统进行定级工作。针对电网工控系统的定级指导如下表所示：

表格 3.2　电网的电力二次系统等保的定级指导

类别	定级对象	系统级别		
		总部	区域（省）	地市
电力二次系统	能量管理系统（具有 SCADA、AGC、AVC 等控制功能）	4		3
	变电站自动化系统 (含开关站、换流站、集控站)	220kV 及以上变电站为 3 级，以下为 2 级；集控站为 3 级；		
	电能量计量系统	3		2
	广域相量测量系统（WAMS）	3		无
	电网动态预警系统	3		无
	调度交易计划系统	3		无
	水调自动化系统	2		
	调度管理系统（OMS）	2		2
	雷电监测系统	2		
	电力调度数据网络（SGDnet）	3		2
	通信设备网管系统	3		2
	通信资源管理系统	3		2
	综合数据通信网络(SGTnet)	2		

从国家电网和南网电网对二次系统定级执行情况看，国家电网各个网省公司对于二次系统定级的执行情况较好。在执行相关的等保定级和测评方面，由国调发文指导相关的等保定级和测评，并且对于相关业务系统在等保定级和整改方面制定了相关的时间点。因为国家电网的总部要求在各个网省执行力很强，大部分的网省已经完成了相关业务系统的定级和整改，并且按照相关的要求进行周期性测评，如三级系统每年进行一次测评。

南网电网在等保建设上要相对滞后于国家电网，南网总部对各个网省公司在影响力上不及国家电网。但是作为整个电力系统一个比较重要的安全建设方向，且南网电网规模较小，只涉及 5 个省的建设，所以，尽管在整体进度上不如国家电网，但所涉及 5 个网省的各个省调度中心都已经完成了等保测评和建设，只是部分地市电力公司还存在一定的建设的缺口。

（3）生产控制信息系统类的总体技术与管理要求

依据等级保护的基本要求结合电力行业的特点，主要是在融合电力二次系统安全防护的要求的基础上，提出了针对电力行业生产控制信息系统类系统安全的总体技术及管理要求，详见如下表格。

表格 3.3　生产控制信息系统类总体技术要求

生产控制信息系统类总体技术要求
电力生产企业、电网企业、供电企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区，生产控制大区可以分为控制区（又称安全区 I）和非控制区（又称安全区 II）；
生产控制大区网络与管理信息大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置，确保单向隔离装置策略配置安全有效，禁止任何穿越边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务；
在生产控制大区与广域网的纵向交接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施，确保纵向加密认证装置策略配置安全有效，实现双向身份认证、数据加密和访问控制；
电力调度数据网应当在专用通道上使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离；
控制区的信息系统数据通信应使用电力调度数据网的实时子网或专用通道进行传输，非控制区的信息系统数据通信应使用电力调度数据网的非实时子网； 控制区与非控制区之间应采用国产防火墙，或采用具有访问控制功能的设备进行隔离；
二级系统统一成域，三级及以上系统单独成域；
三级及以上系统域由独立子网承载，每个域有唯一网络出口，可在网络出日处部署满足相应等级要求的等级保护专用装置为系统提供整体安全防护；（注 1：等级保护装置）
省级以上及有实际业务需要的地区调度中心的电力监控系统、电力调度数据网上的关键应用、关键用户和关键设备应使用电力调度数字证书系统实现身份认证、安全数据传输及鉴权；
生产控制大区所部署的安全审计系统，可对网络运行日志、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。

表格 3.4　生产控制信息系统类总体管理要求

生产控制信息系统类总体管理要求
如果本单位生产控制大区仅有一级信息系统时，通用管理要求等同采用一级；
如果本单位生产控制大区含有二级及以下等级信息系统时，通用管理要求等同采用二级；
如果本单位生产控制大区含有三级及以下等级信息系统时，通用管理要求等同采用三级；
如果本单位生产控制大区含有四级及以下等级信息系统时，通用管理要求等同采用四级。

