SECURITY+

NSFOCUS

2014

工业控制系统的安全研究与实践

执行摘要

在 2013 年，工业控制系统的安全问题在国内许多信息安全相关的技术大会上作为重要的研讨议题频繁出现，已成为工业控制系统相关的各行业以及信息安全领域的研究机构、厂商所关注的热点方向之一。同时，国家在政策订、技术标准研制、科研基金支持、促进行业内合作等方面也再逐步加大推动的力度。

在此背景下，本报告首先基于我们 2013 年推出的“工业控制系统及其安全性研究报告”，进一步讨论工业控制系统在 2013 年新增公开漏洞的变化趋势及统计特征、分析工业控制系统所面临的安全威胁及 APT 攻击的特征，探索针对工业控制系统脆弱性及攻击威胁的检测及防护方法，提出我们的安全防护建议。其次，结合我们的项目实践经验选择了电力、市政这两个行业的典型系统（智能变电站、自来水厂）作为案例，对其相关工业控制系统的安全问题进行了较为详细分析讨论，并分别通过两个虚构的攻击场景对它们可能存在的安全风险给出了一个直观的描述。最后则是讨论了关于工业控制系统的安全保障需要国家、行业监管部门、用户、工业控制系统提供商以及信息安全厂商等多方面协同努力的行业发展建议，并初步探讨了信息安全厂商关于工业控制系统相关的安全研究、产品开发及安全服务提供的发展思路。

本报告的内容将有助于工业控制系统的用户了解工业控制系统的脆弱性、所面临的安全威胁及初步的防护建议，提升用户的信息安全意识。同时，本报告对于行业政策的制订者以及工业控制系统安全的产品及服务提供商也有一定的参考价值。

目录

表格索引

插图索引

一. 引言

1.1 研究背景

工业控制系统的重要性、脆弱的安全状况以及日益严重的攻击威胁，已引起了世界各国的高度重视，并在政策、标准、技术、方案等方面展开了积极应对[LYHC2012]。进入 2013 年以来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。

因为历史上相对封闭的使用环境，工业控制系统在开发时多重视系统的功能实现，对安全的关注相对缺乏。不像传统 IT 信息系统软件在开发时拥有严格的安全软件开发规范及安全测试流程，这必然造成工业控制系统不可避免地拥有较多的安全缺陷。因此，针对工业控制系统软件自身的安全性评测分析及脆弱性评估是当前首要考虑的问题。

美国国土安全部（The U.S. Department of Homeland Securty，DHS）的控制系统安全计划（Control System Security Program，CSSP）建立了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]，以实施工业控制系统产品的脆弱性验证和分析工作。美国国土安全部下属的 ICS-CERT（工业控制系统应急响应小组）及 CSSP 通过对工业控制系统软件的缺陷性分析发现，工业控制系统软件的安全脆弱性问题主要涉及错误输入验证、密码管理、越权访问、不适当的认证、系统配置等方面（如图 1.1 所示）。尤其是错误输入验证方面的脆弱性在 2009-2010 年度参与测评的工业控制系统软件中占到 45%，这可能会轻易地通过输入不正确的参数，而造成系统故障，显然这种脆弱性对工业控制系统的正常运行具有极大的威胁。

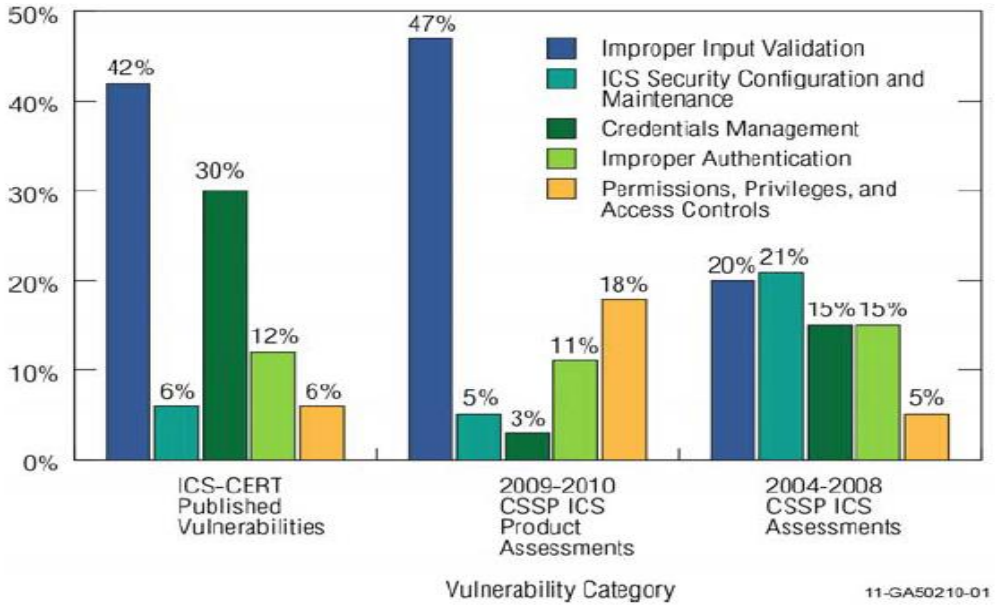

图 1.1 ICS-CERT 及 CSSP 对工业控制系统软件的脆弱性评估分析

同时，工业控制系统应急响应小组（ICS-CERT）更是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]。2012 年 10 月至 2013 年 3 月期间，ICS-CERT 监测到 200 多起工业控制系统安全事件，其中主要集中在能源、关键制造业、交通、通信、水利、核能等领域（图 1.2），而能源行业的安全事故则超过了一半。

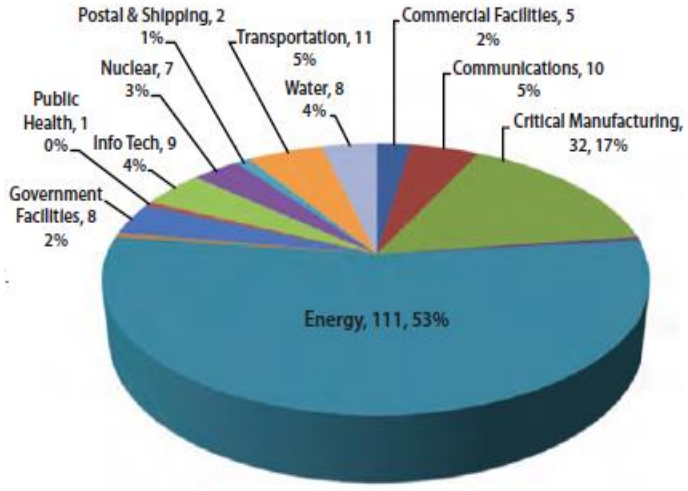

图 1.2 ICS-CERT 关于安全事件行业分布分析（2012.10-2013.03）

结合 ICS-CERT 往年的安全事件统计数据结果可知，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（如图 1.3 所示）。由图中可知，ICS—CERT 在 2013 年上半年统计到的安全事件数已经超过了 2012 年全年的安全事件数。

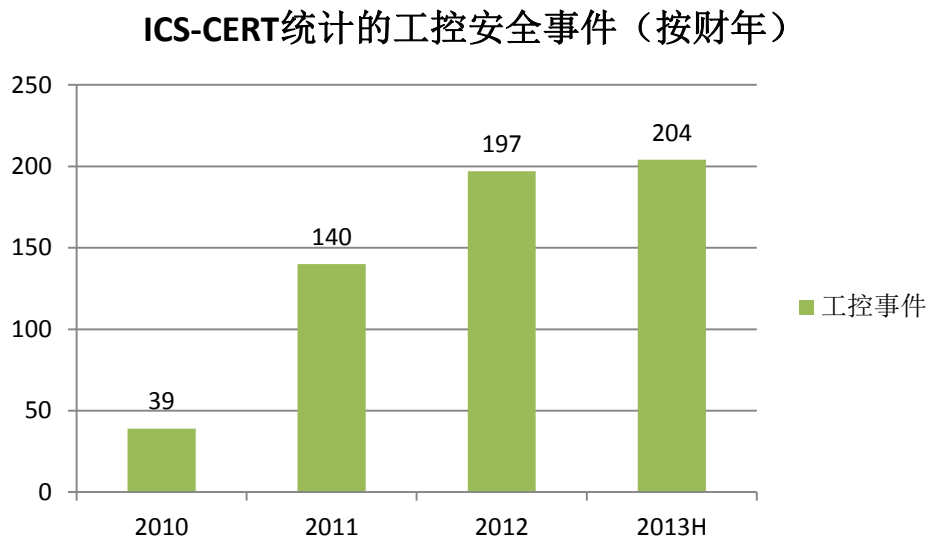

图 1.3　ICS-CERT 统计的工业控制系统安全事件(按财年[①]统计)

此外，CVE 漏洞库也对工业控制系统相关的漏洞非常重视，目前公开的工业控制系统漏洞数以百计，并提供相关漏洞的修补信息。近年的各种信息安全大会上工业控制系统安全已成为一个热点话题[RSA2013] [GK2013]，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）积极推进工业控制系统的相关安全标准，2013 年 5 月份又进一步推出了《工业控制系统安全指南》（NIST SP 800-82）[NIST-1]的最新修订版。

近年来国内电力、高铁、市政、石化行业也出现了一些因病毒入侵所造成的一些安全事件，并造成了一定经济损失，这些安全事件引起了主管部门及用户的极大重视。

2013 年国内已做了大量的关于工业控制系统安全的工作：工业控制系统相关的安全标准正在制订过程中，电力、石化、制造、烟草等多个行业，已在国家主管部门的指导下进行安全检查、整改[工信部 451][电监会 2013][国家烟草局 2013]。在此背景下，我们从 2012 年开始也在积极地开展工业控制系统安全相关的研究工作、技术合作、技术研讨会；在启动相关安全产品的开发、

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。

发布工业控制系统安全研究报告[LYHC2012]的同时，寻求与行业用户合作筹建联合实验室；力图实现工业控制系统的企业（用户）、工业控制系统厂商、信息安全厂商、行业主管部门的多方位战略合作。

虽然国内关于工业控制系统安全的研究及产业化工作刚刚展开。但随着工业化与信息化的深度融合，智能化的工业控制系统在电力、交通、石化、市政、制造的涉及到国计民生的各行各业的重要性也越来越重要，来自信息网络的安全威胁将逐步成为工业控制系统所面临的最大安全威胁，也是我们当前需要迫切进行研究并及时解决的重大问题。不管攻击者的目的是出于经济的目的（比如南美某国电网被攻击者敲诈勒索[Event2008]）、意识形态的纷争[stuxnet1]（比如：燕子行动[LHP2013-1]）甚至是国家间网络战对抗[News2012]的需要，我们必须深入研究工业控制系统的安全性及其可能遭受到的各种威胁，并提供切实有效的安全防护措施，以确保这些时刻关系到国计民生的工业控制系统的安全运营。从这个角度来看，工业控制系统安全相关的产品将不可避免地具有广阔的市场发展前景。根据工信部电子科学技术情报研究所 2013 年 8 月 8 日发布的《2013 年中国工业控制系统信息安全市场研究报告》的预测数据可知[GK2013]：2012 年，中国工业控制系统信息安全市场已达到 11 亿元，未来五年仍将保持年均 15%的增长速度，并将着重于安全审计及运营服务方面。 而根据工控网的预测：中国工业网络安全市场有望在 2015 年达到超 20 亿元的规模，并以每年超过 30%的复合增长率。

行业用户的安全意识培训、工业控制系统的安全状况调查及系统脆弱性评估与整改将是近期的主要工作任务。这就需要建立工业控制系统的安全性测评验证机制，提供系统漏洞信息及厂商的漏洞修补方案及安全补丁的及时通报、分享及可用性验证机制。而以模拟仿真平台为基础的系统脆弱性验证服务和自主可控的测评服务已成为当前工业控制系统信息安全的一种必然趋势。

1.2 研究内容

本文期望在上一期关于工业控制系统及其安全性分析的综述性技术报告的基础上，重点探讨工业控制系统的脆弱性及相关新型攻击技术；并结合行业应用分析电力、市政等领域工业控制系统的安全性及典型攻击场景，提出基于实践的安全建议。期望本报告能够为日益关注工业控制系统安全的用户及相应监管部门提供实用性的帮助。

为方便读者的阅读，这里对报告后续内容的组织逻辑进行简单介绍。

- 第二章，从工业控制系统相关的公开漏洞的统计分析入手，讨论工业控制系统自身的脆弱性及其检测防护建议。
- 第三章，首先基于一个逻辑的工业控制系统部署图识别其所面临的潜在安全威胁，并对可能的攻击途径进行分析。其次，通过分析工业控制系统安全事件，讨论针对工业控制系统的 APT 攻击技术及其检测与防护建议。
- 第四章，通过对智能变电站系统及其安全性分析，讨论当前智能变电站建设中存在的各种潜在安全问题。并通过一个虚拟的攻击场景让用户直观感受所面临的安全威胁。
- 第五章，简要讨论了市政自来水系统所可能面临的安全威胁及可能的虚拟攻击场景。
- 第六章，将在上述分析的基础，对工业控制系统安全行业及相关技术、产品的发展趋势进行了初步的探讨，并给出相关的发展建议。

二. 工业控制系统的脆弱性分析

依据绿盟科技 2012 年上半年的安全威胁态势报告[BL2012]针对整个 IT 行业漏洞发展趋势的分析及预测结果（如图 2.1）：从 2011 年第二季度开始信息网络及系统相关的高风险的安全漏洞正在逐渐被雪藏。造成这种现象的最大可能就是：针对伊朗核电站的“震网病毒”事件之后，大量高风险未公开漏洞通过地下经济出卖或被某些国家/组织高价收购，并被利用来开发 0-day 攻击或高级持久威胁（Advanced Persistent Threat ，简称 APT）的攻击技术，为未来可能的网络对抗做准备。因此，利用 0-day 漏洞的新型攻击正成为网络空间安全防护的新挑战，而涉及国计民生的电力、交通、市政、化工、关键制造业等行业的工业控制系统在工业化和信息化日益融合的今天，将极大可能地成为未来网络战的重要攻击目标。

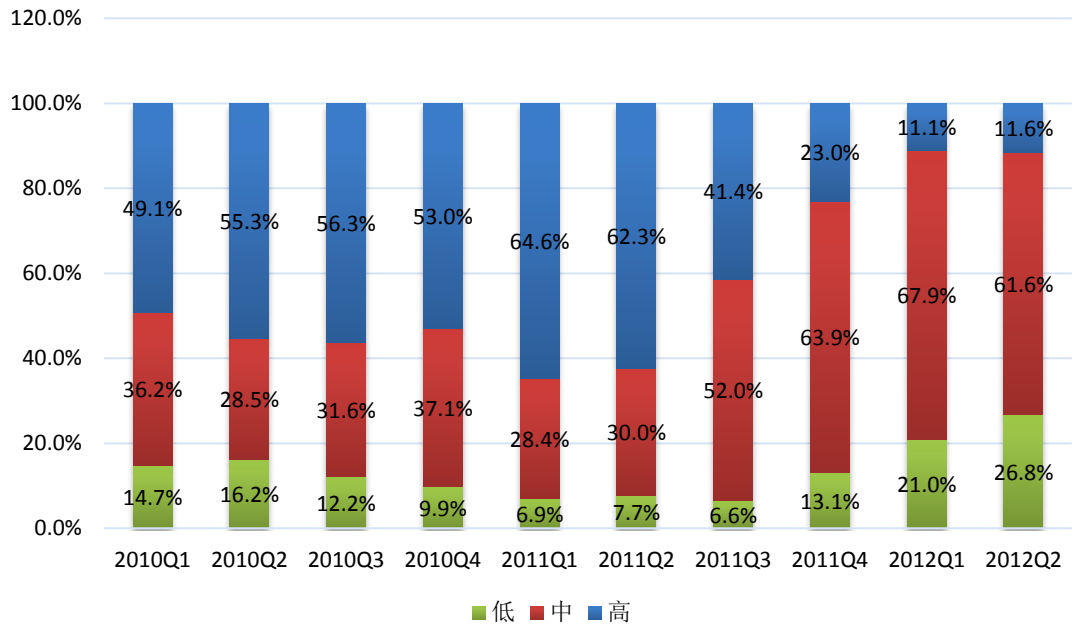

图 2.1 2010-2012 漏洞按风险级别分类的统计分析

随着我国工业化与信息化深度融合的快速发展，成熟的 IT 及互联网技术正在不断地被引入到工业控制系统中，这必然因为需要与其它系统进行互联、互通、互操作而打破工业控制系统的相对封闭性。由于工业控制系统开发时仅重视系统功能实现而缺乏相应的安全考虑，现有的工业控制系统中难免会存在不少危及系统安全的漏洞或系统配置问题，而这些系统的

脆弱性均有可能被系统外部的入侵攻击者所利用，轻则干扰系统运行、窃取敏感信息，重则有可能造成严重的安全事件。

本章将从工业控制系统公开安全漏洞的统计分析入手，来讨论工业控制系统的安全脆弱性及其检测防护的问题。

2.1 工业控制系统的公开漏洞分析

本文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[①]所发布的漏洞信息[CNVD]，共整理出了 386 个与工业控制系统相关的漏洞（截至到 2013 年 12 月）。 因在 2012 年的工业控制系统安全研究报告[LYHC2012]中对 2013 年之前工业控制系统的公开漏洞的情况分析较为详细，本文将重点分析 2013 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、主要工业控制系统厂商分布情况等数据的对比分析。

2.1.1 公开漏洞数的变化趋势分析

图 2.2 给出了截止到 2013 年 12 月之前所公开发布的的工业控制系统相关漏洞按年度进行统计分析的结果。从图中可以很明显地看出：公开 ICS 漏洞数总体仍呈增长趋势，但 2013 年漏洞数增长变缓。

[①] 中国国家信息安全漏洞共享平台（CNVD），由国家计算机网络应急技术处理协调中心运营管理。

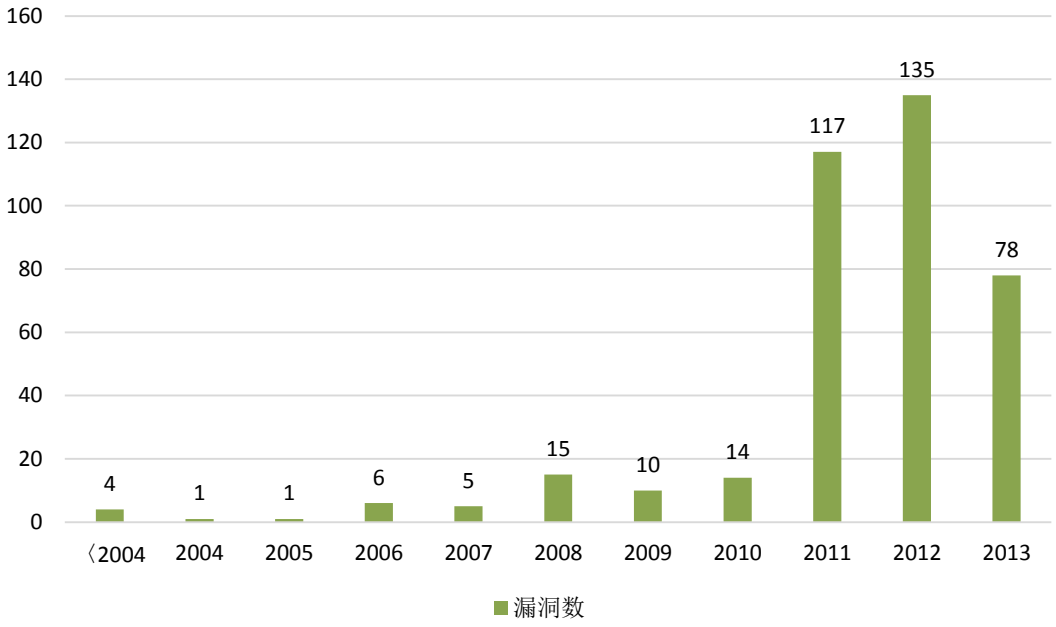

图 2.2 公开的 ICS 漏洞的年度变化趋势

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，并持续到 2012 年；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极度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井喷现象。而 2013 年的新增漏洞数又有所下降，则可能有多方面的原因：

（1） 由于工业控制系统多为行业相关的专有系统，普通的漏洞分析人员因难以接触这些系统且缺乏相关行业知识而很少进行相应的漏洞分析与研究工作；

（2） 工业控制系统的主力厂商（比如西门子、施耐德电气、罗克韦尔、通用电气等），随着对其工业控制系统产品的脆弱性进行针对性分析、挖掘一段时间后，在其产品中发现新漏洞的难度大大提高，发现的公开漏洞数量也将逐渐出现增速放缓或减少的趋势（图 2-3）所示。其中西门子则可能因其信息安全的技术实力相对其他专业工业控制系统厂商而言更强一些，且因当年 Stuxnet 蠕虫事件使其更为关注其工业控制系统产品的安全性问题，在 2013 年与其相关的工业控制系统公开漏洞依然处于快速增长的势头。

（3） 部分工业控制系统厂商因市场影响力不足，不再作为漏洞挖掘分析人员的分析目标。

（4） 同时部分涉及关键行业系统的脆弱性（漏洞）信息被限制公开以及地下交易的影响，可能有许多新发现的系统漏洞被雪藏了，而没有公开发布出来。

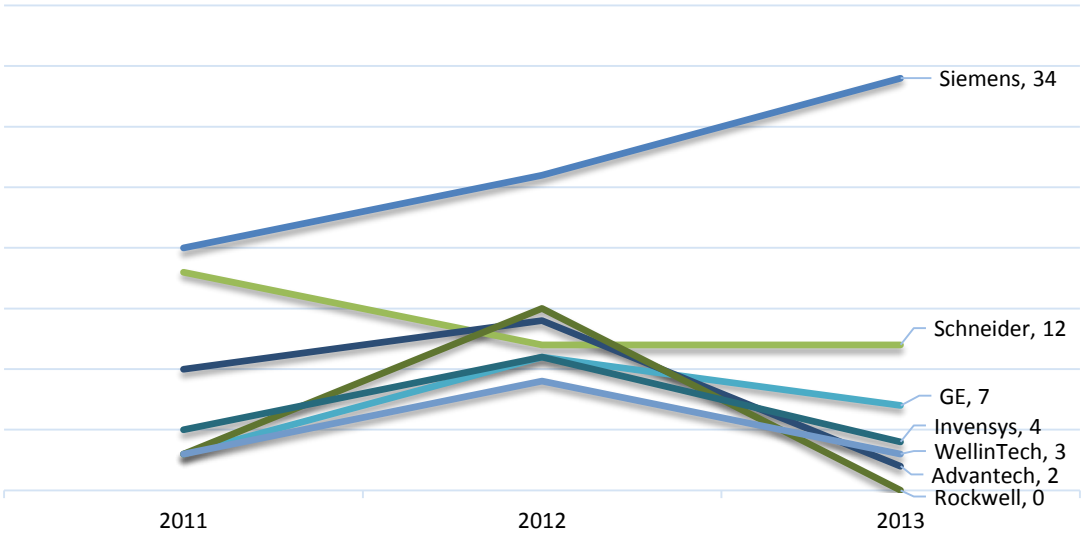

图 2.3　主要工业控制系统厂商[①]相关的公开漏洞的趋势

2.1.2 公开漏洞所涉及工业控制系统厂商的情况分析

通过对漏洞的统计分析，图 2-4、图 2-5 给出了公开漏洞所涉及的主要工业控制系统厂商及各厂商的系统中所发现漏洞及其占漏洞库中所有漏洞的比例。

分析结果表明，公开漏洞所涉及的工业控制系统厂商主要是国际著名的工业控制系统厂商。但国内也有两家工业控制系统厂商进入到了前十的行列，其中北京亚控科技发展有限公司（亚控科技，WellinTech）公布有 17 个漏洞，其中被 CVE 收录 14 个，北京三维力控科技有限公司（力控科技，Sunway）搜集到 11 个相关漏洞，其中被 CVE 收录 2 个。虽然图 2.4、图 2.5 反映的是这些公司产品的脆弱性问题，但这些数据也很可能与这些公司产品的市场排名有较大的联系。

需要说明的是：各厂商产品的漏洞数量不仅与产品自身的安全性有关，而且也和厂商的产品数量、产品的复杂度、受研究者关注程度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。

[①] 这里列出了被 CVE 收录漏洞总数排名前五的工业控制系统厂商（其中 Rockwell 与 Invensys 并列第五）以及国内工业控制系统厂商 WellinTech（亚控科技）近 3 年被 CVE 所收录漏洞数的变化趋势