（4）能源局驻点安全检查

为进一步加强电力企业网络与信息安全监督管理工作，提高电力企业重要信息系统（尤其是生产控制大区信息系统）抵御恶意信息攻击的能力，根据《国家能源局 关于近期重点专项监管工作的通知》（国能监管[2013]432 号）要求，国家能源局 2014 年组织对 XX 省电力企业网络与信息安全工作开展了专项驻点监管。根据驻点监管情况，编制形成《电力企业网络与信息安全驻点 XX 监管报告》。根据实地调查摸清了 XX 电力企业的分布情况，也发现了电力企业存在的一些突出问题，主要集中在：

- 管理不足：部分电力企业网络与信息安全工作多头管理，职能交叉，缺乏统一领导和沟通协调；信息安全工作人员配备不足，甚至身兼数职，不利于信息安全工作的落实。部分电力企业对网络与信息安全的应急处置工作重视不足，应急预案针对性、可操作性不足，应急演练形式大于内容，起不到发现问题、解决问题的作用。部分电力企业对信息安全等级保护工作重视不够，定级、备案、测评、整改等环节的各项要求落实不严。
- 技术不足：部分企业生产环境与企业信息网之间缺乏有效的安全隔离。部分企业电力二次系统安全防护设备运行维护不及时、安全配置不完整。

针对存在的问题，能源局提出了如下的监管意见：

1) 强化组织保障体系建设。各电力企业要梳理网络与信息安全管理涉及的部门、岗位和人员，进一步明确各相关部门，特别是牵头管理部门的权利、责任和义务，明确部门间工作协调机制，各部门要设立信息安全管理专职岗位，责任到人，强化信息安全组织保障体系。

2) 建立健全常态化工作机制。各电力企业要深刻认识到电力信息安全与电力生产安全同等重要。要根据国家和行业监管部门有关要求，落实专项 资金、制定工作计划，定期对电力二次系统开展安全评估、等级保护测评，形成常态化工作机制。对评估、测评中发现的问题，要安排资金，及时整改，消除安全隐患。

3) 统筹做好电力工控 PLC 设备安全整改工作。各电力企业要按照《关于开展电力工控 PLC 设备信息安全隐患排查及漏洞整改工作的通知》（国能综安全[2013]387 号）的有关要求，根据实际情况，统筹安排，采取召回、固件升级、老旧设备更新等方式分批分期开展电力工控 PLC 设备的整改加固工作。新建系统中要选用安全、可靠、可控的 PLC 等工控设备。

4) 强化信息安全人才队伍建设。各电力企业要面向公司领导、相关部门主要负责人和企业员工，定期组织开展信息安全政策宣贯培训，提高领导层的认识，提高员工信息安全防范意识。同时要制定培训计划，派送技术人员参加行业和其它专业机构举办的信息安全培训，提高信息安全从业人员的专业技术水平。

5) 加大科技支撑力度。各电力企业要进一步加大科技投入，针对电力行业重要信息系统（尤其是生产监控系统）的实际特点及技术发展情况，充分发挥科研院所、高等院校的科研创新能力，深入开展基于可信计算的系统安全免疫、电力工控设备信息安全漏洞的监测/检测、信息系统安全审计等内容研究，切实保证电力企业重要信息系统的安全可靠运行。

■ **国调中心要求**

（1）695 号文

国家电网调度中心在 2011 年发 695 号文，要求各个网省公司开展电力二次系统安全等保的定级备案和开展电力等保建设的工作。并且把等保的定级和建设作为电网安全建设中一个重点，并且提出等保建设要与电力二次系统安全防护相结合.。

（2）168 号文

伴随着智能电网的在国内的建设和发展，配电网的自动化建设也迎来了一个建设的高峰。配电是整个电网生产系统中距离用户最新的业务环境。对于配电的安全性来说，任意可接入配电网的主机下发的控制指令只要是和配电指令要求一致，相关的配电终端就会按照指令的要求执行，如开关旁路、断路器旁路等，就会引起部分区域的断电，对于实际环境来说危害较大。为了有效解决配电终端对主站发送的指令无认证执行的问题，国家电网调度中心发布了 168 号文，在主站与配电终端之间通信时，需要用基于证书的方式对主站下达的指令经过认证后才可以执行。168 号文要求，各个地调中心对新上线的配电终端要采用支持认证的配电终端，主站前置机要加装相关的模块或者加入相关的加密认证装置，对于受条件限制的配电终端，要实现逐步替换，在 2015 年前完成所有配电终端的整改。