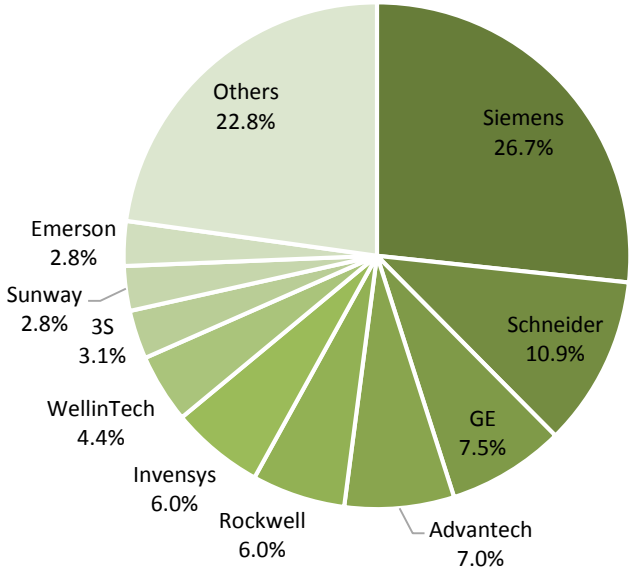

图 2.4　公开漏洞所涉及到的主要工业控制系统厂商（Top10）

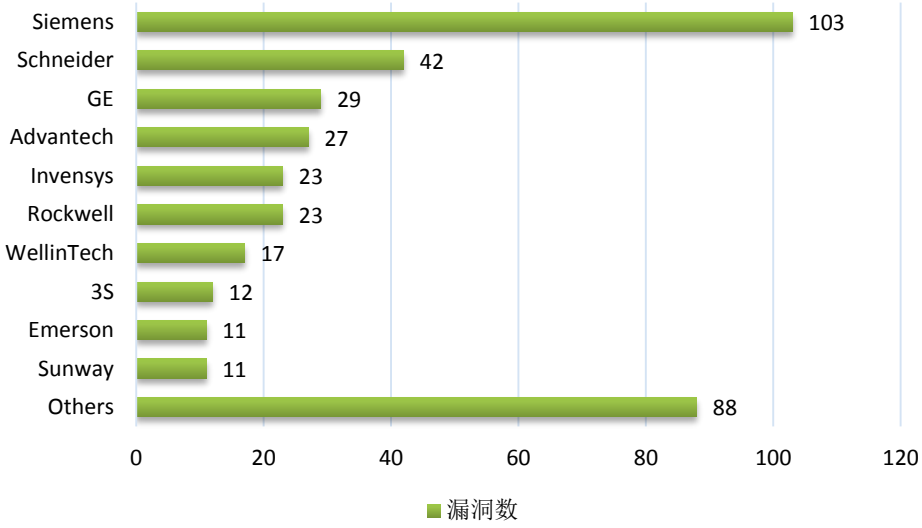

图 2.5　公开漏洞所及到的主要工业控制系统厂商（漏洞数 Top10）

由图 2.6 可知，自 2011 年以来，新增公开漏洞所涉及到的工业控制系统厂商数呈逐步减少的趋势，而且在 2013 年减少明显，仅涉及 12 家工业控制系统厂商。2013 年的新增漏洞则主要集中在西门子（Siemens）、施耐德电气（Schneider Electric）、通用

电气（GE）、爱默生（Emerson）等国际著名厂商的系统中（图 2.7、图 2.8 所示）。其中西门子以年度新增 37 个公开漏洞（47.4%）居于首位，施耐德电气也以年度新增 12 个公开漏洞（15.4%）占据第二的位置。

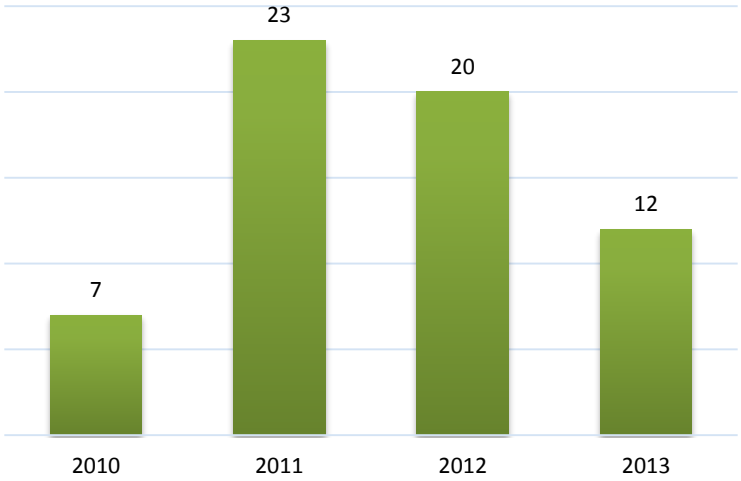

图 2.6　公开漏洞涉及到的工业控制系统厂商的数目变化趋势

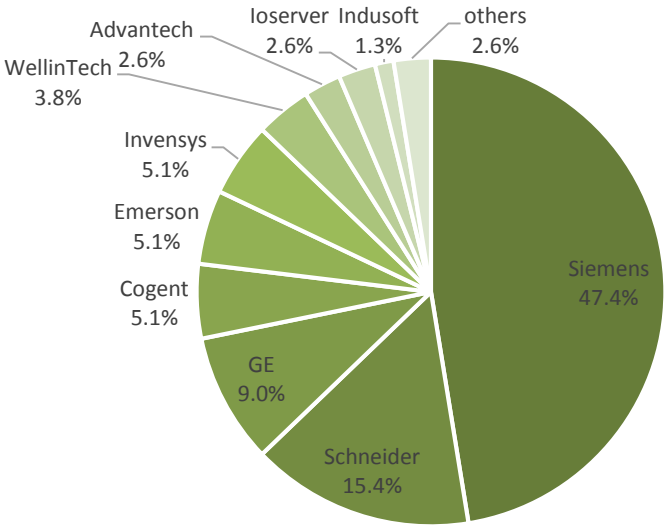

图 2.7　2013 年新增工业控制系统漏洞所涉及到的主要厂商

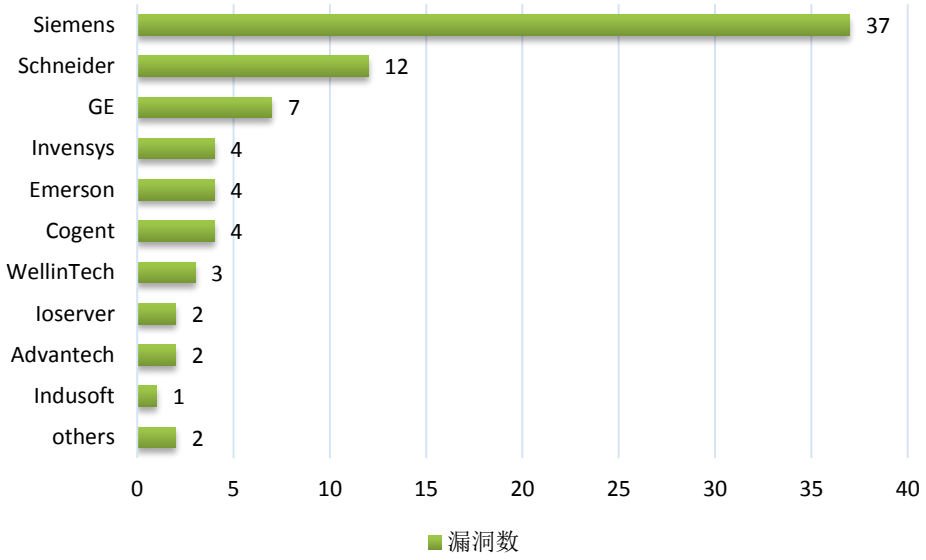

图 2.8　2013 年主要工业控制系统厂商的新增漏洞数

显然，在 2013 年度西门子（Siemens）、施耐德电气（Schneider Electric）、通用电气（GE）等公司的新增漏洞占比（图 2.7 中的 47.4%、15.4%、9%）相对于图 2.4 中的占比（26.7%、10.9%、7.5%）情况增幅明显；这说明公开漏洞所涉及厂商的范围越来越集中。发生这种新增漏洞涉及到的厂商数明显减少且多集中到几大著名的国际大公司情况的主要原因可能是：

（1） 著名公司产品的市场份额大、受到攻击后影响力大，更易引起攻击者、用户、监管者等各方面的重视，漏洞挖掘及分析者投入分析的动力较大；

（2） 企业并购造成被关注的工业控制系统厂商减少，例如施耐德电气并购 7-Technologies、CitectScada 等多家工业控制系统厂商；

（3） 西门子等优势厂商也在积极完善自己的产品系统，并加强对产品的脆弱性进行分析研究[①]。

此外，还可能是因安全事件受控，一些重要行业系统供应商的漏洞信息被屏蔽掉了。

[①] 工业控制系统的专业性知识壁垒，使的系统的相关脆弱性（漏洞）也需要工业控制系统厂商亲自来解决。

2.1.3 2013 年新增漏洞严重程度分析

因本文收集处理的公开漏洞基本上都被 CVE 所收录， 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[①]来判断，并划分为高、中、低三种情况。

根据图 2.9 的统计分析，2013 年的新增漏洞中高危漏洞超过一半（54%）。

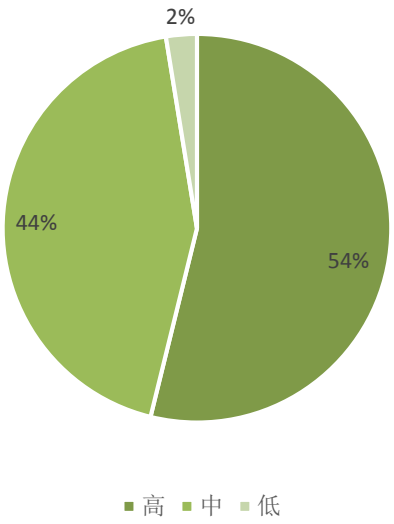

图 2.9 2013 年收录的新增漏洞按严重程度的分类情况

[①] CVSS:Common Vulnerability Scoring System，即“通用漏洞评分系统”，这是一个“行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。
通常 CVSS 同 CVE 一同由美国国家漏洞库（NVD）发布并保持数据的更新。

2.2 工业控制系统脆弱性的检测及防护建议

通过上述分析，我们可以看到工业控制系统自身的脆弱性问题正在越来越多的被工业控制系统厂商、安全机构等重视起来。因此对工业控制系统脆弱性的安全防护工作也应该尽快得到应有的重视。

对工业控制系统脆弱性的安全防护是一个系统工程，包括从技术到管理各个方面的工作。其中最重要的就是对工业控制系统自身脆弱性问题的检测与发现，只有及时发现工业控制系统存在的脆弱性问题，才能进一步执行相应的安全加固及防护工作。

工业控制系统在建设部署时具有设备单元数量多，物理位置分布广的特点。因此工业控制系统脆弱性检测工作需要专业的检测设备辅助进行。对此我们认为，安全行业厂商和工业控制系统厂商应尽早建立合作机制、建立国家或行业级的漏洞信息分享平台与专业的关于工控系统的攻防研究团队，并尽早开发出适合于工业控制系统使用的脆弱性扫描设备。

适用于工业控制系统的漏洞扫描器和传统的 IT 系统漏洞扫描器相比，除了可以支持对常见的通用操作系统、数据库、应用服务、网络设备进行漏洞检测以外，还应该支持常见的工业控制系统协议，识别工业控制系统设备资产，检测工业控制系统的漏洞与配置隐患（如图 2.10 所示，红线框内标识了工业控制系统漏洞扫描器与工业控制系统相关的功能）。

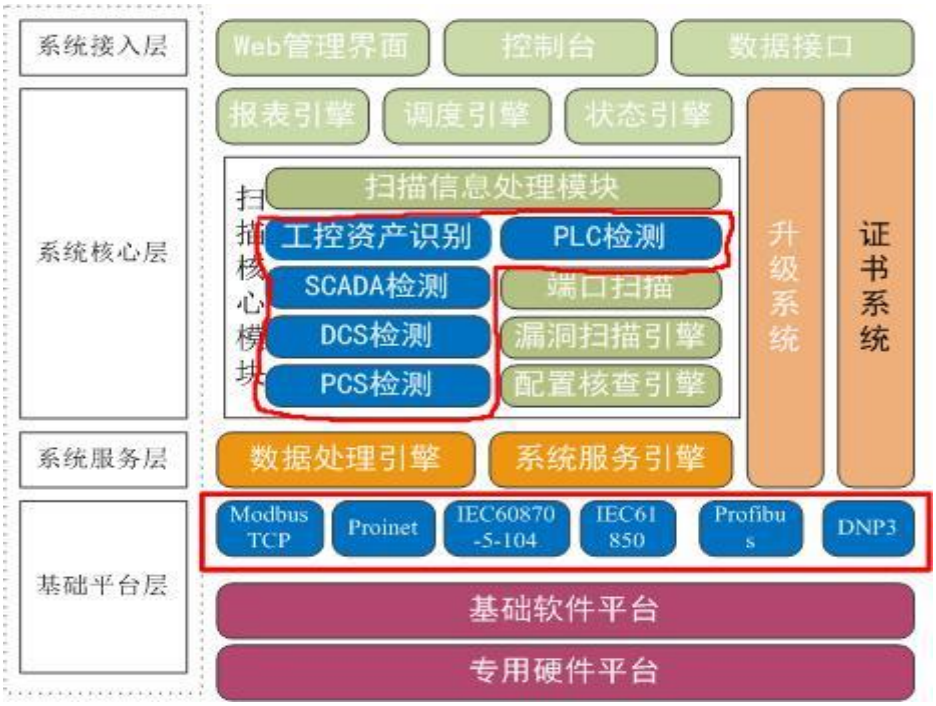

图 2.10　工业控制系统漏洞扫描器的功能示意图

通过使用工业控制系统扫描器，在工业控制系统设备上线前及维护期间进行脆弱性扫描，可以及时发现工业控制系统存在的脆弱性问题，了解工业控制系统自身的安全状况，以便能够及时地提供针对性的安全加固及安全防护措施。因此，工业控制系统脆弱性的检测与发现对完善工业控制系统安全的工作来说至关重要，是需要首先解决的问题之一。

三. 工业控制系统的安全威胁分析

3.1 工业控制系统所面临的安全威胁

根据我们对工业控制系统所涉及到的相关网络的研究，当前的工业控制系统在具体部署时通常涉及到如下几种网络：企业办公网络（简称办公网络）、过程控制与监控网络（简称监控网络）以及现场控制系统网络（如**错误!未找到引用源。**所示）[LYHC2012]。下面我们在简单介绍这三种网络功能的同时，讨论可能存在的部分安全威胁[Tofino]及攻击途径。

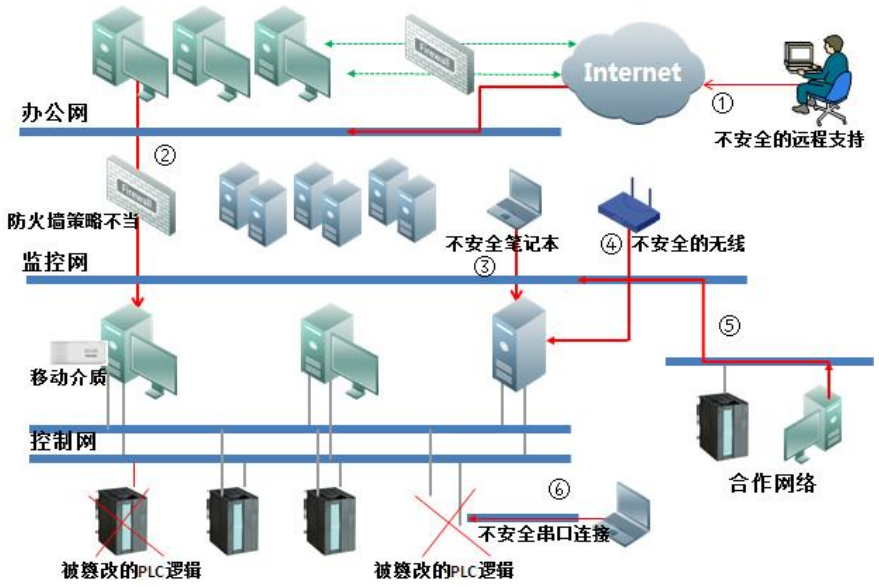

图 3.1 工业控制系统所面临的安全威胁

- **企业办公网络**

主要涉及企业应用，如 ERP、CRM 和 OA 等与企业运营息息相关的系统。

根据风险敏感程度和企业应用场景的不同，企业办公网络可能存在与外部的互联网通信边界；而一旦存在互联网通信，就可能存在来自互联网的安全威胁（比如：不安全的远程支持（图 3.1 中攻击途径①）。这时通常就需要具有较完备的安全边界防护措施，如防火墙、严格的身份认证及准入控制机制等。

另一方面，工业控制系统的监控及采集数据也需要被企业内部的系统或人员访问或处理，这样在企业网络与工业控制系统的监控网络甚至现场网络（总线层）之间存在信息访问路径；但其中由于实时性要求及工业控制系统通信协议私有性的局限，多数情况在这些访问过程并未能实现基本访问控制及认证机制[LYHC2012]，即使在企业办公网与监控网络之间存在物理隔离设备（防火墙、网闸等），但也存在因策略配置不当而被穿透的威胁（图 3.1 中攻击途径②）。

- **过程控制与监控网络**

过程控制与监控网络中主要部署：SCADA 服务器、历史数据库、实时数据库以及人机界面等关键工业控制系统组件。在这个网络中，系统操作人员可以通过 HMI 界面、SCADA 系统及其他远程控制设备，对现场控制系统网络中的远程终端单元（RTU）、现场总线的控制和采集设备（PLC 或者 RTU）的运行状态进行监控、评估、分析；并依据运行状况对 PLC 或 RTU 进行调整或控制。监控网络负责工业控制系统的管控，其重要性不言而喻。对现场设备的远程无线控制、监控网络设备维护工作及需要合作伙伴协同等现实需求，在监控网络中就需要考虑相应的安全威胁：

- 不安全的移动维护设备（比如笔记本、移动 U 盘等）的未授权接入，而造成木马、病毒等恶意代码在网络中的传播（图 3.1 中攻击途径③）
- 监控网络与 RTU/PLC 之间不安全的无线通信，可能被利用攻击工业控制系统（图 3.1 攻击途径④）。在《工业控制系统的安全性研究报告》[LYHC2012]给出了一个典型的利用无线通信进行入侵攻击的攻击场景。
    - 因合作的需要，工业控制网络有可能存在外联的第三方合作网络并且在网络之间存在重要的数据信息交换。虽然这些网络之间存在一定的隔离及访问控制策略，但日新月异的新型攻击技术也可能造成这些防护措施的失效，从而来自合作网络的安全威胁也是不容忽视的。（图 3.1 攻击途径⑤）。

- **控制系统网络：**

控制系统网络利用总线技术(如 PROFIBUS 等)将传感器/计数器等设备与 PLC 以及其他控制器相连，PLC 或者 RTU 可以自行处理一些简单的逻辑程序，不需要主系统的介入即能完成现场的大部分控制功能和数据采集功能，如控制流量和温度或者读取传感器数据，使得信息处理工作实现了现场化。

控制系统网络由于通常处于作业现场，因此环境复杂，部分控制系统网络采用各种接入技术作为现有网络的延伸，如无线和微波，这也将引入一定的安全风险（图 3.1 攻击途径④）。同时 PLC 等现场设备在现场维护时，也可能因不安全的串口连接（比如，缺乏连接认证）或缺乏有效的配置有效性核查，而造成 PLC 设备运行参数被篡改，从而对整个工业控制系统的运行造成危害（例如，伊朗核电站离心机转速参数被篡改造成的危害）。

由于工业控制系统的正常运行甚至会影响到国计民生（诸如电力、石化、市政、交通以及重要的制造业的工业控制系统），其重要性不言而喻。因此他们也必然会成为网络战的重点关注对象，而且目前 APT 等新型、复杂攻击技术的存在，也将使得系统面临的安全威胁日益严重。

3.2 APT 攻击方法与工业控制系统安全

工业控制系统已经成为国家关键基础设施的重要组成部分，工业控制系统的安全关系到国家的战略安全。近年来，针对工业控制系统的攻击，不论是在规模宏大的网络战（Cyberwar），还是在一般的网络犯罪（Cybercrime）中，都可以发现高级持久威胁（Advanced Persistent Threat，简称 APT）的影子。本章通过对新型 APT 攻击方法的梳理和分析，有针对性地为工业控制系统行业提出可行的安全防护建议。

3.2.1 高级持久威胁概述

简单地说，APT 指一个具备相应能力和意图的组织，针对特定实体发起的持续和有效的威胁。

严格来说，APT 能够灵活地组合使用多种新型攻击技术和方法，超越了传统的基于特征签名的安全机制的防御能力，能够长时间针对特定目标进行渗透，并长期潜伏而不被发现，是一种严密组织化的行为，拥有大量的资金支持、优秀的管理能力和大量高端人才。具体来说，应当具备以下三方面的特征[APT]：

高级：威胁背后的操纵者有能力进行全方位的情报收集工作。不仅包括通过计算机入侵获取信息，而且还可以扩展到传统的情报搜集，如电话拦截技术和卫星成像技术。虽然攻击的

个别手段可能无法被归类为特别“先进”，但操纵者通常可以根据需要开发更为先进的工具。他们经常结合多种方法、工具和技术，以保持接触与尝试并最终攻陷目标。

持久：操纵者会执着地进行特定任务，而不是随机地搜索目标。通过持续监测和接触，以实现针对目标的任务。如果操纵者暂时无法取得进展，他们通常会不断地重新尝试，并最终取得成功。操纵者的目的还包括长时间保持对目标的访问权，而不只是取得一次性的攻击机会。

威胁：同时具备了能力和意图。APT 攻击的关键在于协调人的行动，而不是盲目的执行自动化攻击。操纵者持有具体目标和动机，具备足够的技能、严密的组织力和大量的资金。

通常认为，APT 攻击应该包含情报收集、突破防线、建立据点、隐秘横向渗透和完成任务五个阶段（如图 3.2 所示），各阶段的具体任务描述见表 3-1。

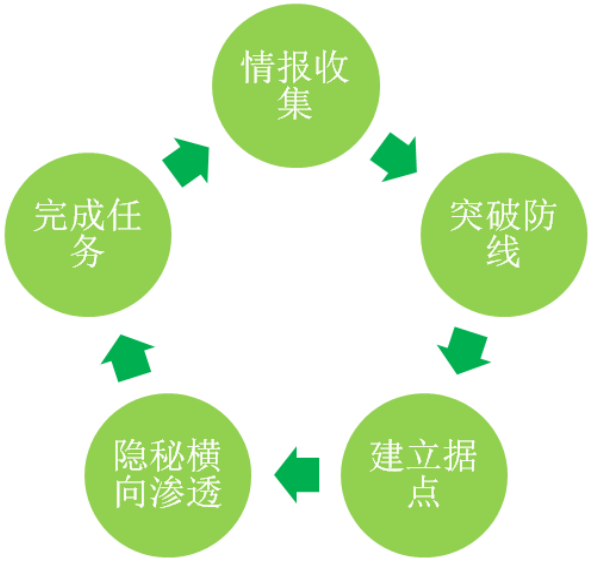

图 3.2　APT 攻击的五个阶段

表 3-1 APT 攻击各阶段的任务描述

阶段名称	任务描述
情报收集	攻击者在社交网站等公开数据源中搜索并锁定特定人员，收集有价值情报并加以研究。
突破防线	收集到足够的情报后，获取第一台受害主机上的代码执行权限。
建立据点	突破防线后，建立 C&C（Command & Control）服务器到第一台受害主机的信道并获取系统的最高权限，将第一个据点变成对内部网络发动后续攻击的前沿阵地。
隐秘横向渗透	在内部网络探测、入侵更多的主机，发掘有价值的资产及数据服务器，并尽可能长时间地避免被发现。
完成任务	设定要完成的任务可能是上传搜集到的敏感信息，或者执行破坏活动。比较高级的 APT 攻击还包括严密的踪迹销毁等撤退策略。

3.2.2 新型 APT 攻击方法分析

鉴于 APT 攻击的对象和目的可能存在差异，不同的 APT 攻击所采用的技术和方法也存在较大的不同；而且随着 APT 攻防的升级，新的攻击技术和方法也会不断涌现。根据对大量 APT 攻击事件的跟踪和分析，我们发现：虽然 APT 攻击具有明显的定制化特征，但是一般来说，所使用技术和方法的差异主要出现在“突破防线”和“完成任务”两个阶段。本节首先枚举影响较大或者具有显著特征的 APT 事件，然后归纳出若干我们认为应该引起业界重点关注的新攻击技术和方法。

3.2.2.1 APT 攻击事件

自 2010 年 APT 出现在公众视野之后，安全业界已经陆续报道了数十起 APT 攻击事件，图 3.3 中部分枚举了其中影响较大或具有较明显新型攻击方法和特征的事件，这些事件的详情参见表 3-2。