（3）常态化的安全检查

电网是整个国家能源供给的核心，电网的安全关乎整个国家的安全。对于电网的安全重视一直以来都是能源行业中的重点。能源局每年都会委托电力信息安全测评实验室对国调和各个省公司的调度中心进行安全检查，已经形成了常态化，尤其是重大节日的保电检查。检查中会参照电力二次防护的要求从技术和管理两个方面对调度中心三个区域的不同业务的安全性进行检查，如发现重大信息安全隐患，会要求相关业务单位进行安全整改，对于问题严重要要在电网范围内进行通报。

行业工控系统的安全现状及问题

- **安全现状**

（1）二次防护构建

电力调度中心主要由 EMS（能量管理系统）、WAMS（广域监测系统）、安全自动控制系统、保护设置工作站等组成的一个实时性的生产系统和 DTS（调度员培训系统）、电量管理系统和继保及故障录波等非实时性生产系统，以及雷电监测系统、气象信息、日报/早报等生产管理系统等系统组成。其中实时系统主要提供基于毫秒级的实时业务处理能力，主要通过 SCADA 系统的下位机对采集的各个一次设备的状态值包括厂站开关、刀闸的状态值、潮流的实时信息、电能量相关状态等实时数据信息，结合这些实时信息对电力系统进行经济、安全评估，并给出调度决策的建议，提高调度的水平，降低调度员的工作状态等功能。非实时系统主要完成调度管理员的模拟操作培训；实现电能量信息、瞬时量信息的采集、存储、上传、发布和维护；实现故障的记录和继电保护的功能。生产管理系统主要实现调度生产区的信息发布和其他支撑调度系统的相关数据支撑的作用，是调度生产相关的业务的集中区域。

根据电网二次防护的要求，根据对业务的实时性和重要性的要求分为三个区，分别对应着实时业务控制区、非实时业务控制区和生产管理区。

根据电网二次防护的要求，根据对业务的实时性和重要性的要求分为三个区，分别对应着实时业务控制区、非实时业务控制区和生产管理区。一区和二区同属于生产控制大区，一、二区之间通过防火墙进行逻辑隔离，在纵向区域和横向区域之间部署入侵检测来检测潜在的入侵行为。在二区和三区之间、一区和三区之间使用正向和反向隔离装置实现数据的定向传输。在三区信息大区与信息外网之间也要使用单项隔离装置实现数据的传输。为了有效加强对内部相关日志的管理，要求日志审计和管理机制。在调度中心与变电站和电厂之间，通过纵向加密认证装置现实通信的安全性。为了有效

管理电网的安全，建立了国调、网调、省调、地调 4 级人员安全管理，并建立了安全专责负责制，由安全专责对相关的电力二次系统的安全防护的运维负责，依据电力二次防护方案的要求对电网安全的建设提供合理的安全规划建议。

电网的整体安全建设依据分区、分域、边界防护、责任到人的方式来进行相关的安全建设和管理，更多的是强调在边界处对威胁的抵御能力。

（2）自主可控建设

电网因其所处的行业的重要性，自主可控在电网中提出的比较早，并且也是国内比较早开始实践的行业。在 2000 年之前电网中从调度中心到变电站普遍都在采用国外的控制设备软件系统。在变电站和调度中心陆续出现了由于国外运维人员所导致的安全事故后，对于自主可控的建设提上了整个电网的议题中，尤其是国家电网，已经陆续在新建和改造的变电站中大量采用了国产设备，从测控装置到继保装置到合并单元，涵盖了整个变电站控制设备的绝对部分。工程师站和操作员站的应用软件都已经国产化，部分新建站的操作系统都已经开始在应用国产的 linux 系统。