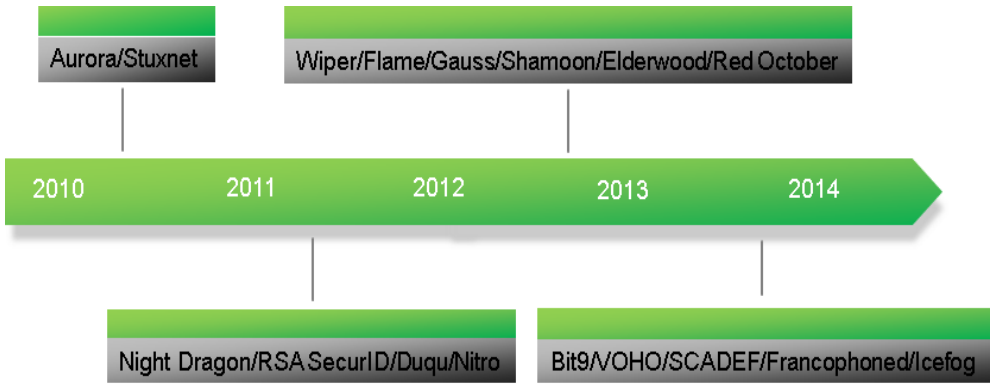

图 3.3 2010 年以来重要 APT 事件

表 3-2 重要 APT 攻击事件的特征枚举

时间	名称	目标	重要影响或者显著特征
2010-1	Aurora	Google 等 20 多家 IT 公司	1、水坑攻击，利用 IE 漏洞 MS010-002 得到执行 2、利用 SSL 加密隧道传输数据 3、窃取 GMAIL 邮件账户和内容
2010-6	Stuxnet	中东能源行业	1、使用可移动存储实现摆渡攻击 2、用 5 个微软漏洞（包括 4 个零日）：MS10-046，MS10-061，两个未公开的提权，MS08-067 3、使用 Realtek、JMicron 公司的数字签名 4、攻击物理设备
2011-2	Night Dragon	全球石油天然气和石化公司	1、利用 SQL 注入突破防线 2、利用鱼叉式钓鱼邮件进行隐秘横向渗透 3、禁用受害主机的 IE 代理，建立直连通道
2011-3	RSA SecurID	RSA 公司	1、使用 Adobe Flash 的零日漏洞（CVE-2011-0609） 2、主动撤离并清除痕迹 3、窃取 SecurID 技术及客户资料
2011-9	Duqu	中东和欧洲能源行业	1、大量重用 Stuxnet 的代码 2、利用微软零日漏洞：MS11-087 3、使用 C-Media 公司的数字签名
2011-10	Nitro	全球化工行业	1、加密窃取的数据
2012-4	Wiper	中东能源行业	1、彻底自我销毁，目前未发现有效样本
2012-5	Flame	中东能源行业	1、创建屏幕快照 2、使用麦克风收集声音信息 3、通过 SSH 和 HTTPS 建立安全连接 4、加密压缩窃取的数据，使用 5 种加密算法（不包括变种），3 种数据压缩技术
2012-6	Gauss	黎巴嫩、以色列、巴勒斯坦	1、Flame 变种 2、银行、社交网络、email、以及即时通信账号和密码
2012-8	Shamoon	中东能源行业	1、擦写硬盘数据和主引导记录

2012-9	Elderwood	国防相关的供应链制造商、IT 服务提供商、非政府组织	1、专业提供 APT 攻击服务的组织操作 2、使用大量零日漏洞：CVE-2012-0779，CVE-2012-1875，CVE-2012-1889，CVE-2012-1535，CVE-2011-0609，CVE-2011-0611，CVE-2011-2110，CVE-2010-0249 3、供应链攻击 4、单漏洞多水坑
2012-10	Red October	东欧、前苏联、西欧、北非	1、能够从智能手机窃取数据 2、篡改网络设备（Cisco）配置 3、窃取可移动存储设备数据（甚至包括数据恢复算法窃取已经删除的数据） 4、使用大量已公开文件解析漏洞 5、窃取大量 email 内容
2013-2	Bit9	Bit9	1、专业提供 APT 攻击服务的组织操作 2、利用 SQL 注入突破 Bit9 防线 3、窃取 Bit9 数字证书
2013-2	VOHO	Bit9 客户	1、专业提供 APT 攻击服务的组织操作 2、最大规模水坑，10 多个合法网站被挂马，利用 IE 零日漏洞 MS12-043，JAVA 零日漏洞 CVE-2012-1723 3、供应链攻击（安全服务供应商 Bit9）
2013-2	SCADEF	美国军方的供应链厂商	1、专业提供 APT 攻击服务的组织操作 2、固件后门 3、供应链攻击（零部件供应商）
2013-4	Francophoned	法国	1、鱼叉式钓鱼邮件后，紧接着使用电话社工
2013-9	Icefog	日本、韩国	1、使用地域性文档格式作为载体 2、使用直接受攻击者控制的交互式工具，而不是完全自动化的工具 3、使用匿名网络 4、针对 Windows 和 Mac OS X

注 1：由于 APT 攻击持续的时间一般较长，其开始时间往往是不可考证的，本文使用的时间统一按照事件被报道的时间。

注 2：Bit9 提供基于信任的安全平台，融合基于云的信誉服务和策略驱动的应用控制及白名单机制，故对于恶意第三方来说，成功安装不可信应用极其困难。攻击者针对 Bit9 客户的攻击被 Bit9 的安全模型阻断后，转而攻击 Bit9，并窃取大量数字签名，然后继续对 Bit9 客户进行攻击。

3.2.2.2 突破防线

一般来说，攻击者突破防线的常用技术包括：水坑+网站挂马，鱼叉式钓鱼邮件+客户端漏洞利用、网站挂马+URL 社工、服务端漏洞利用等。

（1） **水坑+网站挂马** 攻击者收集潜在受害者经常访问的网站（水坑），并寻找这些网站中存在漏洞（攻击者自己发现漏洞或通过黑市购买漏洞）；通过存储型 XSS 漏洞在这些网站上植入恶意代码；等待潜在受害者使用包含漏洞的 Web 客户端（例如 IE 浏览器）访问植入了恶意代码的网页。

（2） **鱼叉式钓鱼邮件+客户端漏洞利用** 根据潜在受害者的行业和爱好，攻击者直接向受害者发送其可能感兴趣的电子邮件（电子邮件社工），这些电子邮件会包含植入了恶意代码的附件；一旦潜在受害者使用关联的客户端工具（包含漏洞）打开了恶意附件，则攻击者就可以利用客户端漏洞轻易突破防线。

（3） **网站挂马+URL 社工** 攻击者首先在包含存储型 XSS 漏洞的某些知名网站上植入恶意代码；然后将包含恶意代码的 URL 通过即时通讯/电子邮件等方式发送给潜在受害者（URL 社工）；一旦潜在受害者使用包含漏洞的 Web 客户端（例如 IE 浏览器）打开包含恶意代码的 URL，则攻击者就可以利用客户端漏洞轻易突破防线。

（4） **服务端漏洞利用** 攻击者利用目标网络所提供的服务中存在的 SQL 注入、远程溢出等漏洞，直接进入目标网络。鉴于目前网络上已经或正在部署大量的安全防护设备，服务端漏洞利用的难度越来越大，因此这种直接的方式会逐渐减少。

从近几年的 APT 攻击事件上来看，上述技术仍能很好地工作，因此攻击者并不急于采用大量更新奇的攻击技术，而更多的是在这些技术的使用策略和方法上下功夫。目前，能够看到的新攻击策略和方法主要有以下几个方面：

（1） **单漏洞多水坑** 攻击者使用一个漏洞攻占一个网站后，并不急于立即使用该网站发起攻击，而是在攻占多个网站后，集中地发起对多个目标的攻击。攻击者采用这种策略可能有两方面原因：一是攻击者为了提高漏洞的利用效率，减少开销；另一个可能是不同的攻击者之间交换漏洞信息，增加可用漏洞储备。更多细节，参考 VOHO[HL]和 Elderwood[EW]。

（2） **更激进的鱼叉式钓鱼** 攻击者不仅发送鱼叉式钓鱼邮件，而且紧接着会使用电话等途径对潜在的受害者实施进一步的社工。更多细节，参考 Francophoned[FP]。

（3） **供应链攻击** 生产力的发展促进社会分工的细化，当前极少有一个组织或者行业能做到完全不依赖于外部环境。虽然最终目标的防护可能非常坚固，但是却不能保证其供应链上的每一个合作伙伴都能达到同样的标准。

更多细节，参考 Elderwood[EW]、VOHO[HL]和 SCADEF[HL]。

3.2.2.3 完成任务

根据任务的性质不同，完成任务所使用的技术之间必定存在较大的差异。一般来说，信息窃取任务中使用的主要技术可能包括：网络窃听（通过网络嗅探截获网络上传输的账户登录信息）、击键记录（通过文件过滤驱动窃取用户输入的账户登录信息）、信息过滤（扫描受害主机磁盘，寻找具有特定扩展名或者内容的文件）等；而破坏性任务中使用的主要技术表现为对 PLC 设备的物理攻击。

目前，虽然信息窃取任务占据绝对的主流，但是绝不能排除破坏性任务增多的可能性。相反，作为信息窃取的一个合乎逻辑的扩展，修改或破坏数据，甚至造成物理基础设施或设备损坏的攻击在未来几年可能会急剧增多。

从最近几年被公开报道的 APT 攻击事件上来看，攻击者在完成其 APT 攻击任务中已经采用的新技术主要有以下几个方面：

（1） **屏幕记录** 某些特定的敏感信息可能不方便使用简单的文档方式记录，例如发现受害主机中特定进程或者窗口激活情况的信息（这些信息能够为特定资产识别和进一步攻击提供帮助），可以通过创建一系列用户屏幕快照实现收集。更多细节，参考 Flame[FL]。

（2） **交互式操作** 攻击者更多地使用交互式工具，而不是完全自动化的工具，来实施信息过滤，确保更隐蔽同时更精确的外科手术式信息窃取。更多细节，参考 Icefog[IF]。

（3） **加密通信** 通过加密网络协议建立与 C&C 服务器之间的加密连接，躲避常规的基于特征签名的安全机制。更多细节，参考 Flame[FL]等。

（4） **匿名网络** 通过 Tor 等匿名网络（该网络使用一种称为洋葱路由的技术实现匿名机制），隐藏 C&C 服务器的位置，增加追查的难度。更多细节，参考 Icefog[IF]等。

（5） **声波通信** 使用受害主机上附带的麦克风设备记录周围环境中的声波（除了 Stuxnet 中使用可移动存储实现摆渡攻击外，通过声卡或其它计算机自带物理设备实现摆渡攻击很可能也已经出现了）。更多细节，参考 Flame[FL]。

（6） **清除痕迹** 某些特定的 APT 攻击会使用附加的模块执行精心设计的清除痕迹子任务，例如彻底擦除（基本上无法恢复）攻击存在的蛛丝马迹（包括彻底清除擦写模块自身存在的证据），或者大规模恶意擦写受害主机上的文件。更多细节，参考 Wiper[WP]、Shamoon[SM]和 RSA SecurID。

3.2.3 工业控制系统攻击中的 APT

针对工业控制系统的攻击，不论在规模宏大的网络战（Cyberwar），还是在一般的网络犯罪（Cybercrime）中，都可以发现 APT 的影子。

3.2.3.1 网络战中的 APT——Stuxnet

2010 年 6 月，白俄罗斯 VirusBlokAda 公司发现了一种复杂的恶意程序——Stuxnet[Stuxnet1][Stuxnet2]。2010 年 9 月 26 日，伊朗媒体报道，伊朗在建的布什尔核电站遭到 Stuxnet 病毒的攻击。这种病毒以核燃料离心机为目标，而伊朗几乎每一个核燃料提纯设备中都使用了这种离心机。最后 Stuxnet 感染了全球超过 45000 个网络，其中伊朗遭到的攻击最为严重。

根据微软安全漏洞公告和西门子向外界公开的报告，Stuxnet 利用了微软 Windows 操作系统中的 5 个漏洞（其中包括 MS10-046、MS10-061 两个零日漏洞和另两个尚未修复的提权漏洞），以及西门子工业控制系统的 2 个漏洞，并盗用了 Realtek 和 JMicron 公司的多个数字签名，可通过移动存储设备（例如 U 盘）和局域网传播。