在调度中心除了依据电力二次安全防护进行防护外，经过几年的国产化改造调度系统的主要业务系统都已经实现了国产化，相关的支撑平台，如操作系统、数据库、中间件都已经实现了国产化。并且基于可信计算的思路，建立了一套安全调度系统平台（D5000 平台），通过 D5000 平台把原先分散的控制系统通过总线集成的方式放入一个系统中，在系统中建立了完善的人员身份认证和权限管理的机制。系统之间不同模块之间的通信需要基于可信通信的方式进行通信，通信的过程要进行严格的审计记录，为了对整个系统的安全和厂站安全进行有效的监控，D5000 平台中集成了内网监视模块，来对系统内各个业务系统的安全状况进行监控。

整体思路是以自主可控的产品来构建控制系统内部的安全，并结合二次系统防护对边界的要求，从整体上构建电网控制系统的安全。

- **面临的问题与挑战**

尽管电网已经从边界防护、管理和自主可控方面下大力气进行相关的安全建设。但是，智能电网的发展使更多的互联互通成为可能，未来开放用电侧的接入配电与用电的接口互通等所带来的外部暴露面的扩大，都将为电网的安全运营带来隐患。另一方面，新型攻击如 APT 攻击等所带来的冲击已经对电网的安全构成了足够的威胁。

行业安全建设的需求分析

- **APT 检测与防护需求**

伴随着 APT 攻击给国外工控所带来的巨大影响。而且从调度系统本质上来说，是一个内部全互连，外部有限互连的系统，尽管有相关的隔离装置，但仍然存在着对外交互数据和信息的流入和流出。而且外部的组织从来没有停止试图对调度系统的渗透，尤其是在 APT 攻击盛行的现在。调度中心已经开始着手对 APT 攻击的检测和防御的预研，但是现阶段缺乏相关成熟的针对调度系统的成熟方案和产品，整体进度比较慢。但是，从实际需求的角度考虑，是刚性的，是未来一段时间内调度系统在安全建设方面的一个新的着力点。

- **工控运维堡垒机**

在变电站的运维过程中普遍缺乏有力的监管技术手段，虽然从制度上进行了对运维人员的行为进行约束，但是从实际效果看，一方面在缺乏技术手段的情况下，执行的效果有限；另一方面运维人员自身安全意识不强，也导致了相关运维中把风险引入到系统中。此部分需求是潜在的安全需求，因为实际用户在运维过程中遇到的安全事件很难定性为信息安全事件，造成现实中信息安全需求的刚性不足。

- **被动式漏洞扫描**

鉴于调度系统的主站和厂站的重要地位。从能源到调度中心已经明确提出，禁止在线扫描相关控制系统。而对于工控组件的安全漏洞从能源局到调度中心都是非常关注的，都希望有被动式的扫描产品可以部署在客户现场来对各个系统的漏洞进行在线检测，可以对配置发生变更时，及时进行预警。

- **评估加固服务**

调度系统每年都有相关的评估和加固的需求，在执行过程中，基本是由电力信息安全测评结构所承揽，缺乏有效的检测工具和人力等问题，评估和加固的效果有限，并没有很好的满足其安全需求。虽然因为体制的问题，现阶段从风险规避的角度来讲，由相关的测评机构承揽风险最小，但调度中心更希望由独立第三方受测评机构委托的形式，进行相关的安全评估和加固。

工控安全发展的制约因素

- **业务的重要性**

电网是关乎国计民生的重要国家基础设施，而电网调度中心是电网业务的核心承载组件。因为电网的重要程度，电网是国内最早开始工控安全防护和建设的企业，依托于电力系统二次安全防护的要求，电网构建起了一套边界防御的铜墙铁壁。也因为电网的重要，电网在推动工控安全新的思路和方向时，相对比较保守，在满足合规性要求的情况下，新的工控思路在不完全成熟的情况下，电网一般不会主动引入新的防护思路。

- **网络隔离**

调度系统本身是一个内部全互连外部有限连接的网络，通过有效的安装隔离装置实现了与外部资源之间有限的信息传送。在有限外部通信被控制在小范围可控的情况下，电网短期内是不容易接受新的防护思路。