（1）首先感染可移动存储设备对物理隔离网络实现“摆渡”攻击；

（2）然后利用快捷方式文件解析漏洞（MS10-046），传播到内部网络；

（3）在内部网络中，通过快捷方式解析漏洞（MS10-046）、打印机后台程序服务漏洞（MS10-061）、RPC 远程执行漏洞（MS08-067），寻找安装了 WinCC 软件的主机，并探测计算机是否连接一种由西门子公司制造、广泛用于铀浓缩设施（离心机）的可编程序控制器；

（4）最后，寻找一个特别型号的“变频转换器”，并对其数据进行修改，使该设备转速降低，从而无法生成浓缩铀，而这种突然的降速会造成硬件的永久损坏。

这次事件促使西门子（Siemens）加大了对其工业控制系统产品安全性的重视程度，这也是现在西门子提供的工业控制系统相关漏洞数目偏多的原因。

3.2.3.2 网络犯罪中的 APT——Nitro

2011 年 10 月底，赛门铁克公司发布的一份报告公开了主要针对全球化工企业进行信息窃取的 Nitro 攻击[Nitro]。从该攻击的操作过程也可以发现非常典型的 APT 特征：

（1） 首先受害企业的部分雇员收到带有欺骗性的鱼叉式钓鱼邮件，当其中一个受害人阅读邮件的时候，看到一个把文件名和图标伪装成类似文本文件形式的恶意可执行程序附件（该附件也可能是一个有密码保护的压缩文件，密码在邮件中注明，解压后也会产生一个可执行程序）；

（2） 该受害人执行了附件中的可执行程序后，被植入 Poison Ivy 后门程序，并通过 TCP 80 端口与 C&C 服务器进行加密通讯，将受害人的电脑上的帐号相关的文件信息上传；

（3） 然后攻击者借助事先植入的木马在受害企业的网络寻找目标、伺机行动、不断收集企业的敏感信息；

（4） 所有的敏感信息会加密存储在内部网络中的一台临时服务器上，并最终上传到公司外部的某个服务器上，从而完成攻击。

3.3 工业控制系统的安全防护建议

综合上述分析，工业控制系统不仅因其开发及应用时缺乏足够的安全性考虑，使得工业控制系统中存在不少危及系统安全的漏洞或不安全的配置；而且因为很多行业（诸如电力、石化、市政、交通、重要制造业等）的工业控制系统能否正常运行，甚至会影响到国计民生，其重要性不言而喻。因此，它们也必然会成为网络战的重点关注对象。淡薄的安全意识、脆弱的安全防护能力，在当前各种新型、复杂攻击技术（APT）面前，这些工业控制系统所面临的安全威胁将不言而喻。

这里我们期望在上文讨论工业控制系统自身脆弱性及其所面临的各种安全威胁的基础上，结合我们以往的一些工业控制系统安全项目的实践经验，给出一些关于工业控制系统的安全防护策略及建议，并针对 APT 攻击的检测与防护方法进行讨论。

3.3.1 工业控制系统的安全防护策略及建议

为保障工业控制系统的安全运行，除提供工业控制系统传统必备的功能安全之外，我们还必需加强工业控制系统的信息安全防护能力。针对工业控制系统的业务特点、自身脆弱性以及所可能面临的各种网络安全威胁，需要我们在工业控制系统的安全体系架构设计、工业控制系统的供应链安全、工业控制系统上线前安全检查、工业控制系统的安全运维与管理等方面进行综合、全面地考虑。

- 工业控制系统的安全体系架构设计

应把信息安全融入到工业控制系统的整体设计之中，在综合考虑工业控制系统的业务重要性、数据机密性、潜在的安全威胁、人员安全管理规范以及相关的技术标准等多种因素的基础上，划分不同的工业控制系统安全域、明确相应的信息安全责任人及其职责。不同的安全域应根据安全域内系统重要性的差异而采用不同级别的安全防护策略及人员安全管理的制度、规范。在安全域之间，可通过工业防火墙、隔离网闸等网关类安全设备实现工业控制系统与其他信息系统间的有效隔离，并通过系统准入控制机制，确保系统访问者的可信身份及使用设备的安全性，并通过严格的访问控制策略及操作行为的监管与审计机制确保安全域间信息交换的安全性。

“道高一尺，魔高一丈”，工业控制系统所面临的安全威胁也在不断地变化之中，自然其安全防护体系也必须与时俱进、及时优化。对此，可通过安全的供应链管理选择安全可信的系统（或设备），加强上线前对系统（或设备）的安全检测、脆弱性评估与安全加固、运维时的实时异常行为检测、审计以及通过定期或不定期的安全风险评估对安全防护策略持续优化的动态过程，形成一套基于工业控制系统全生命周期的安全管控体系。

- 工业控制系统的供应链安全

应将工业控制系统的供应链安全作为工业控制系统信息安全防护体系的组成部分，以防工业控制系统及其组件遭受因供应链安全所造成威胁。

工业控制系统或系统组件在采购时，在采购合同中应明确描述系统的预期运行环境、开发环境、厂商资格及验收标准，并提出系统的安全功能、安全增强、安全保障及安全文档需求。对于重要行业的工业控制系统及其组件的采购必要时可指定系统开发商的选择范围。

- 工业控制系统上线前的安全检查

工业控制系统、系统组件或设备在上线运行前，应使用专门的工具（或通过第三方测评机构）对其中可能存在的安全隐患进行相应的安全检测（包括但不限于漏洞扫描、配置核查、脆弱性评估以及后门探测等）；期望通过上线前安全检测能够及时地发现潜在的安全隐患，进而通过系统加固、优化安全配置及安全防护策略等手段尽可能避免因工业控制系统（系统组件或设备）自身的脆弱性所带来的安全威胁。

从工业控制系统上线前的安全检查开始，把信息安全融入到正常的验收体系中，除了功能性安全验收外，信息安全验收也要作为工业控制系统（系统组件或设备）能否正常上线的一个重要评估依据。

- 工业控制系统的安全运维与管理

在工业控制系统的日常运行阶段，应建立相应的人员安全管理制度及安全意识培训机制，明确系统操作、管理人员的职责及授权，建立相关人员的操作行为监管及审计机制。通过制度、管理和技术手段来规范系统相关人员的系统操作行为。

对在线运行的系统（或设备），根据系统（或设备）的实际情况可通过对系统操作行为的审计及合规性检测提高对未知威胁的检测与发现能力；并可通过定期、不定期（或在系统检修时）的安全检测及风险评估，尽早发现系统中潜在的安全风险，进而通过安全防护策略优化、工业控制系统的安全整改实现整个工业控制系统防护能力的提升。

3.3.2 APT 攻击的检测与防护方法

针对上一节归纳出的若干我们认为应该引起业界重点关注的新攻击技术和方法，本节提出相应的防护建议和更进一步的思考。

针对 APT 逐步渗透攻击的特点，我们提出了一个针对工控 APT 攻击的检测与防护方案（如图 3.4 所示），针对 APT 攻击的五个阶段分别讨论了相应的应对策略。

应对策略	建议方法与工具
防范社会工程攻击	安全意识培训
全方位抵御水坑攻击	WEB 漏洞扫描器
工控系统组件漏洞及后门的检测与防护	工控漏洞扫描器 高级威胁检测工具
阻断C&C通道	网络入侵防护系统
异常行为发现	工控审计系统 异常行为检测
异常行为发现	工控审计系统 异常行为检测

图 3.4 针对工业控制系统的 APT 攻击的检测与防护方案

（1） **全方位抵御水坑攻击** 基于“水坑+网站挂马方式”的突破防线技术愈演愈烈，并出现了单漏洞多水坑的新攻击方法。针对这种趋势，一方面寄希望于网站管理员重视并做好网站漏洞检测和挂马检测；另一方面要求用户（尤其是能接触到工业控制设备的雇员）尽量使用相对较安全的 Web 浏览器，及时安装安全补丁，最好能够部署成熟的主机入侵防御系统。

（2） **防范社会工程攻击、阻断 C&C 通道** 在工业控制系统运行的各个环节和参与者中，人往往是其中最薄弱的环节，故非常有必要通过周期性的安全培训课程努力提高员工的安全意识。另外，也应该加强从技术上阻断攻击者通过社会工程突破防线后建立 C&C 通道的行为，建议部署值得信赖的网络入侵防御系统。

（3） **工业控制系统组件漏洞与后门检测与防护**

工业控制系统行业使用的任何工业控制系统组件均应假定为不安全或存在恶意的，上线前必需经过严格的漏洞、后门检测以及配置核查，尽可能避免工业控制系统中存在

的各种已知或未知的安全缺陷。其中针对未知安全缺陷（后门或系统未声明功能）的检测相对困难，目前多采用系统代码的静态分析方法或基于系统虚拟执行的动态分析方法相结合的方式[①]。

（4） **异常行为的检测与审计**

上述列举出的 APT 突破防线和完成任务阶段采用的各种新技术和方法，以及其他已经出现或者即将出现的新技术和方法，直观上均表现为一种异常行为。建议部署工控审计系统，全面采集工业控制系统相关网络设备的原始流量以及各终端和服务器上的日志；结合基于行为的业务审计模型对采集到的信息进行综合分析，识别发现业务中可能存在的异常流量与异常操作行为，发现 APT 攻击的一些蛛丝马迹，甚至可能还原整个 APT 攻击场景。

鉴于工业控制系统业务场景比较稳定、操作行为比较规范的实际情况，在实施异常行为审计的同时，也可以考虑引入基于白环境的异常检测模型[LHP2013]，对工业控制系统中的异常操作行为进行实时检测与发现。

[①]绿盟科技的威胁分析系统（NSFOCUS TAC）[NS2013]，通过基于虚拟执行技术的动态解码能力，使得 TAC 可检测多态 Shellcode、防范零日漏洞攻击，并通过于 NGIPS 等产品的协同提高了识别并防范未知安全威胁的能力。

四. 智能变电站的安全性研究

根据国家电网公司《智能变电站技术导则》，智能变电站是采用先进的传感器、信息、通信、控制、智能等技术，以一次设备参量数字化和标准化、规范化信息平台为基础，实现变电站实时全景监测、自动运行控制、与站外系统协同互动等功能；达到提高变电可靠性、优化资产利用率、减少人工干预、支撑电网安全运行等目标的变电站。其内涵为可靠、经济、兼容、自主、互动、协同，并具有一次设备智能化、信息交换标准化、系统高度集成化、运行控制自动化、保护控制协同化、分析决策在线化等技术特征。

智能化变电站的二次监控、保护系统是基于 DL/T860 标准平台，可实现统一的配置语言、统一建模、组网，共享信息和设备间的互操作性。通常智能变电站可划分为站控层、间隔层、过程层。下面简单介绍各层涉及到的设备及网络情况：

- **站控层设备** 主机兼操作员工作站、一体化平台主机、远动通信设备、智能接口设备、故障录波及网络分析、网络交换机。（其中还有打印机、音响音响告警输出装置）
- **间隔层设备** 间隔层都是 I/O 测控装置。I/O 测控装置具有状态量采集、交流采样及测量、防误闭锁、同期检测、就地断路器紧急操作和单接线状态及数字显示等功能，对全站运行设备的信息进行采集、转换、处理和传送。I/O 测控装置还应配置有 “就地/远方”切换开关。
- **过程层设备** 过程层设备包含智能终端、合并单元及智能一次设备接口等。可完成变电站断路器、隔离开关的信号采集、处理和控制，以及互感器采样值信息的采集和处理。
- **间隔层网络** 通过相关网络设备与本间隔其他设备、其他间隔设备以及站控层设备通信。逻辑功能上，覆盖间隔层内数据交换、间隔层与站控层数据交换、间隔层之间（根据需要） 数据交换，数据交换接口支持 MMS 报文和 GOOSE 报文。同时，间隔层网络与过程层数据交换接口，可传输采样值和 GOOSE 报文。
- **过程层网络** 通过相关网络设备与间隔层设备通信。逻辑功能上，覆盖间隔层与过程层数据交换接口。可传输采样值和 GOOSE 报文。提供（如命令、告警等）快速传输的机制，可用于跳闸和故障录波启动等。智能变电站的系统架构如图 4.1 所示[wxp2013]：

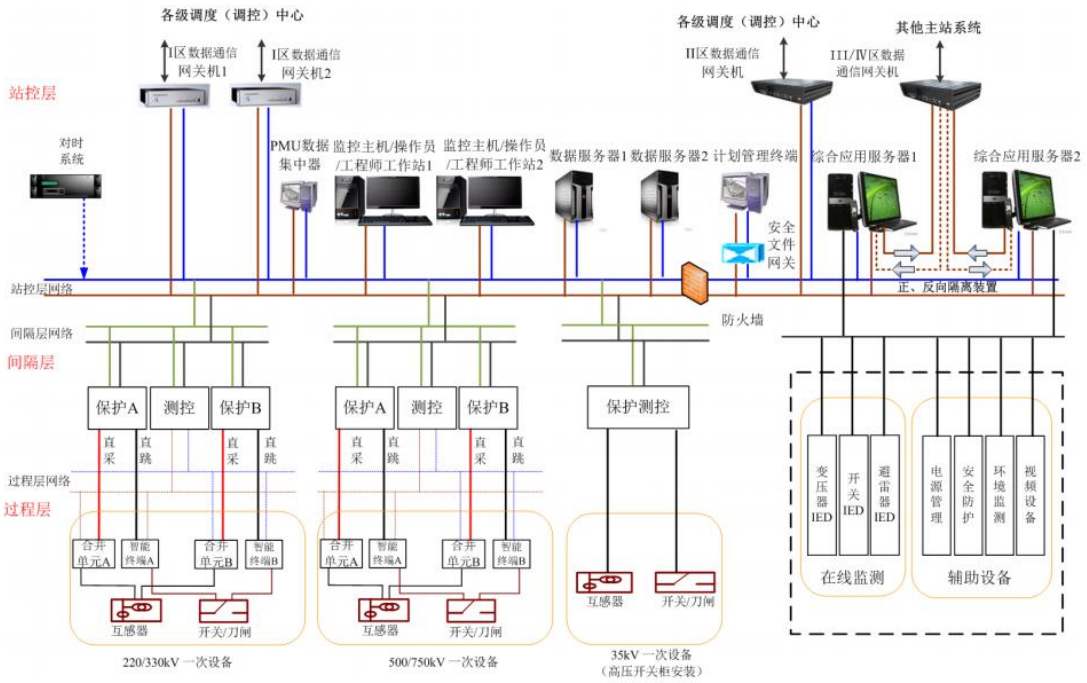

图 4.1　智能变电站的系统架构图

4.1 变电站的安全性分析

本节我们将重点从人员管理与制度流程的规范性、系统软硬件安全性、网络通信安全以及系统操作的合规性等几个方面讨论智能变电站所存在的安全问题。

4.1.1 制度和流程

智能变电站作为智能电网的核心节点，其重要性不言而喻。为维护其正常安全的运行，相关的人员操作和系统维护工作必须遵循严格的安全操作规范、工作流程以及安全管理制度。但通过我们的调研分析，现实情况中依然存在不少安全问题，如表 4-1 所示：

表 4-1 智能变电站安全管理制度及流程方面的安全问题

安全问题	描述
缺乏完善的安全制度与流程文件	由于安全制度缺乏或不完善，没有具体安全要求，造成安全制度难以执行，无法对相关人员提出明确的安全管理要求。智能变电站设备的操作日志记录及合规性审查机制缺失或虽有制度但得不到落实。
缺乏正式的安全意识教育及安全技术培训	将使智能变电站的安全管理人员难以及时地掌握最新的安全防护技术、安全产品及最佳安全实践，难以提升防范新型入侵攻击的能力。
智能变电站安全操作规范或设备使用手册缺失	这些设备操作规范和使用手册是智能变电站安全运行操作、系统配置管理以及故障排除的重要参考文档，应妥善管理并保持随时可用。
没有明确的业务连续性计划或灾难恢复计划	应当制定业务连续性计划或灾难恢复计划并进行定期演练，尽可能避免因系统软、硬件故障的发生，而造成供电中断等安全事故。
没有明确的配置变更管理流程	配置变更管理流程的缺失将导致因不安全新系统部件的引入而造成的系统安全脆弱性，进而增大智能变电站的安全风险。 因此，应制定严格的智能变电站相关硬件、固件、软件的变更管理工作流程，通过系统变更后的安全评估制定相应的安全防护计划，以保证智能变电站得到实时保护。
没有明确的上线前或系统变更时的安全风险评估规范	新系统在上线时多缺乏严格的安全性评估。新系统自身的脆弱性或被故意植入的后门将为后续系统的正常运行带来很大的安全隐患。

4.1.2 系统软硬件

因智能变电站相关软硬件在设计开发时重点关注系统功能的实现，而对安全性及相应的防护能力考虑不足，从而存在较多的安全脆弱性问题，本节将从配置管理、硬件、软件等角度讨论智能变电站系统所面临的一些安全问题。具体分析见表 4-2、表 4-3、表 4-4。

表 4-2 配置管理相关的安全问题

安全问题	描述
安全漏洞被发现后供应商不能及时发布相应的补丁程序	工业控制系统提供商难以及时发布针对漏洞的补丁程序，同时由于工业控制系统使用范围广，数量庞大，用户难以快速准确掌握系统存在漏洞的具体情况，导致用户难以及时加固系统、提升系统的安全性[①]。
使用缺省配置	使用缺省配置可能导致不安全（或不必要）的端口（或服务）没有关闭，甚至缺省帐户、缺省密码的存在。同时由于工业控制系统数量庞大，需关注的配置项目较多，导致用户无法快速准确掌握系统存在配置隐患的具体情况，无法及时修补，这都将为系统带来极大的安全风险。
缺乏系统关键配置信息的维护管理措施	应明确如何对智能变电站系统的配置信息进行安全管理，以防因偶然事故的发生、黑客对配置文件的篡改，而造成业务中断或数据的丢失。
密码管理不当	可导致未授权的系统访问，具体的密码管理不当问题主要涉及： ● 没有制定明确的密码管理策略（包括密码强度、更改周期等）； ● 智能变电站系统的开机、帐户登陆或屏幕保护程序等未按要求设置足够强度的访问密码，甚至未设置密码； ● 密码因保存不当造成泄漏，比如，在系统上张贴系统登录密码、共享帐户密码、通过不安全的通信线路发送明文密码等； ● 密码不按要求及时变更，增大被猜测破解的可能； 等等。
访问控制配置不当	可能导致智能变电站系统操作人员无法在紧急情况下采取应急响应措施；若采用缺省配置，系统管理员权限可能过大。[②]

[①]由于智能变电站系统软件及操作系统更新的复杂性，补丁程序的更新必须面对广泛的回归测试，从测试到最终发布之间有较长的漏洞暴露周期。

[②]可基于系统操作人员的职责明确系统角色和相应的访问控制策略，并辅以操作日志审计制度、相关审查及合规性检测机制规范各角色的操作行为。

表 4-3 系统硬件相关的安全问题

安全问题	描述
安全变更时没有进行充分的测试	许多智能变电站的设施，尤其是较小的设施，没有检测设备，业务系统的安全性变更测试必须在现场环境下进行。
对关键设备没有充分的物理保护措施	访问控制中心、现场设备、便携设备及其他智能变电站组件需要被管控。许多远程站点往往没有人员和物理监测控制措施。
未授权用户能够接触设备	智能变电站设备应仅限于指定的系统运维管理人员、得到授权并在陪同下的厂商人员接触。未授权的操作可能导致：数据或硬件的窃取、损毁或擅自变更系统的配置、恶意代码传播以及物理通信连路断开、系统关机等其他故意的破坏性行为。
关键设备没有冗余备份	关键设备没有冗余备份可能导致单点故障发生。
不安全的智能变电站远程访问组件	调制解调器或其他远程访问组件的开启，可使维护工程师和供应商获得远程访问系统的能力的同时，也为潜在攻击者提供了方便之门。应部署安全的授权访问控制机制，以防止未经授权的个人，通过远程访问进入到智能变电站。

表 4-4 系统软件相关的安全问题

安全问题	描述
缺乏对输入数据的有效性验证及出错处理机制	执行操作指令时对输入的数据、参数缺乏有效性检测，这些数据可能因格式不正确、含有非法或其他意外的字段值，而造成系统无法正常执行、甚至崩溃。这是目前工业控制软件中所存在的最广泛的安全问题[DHS2011]。
可导致缓冲区溢出的安全缺陷	黑客可利用这些漏洞来来发起各种攻击，例如，可用于提升其访问系统权限。
可导致拒绝服务攻击的安全缺陷	智能变电站系统服务端可能会受到 DOS 攻击，可导致合法用户不能访问，或系统访问响应延迟。
内置安全防护功能没有开启	产品内置的安全功能通常默认设置为禁用，需要通过配置开启。
常用通信协议缺乏安全机制	智能变电站标准协议 IEC 61850、IEC 60870-5-104 等通常缺乏内置的安全功能[LYHC2012]。多采用明文传输各种管、控信息，易被攻击者窃听。
开启不必要服务	软件系统许多不必要的应用服务或网络服务很少被禁用，可能会被攻击者利用。
专有软件的使用	专有软件的配置管理手册可从软件商那里获得，这些信息可以帮助黑客发起针对性的攻击。

软件配置缺乏有效的认证授权	可导致未授权的软件配置操作，损害系统的正常运行。
缺乏有效的系统操作日志	没有准确的日志记录，就无法追溯安全事件发生的原因。

4.1.3 网络及通信

虽然智能变电站在建设时将按不同的安全域实施系统间的安全隔离和控制，但工业控制网络设备、通信协议自身的脆弱性以及智能变电站网络架构针对安全性考虑不足的问题，智能变电站依然存在很大的安全风险[wxp2012]。表 4-5 讨论了网络及通信方面的安全问题。

表 4-5 网络与通信相关的安全问题

安全问题	描述
网络设备密码长期不修改/甚至一直采用出厂缺省密码	未定期更换密码，可使密码泄露的风险增大，从而系统遭受未授权操作、窃取数据或攻击破坏的可能性也会大大增加。
关键网络设备没有冗余备份措施	关键网络设备没有冗余备份措施可能导致单点故障
用户、数据与设备缺乏有效认证	部分智能变电站协议没有任何级别的身份验证机制[LYHC2012]。用户身份、设备 ID 的真实性以及传输数据（采集到的设备状态信息、下发的控制指令等）的完整性与真实性就难以得到保证。
未安装防火墙或防火墙策略配置不当	防火墙配置不当可能允许不必要的数据传输，允许攻击数据包和恶意软件在网络之间传播，容易监测其他网络上的敏感数据，造成未经授权的系统访问。
未安装防恶意软件工具	可能因移动设备的违规使用或违规外联而引入恶意代码（木马、病毒等）在智能变电站网络中传播，导致系统性能下降、信息泄露，甚至设备被控制或破坏。因此在智能变电站的计算机系统中应安装经过测试验证的防恶意软件工具。
防恶意软件版本或特征码未更新	未更新的防恶意软件版本和脱离系统定义的规则使防恶意软件无法防范新的恶意软件威胁。
防恶意软件安装前未进行广泛的测试	防恶意软件安装前未进行广泛的测试可能会对智能变电站系统正常运转产生影响。

4.1.4 操作合规性

智能变电站所面临的安全威胁除了上述其系统及网络自身脆弱性之外，来自内部人员的故意违规操作、破坏以及来自外部的新型 APT 攻击（参见第三章内容）也将是智能变电站所面临的最大威胁。而这些威胁的消减将依赖于基于异常行为检测、操作合规性审计以及基于沙箱的虚拟执行[NS2013]等多安全机制的综合安全防御体系。表 4-6 讨论了系统操作行为合规性相关的一些安全问题。

表 4-6 操作合规性相关的安全问题

安全问题	描述
缺乏完善的系统安全操作规范	没有明确系统操作角色定义及授权操作规范集，在系统中就无法定义一个系统的合规性操作行为及授权系统访问
缺乏系统操作行为审计系统	没有相应违规操作行为审计系统，难以追踪事故发生的原因和责任人
缺乏针对 APT 等新型攻击技术的安全防护措施	APT 攻击是融合多种攻击技术、利用最新 0-day 漏洞的新型攻击技术，传统的安全防护措施很难识别并防御它。

4.2 虚拟攻击场景分析

4.2.1 背景描述

某智能变电站 A 是 B 国重要制造单位 C 的供电支撑变电站。敌对组织 D 计划干扰重要制造单位 C 生产活动的正常运行，但是直接进去重要制造单位 C 存在较大的困难和风险。为了完成攻击目的，敌对组织 D 决定通过引起智能变电站 A 供电资源的中断来影响单位 C 的正常生产活动。