- **成熟产品的需求**

在电网中运行了多年的隔离装置和加密认证装置已经在电网中得到普遍认可。而实际从国内工控安全厂商提供的工控安全产品看，缺乏有说服力的、真正符合电网在工控安全方面要求的产品，造成了一些新的防护思路在电网中比较难进行大范围的推广。

工控安全的推广策略

在电网中推广工控安全的新思路，短期内存在一定的障碍，无论是政策层面的导向还是内部责任问题，整体的思路上还是在而二次系统安全防护的增强上。而对于 APT 等新兴威胁的检测和防护从现在的情况看，是电网比较关注的，这对于我们来说是一个比较好的机会点和突破点。从漏洞检测手段上看，电网现在普遍缺乏，尽管也在引入阿基里斯的检测，但是对于实时系统来说，仍然无法实时检测，需要在实时系统的安全漏洞检测和配置变更方面引入相关的技术手段，这方面对于电网来说是比较迫切的。

另一个方面服务对于电网来说是比较重要的，但是限于我们第三方的身份，在实际安全服务方面存在一定的障碍，如果想进入到调度提供安全服务，还是需要我们联合相关的测评机构，以测评机构的名义来推动安全服务。

总体上来说，电网的工控安全需要有新的思路和产品作为支撑，配合与客户环境的贴合，最终才能形成规模化。

结束语

本文首先从工业控制系统自身的脆弱性、最新的安全攻击事件及安全攻击威胁的角度讨论了工业控制系统现阶段的安全威胁态势，分析的结果表明：

（1） 工控系统的相关公开漏洞数 2011 年之后持续保持快速增长的势头。2013 年公开的漏洞数高达 177 个，2014 年上半年也新增了 64 个，而且其中高危漏洞占比超过一半，达到了 51%。而且这些漏洞有以拒绝服务类（33%）、缓冲区溢出类（20%）、信息泄露类（16%）、远程执行类（12%）漏洞占据绝大多数；而且受影响的多是工控系统中的 SCADA/HMI 系统（其占比超过 40%）。显然这对业务连续性、实时性要求高的工业控制系统来说，无论是利用这些漏洞造成业务中断、获得控制权还是窃取敏感生产数据，都将对工控系统用户早成极大的安全威胁。更何况目前这些公开漏洞所涉及的工控系统厂商又是市场优势企业，其系统的广泛使用性及工控系统漏洞的难以及时修复等现实情况，使得各行业工控系统都可能存在严重安全隐患。

（2） 根据 2014 年 6 月包括 ICS-CERT、赛门铁克等多家安全组织或企业的安全通告表明：黑客组织“蜻蜓组织”利用一种类似于“震网病毒”，专门针对工控系统进行攻击的恶意程序 Havex（目前已发现其变种多达 88 种），对欧、美地区的一千多家能源企业进行了攻击。这次攻击事件表明：黑客组织（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最大安全威胁。

（3） 依据 ICS-CERT 的调研分析，近几年工控安全的相关事件呈快速增长的趋势，而且多集中能源行业（59%）和关键制造业（20%）。

其次，则从工控安全领域的国外同行的研究发展动态概述、国内的政策法规动态、国内产业联盟及主要工控安全厂商的发展动态等多个角度入手，讨论了国内工控安全领域的总体发展态势，认为目前国内整个工控安全行业总体上仍处在一个刚起步、需要培育市场的初级阶段，因此在现阶段我们需要与国家主管部门、科研院所、工控系统厂商、行业专家加强合作，针对工控这个大行业中不同的垂直细分行业，进行针对性的分析、研究；通过构建利益共同体（产业联盟等形式）、整合各方的优势技术与产品，提出具有行业特色的工控系统信息安全解决方案，并通过示范工程项目进行试点推广。

在开拓、培育市场方面，甚至与工控安全厂商这些潜在的竞争对手也可能“求同存异”进行合作。也就是说，即使是以前的竞争对手，在现阶段也将会存在“合作大于竞争”的可能。

最后，则是根据我们上半年在发电、电网等几个典型工控行业的调研结果，从行业政策动态，行业工控系统的安全现状、问题与需求，当前制约该行业工控安全建设发展的主要因素等多个角度对这些行业的工控安全发展态势进行讨论；并在此基础上提出我们针对该行业的工控安全服务的推广策略。