4.2.2 攻击过程描述

执行攻击前，敌对组织 D 通过各种途径了解到：

- 因不同厂家的设备在实现和配置方面存在一定的差异，智能变电站中二次设备的运维一般都通过相关设备厂家来进行；

- 智能变电站 A 的二次设备通常是由 E 公司的运维人员 M 负责运维；
- M 是电气自动化技术的爱好者，经常参加技术论坛 T 的话题讨论；且喜欢分享自己去变电站实地运维时发现的细节，并在论坛 T 上留下了自己的邮箱。

了解到这些情报后，敌对组织 D 实施了如图 4.2 所示的攻击过程：

（1） 定向植入恶意代码

a) 考虑到 M 经常出差，推测其平时登录论坛 T 的笔记本电脑很可能就是他在实地运维时所使用的计算机。因此，敌对组织 D 通过运维人员 M 在论坛 T 上留下的电子邮箱发送了一份某电气自动化技术论坛的技术交流邀请信，其中携带着一个邀请函文档附件。

b) 作为一个技术爱好者，M 没有任何的犹豫，直接打开了附件文档。由于敌对组织 D 在该文档中事先内嵌了一段利用一个微软 Word 未知漏洞的利用代码。这段代码在执行后能够从指定链接中下载远程访问终端（Remote Access Terminator，RAT）恶意程序，进而获取管理员权限，全面接管 M 的笔记本电脑的控制权。

c) 邀请函事件之后，M 又收到了一个交流取消的邮件，因此其也就淡忘了这件事情。

（2） 恶意代码植入变电站控制端

a) 几个月后，智能变电站 A 邀请 E 公司的运维人员 M 去执行例行检查。与往常一样，M 直接使用随身携带的笔记本电脑接入到了智能变电站 A 的站控层。每当接入一个新网络的时候，M 的笔记本中一个非常不显眼的进程就会突然活跃了起来，扫描网络中的计算机，使用微软 Windows 操作系统漏洞 MS XX-XXX 控制连接的计算机，植入 RAT 程序并激活。而这次稍微有一点不同，其中一台被攻陷的计算机上安装了一款软件 XXX，而这台电脑正是站控层操作员站所在的计算机。

（3） 执行恶意代码

a) 控制站控操作员站后，一个功能模块被悄无声息地注入操作员站控制软件 XXX 的进程，该模块负责向测控装置发送已经组态好的恶意代码。因为所有的操作都是按照正常的操作规程下发的指令，故障录波和网络分析仪无法感知其中可能存在的异常行为，无法及时进行报警处理。测控装置按照站控计算机下发的指令对刀闸进行了断开的操作，直接导致了向重要制造单位 C 的输电中断。同时，由于未对刀闸的操作进行灭弧处理，引起部分装置烧毁。

（4） 中断电力供应

a) 通过对关键电力供电设施的攻击，达到了对相关的基础制造业的间接攻击并直接影响了单位 C 的生产进度，达到了攻击者的攻击目的。

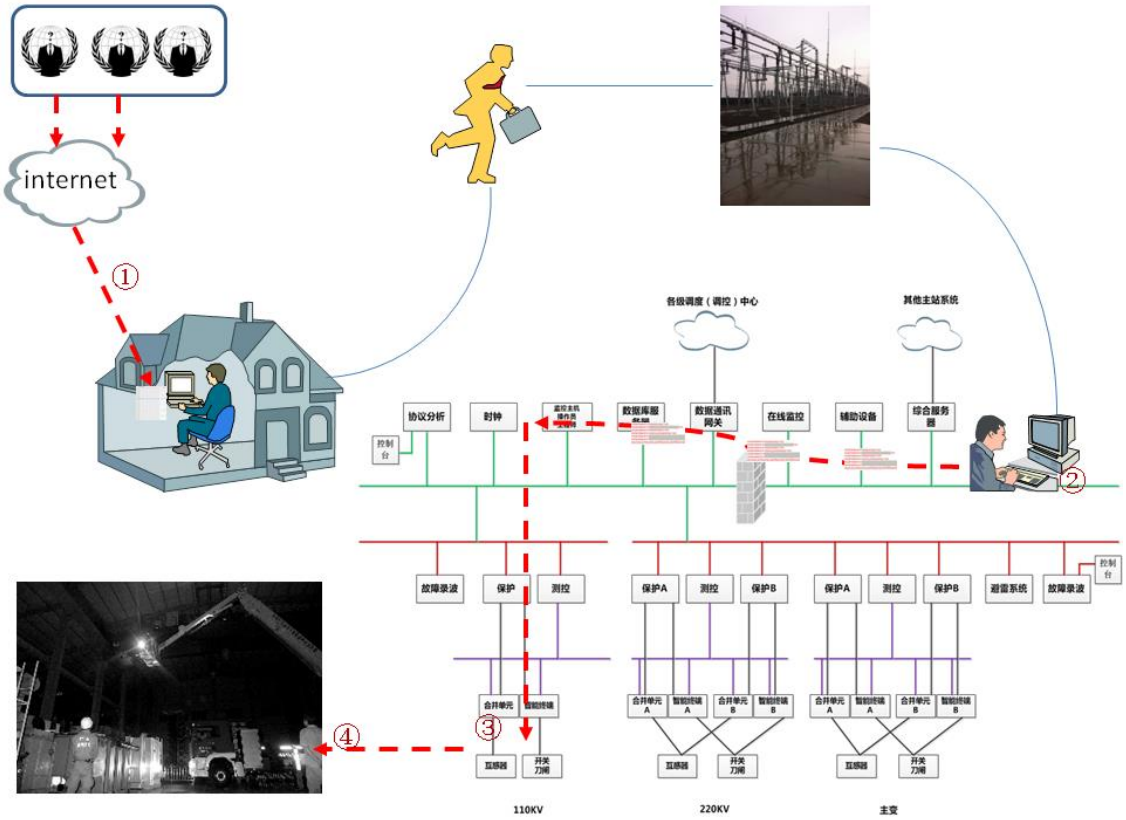

图 4.2 虚拟攻击过程示意图

五. 市政工业控制系统的安全性研究

伴随着工业化与信息化的融合，市政相关的工业控制系统（自来水、污水处理、燃气输送等）的重要性日益重要，并日益成为网络攻击者的目标。近年来国内外均出现了不少相关的入侵攻击事件，如表 5-1、表 5-2[wooyun]所示。

表 5-1 国外典型的市政系统安全事件

年份	事件
2011	黑客通过入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统的供水泵遭到破坏
2011	一个自称 Prof 的黑客示威描述他如何轻松的攻入控制南休斯顿市水厂的 SCADA 系统，用的就是在用户手册上发现的一个默认密码
2007	攻击者侵入加拿大的一个水利 SCADA 控制系统，通过安装恶意软件破坏了用于控制从 Sacrmento 河调水的控制计算机
2006	黑客从 Internet 攻破了美国哈里斯堡的一家污水处理厂的安全措施，在其系统内植入了能够影响污水操作的恶意程序
2001	澳大利亚昆士兰一工程师在被其公司解聘后，利用其对水务工程的熟悉，使用偷窃的无线电台、SCADA 控制器以及控制软件通过不安全无线网络的未授权访问，远程侵入该厂的污水处理控制系统，恶意造成污水处理泵站故障，在当地沿海水域排放了超过一万公升污水，导致严重的环境破坏
……	……

表 5-2 国内典型的市政工业控制系统安全事件

年份	事件
2013	某市自来水公司网站漏洞,可 shell ， SQL 注入直接拿 shell 提权，全市用户资料泄露
2013	XX 市自来水在线查询问题
2013	XX 市燃气集团有限公司存在远程执行漏洞 ， X 市燃气集团有限公司存在远程执行漏洞 存在漏洞的 url
2012	某市燃气管道 SCADA 系统登录绕过 ， 对设备状态的监控可以直接精确到某栋大厦
……	……

因为市政工业控制系统涉及自来水调度管理与控制、污水处理、燃气甚至交通管理等多个领域，本章因篇幅所限，仅以自动化程度较高的自来水厂工业控制系统为例来讨论其安全性。

5.1 自来水厂工业控制系统的安全性分析

自来水厂的工业控制系统的网络结构相对简单（如图 5.1 所示），主要分为生产调度中心和现场控制区两个部分。其中，生产调度中心的 SCADA 系统，通过租用运营商通信线路与水厂的现场控制系统进行连接，以实现对远端 PLC 系统的控制。用于实时监测饮用水生产过程中的水质状态如余氯量、温度、浊度、PH 值等状态信息，监测各机泵的运行状态并通过远端 PLC 控制水泵的启停及阀门的开关。

上位机采用组态软件实时显示各仪表状态、水质状态、同时操作员通过上位机远程控制水泵、阀门。远端的控制指令通过控件加密的方式在远端进行加密，现场的水处理控制系统通过控件解密的方式还原控制指令，再对相关 PLC 进行控制。如图 5.1 所示：

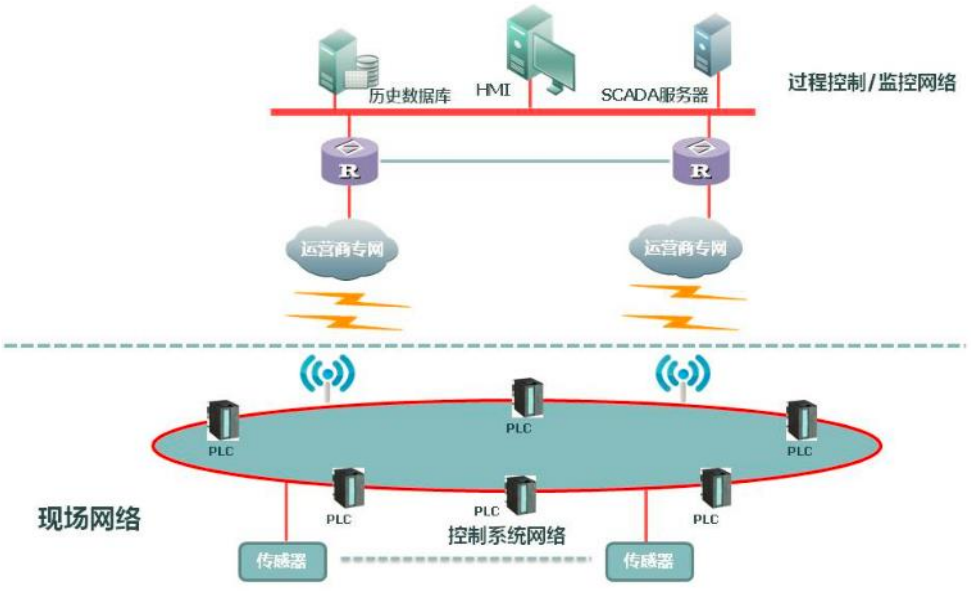

图 5.1 市政自来水厂的工业控制系统架构图

由图 5.1 的描述可知，现场网络中的 PLC 及各种传感器由位于过程控制与监控网络中 SCADA 系统进行远程控制。虽然许多系统在建设时考虑到了系统间远程通信的安全，并采用了专用加密链路，但这仅能保证传感器上传的生产过程的各种状态信息以及下发的系统控制

指令的完整性和机密性，并不能保证这些数据的真实可信性。因为攻击者在侵入过程控制/监控网络后，就可能获得 SCADA 系统的控制权，自然就可以远程发出一些符合工业控制协议的操作命令给 PLC 执行相应的操作，但这些操作自然是违规的。同样也可以篡改传感器数据，使系统操作员无法通过上位机检测到真实的生产状态数据，就可能造成自来水生产的质量问题等等。

同时，因自来水厂的生产系统相对封闭，操作管理人员普遍没有相应的信息安全意识。很少有相关单位制订明确的书面信息安全管理制度和操作规范，即使有也很少能够得到真正的执行。同时因缺乏专业的信息安全意识培训，对行业相关的系统漏洞及威胁情报信息了解很少。很多单位甚至没有对系统做过安全风险评估，不了解系统的真实安全状况：是否存在严重的系统漏洞？是否存在不安全的对外网络链接？是否存在移动介质的违规使用？是否存在违规操作？在监控网络中是否安装有防病毒/木马软件？在监控网络对外的授权网络链路上是否有防火墙等安全防护设备？ 甚至有些单位存在生产系统与办公网直接连通，在办公室直接访问监控网络查询相关数据的情况，而且 U 盘、智能手机也在普遍使用，这就为外部恶意代码进入系统干扰生产系统地正常运行提供了可能。

据我们的调研分析，目前该行业存在的主要问题是：人员安全意识不强，缺乏明确的安全管理制度及人员意识培训；缺乏系统有效的安全防护体系规划和安全风险评估机制；