综上所述，本报告在重点讨论工控系统的安全威胁态势、当前国内工控安全领域的总体发展态势以及发电、电网等几个典型行业的工控系统的安全现状、存在的问题及安全需求的基础上，提出了工控安全厂商的对外战略合作建议以及针对典型工控行业的安全服务推广策略。本报告的内容可以帮助读者了解工控系统安全领域的总体发展态势，并可作为工控安全领域的主管部门、工控系统用户以及工控安全服务商在决定下一步工控安全投入时的决策参考。

附录

A.1 图表索引

表格索引

插图索引

A.2 作者和贡献者

作者：

李鸿培，绿盟科技

Email：lihongpei@nsfocus.com

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

王晓鹏，绿盟科技

Email：wangxiaopeng@nsfocus.com

绿盟科技行业技术部高级顾问，具有多年的能源行业安全服务经验。参与或主持过多项工业控制系统相关的安全咨询项目，项目覆盖了电力、石化、烟草等重点行业。

贡献者：

王洋，绿盟科技

Email：wangyang2@nsfocus.com

如果您对报告内容有建议，有更多见解需要与我们分享，
可以直接发送邮件到如上地址，
或者与绿盟科技官方微博进行在线活动互动 @绿盟科技
对于您的分享，这里先行致谢！

A.3 缩略语中英文对照

APT	Advanced Persistent Threat，高级持续性威胁
CII	Critical Information Infrastructure，关键信息基础设施
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，即“通用漏洞评分系统”
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
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
SCADA	Supervisory Control And Data Acquisition，数据采集与监视控制系统

A.4 参考文献

[工信部 451] 关于加强工业控制系统信息安全管理的通知，工信部协[2011]451 号

[电监会 2005] 电监会 5 号令《电力二次系统安全防护规定》

[电监会 2013] 电监会 2013 年 50 号文，《电力工控信息安全专项监管工作方案》

[国家烟草局 2013] 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》

[国家能源局,2013] 国家能源局国家能源局关于近期重点专项监管工作的通知（国能监管〔2013〕432 号）

[CVE] http://www.cve.mitre.org/

[CNVD] http://www.cnvd.org.cn/

[DHS2011] Common Cybersecurity Vulnerabilities in Industrial Control Systems， May 2011

[Dragonfly] Dragonfly: Western Energy Companies Under Sabotage Threat.

[GK2013] 2013 首届工业信息安全用户高峰论坛，北京，2013 年 8 月 8 日。

http://www.cheminfo.gov.cn/HezuoPage/gongkong.aspx...

[Havex] ICS Focused Malware ,Alert (ICS-ALERT-14-176-02A)

http://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

[Havex2] Havex：类似 Stuxnet 的恶意软件袭击欧洲 SCADA 系统，http://www.freebuf.com/news/37861.html

[Havex3] FireEye：发现 SCADA 间谍软件 Havex 的最新变种， http://www.freebuf.com/news/38954.html

[ICSCERT1] ICS-CERT_Monitor_April-June2013_3

[ICSCERT2] ICS-CERT_Monitor_Jan-Mar2013

[ICSMM2013] ICS-CERT_Monitor_Oct-Dec2013，ICS-MM201312，http://ics-cert.us-cert.gov/monitors/ICS-MM201312

[ICSMM2014] ICS-CERT Monthly Monitor Newsletters，ICS-MM201404

http://ics-cert.us-cert.gov/monitors/ICS-MM201404

[LHW2014] 李鸿培、忽朝俭、王晓鹏，《工业控制系统的安全研究与实践》，绿盟科技，技术报告，2014.03。

http://www.nsfocus.com/report/NSFOCUS_ICS_Security_Report_20140311.pdf

[NIST] Guide to Industrial Control Systems (ICS) Security：NIST，SP800－82，June 2011.

[NVD] http://web.nvd.nist.gov/view/vuln/search

[wooyun] http://www.wooyun.org

A.5 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。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS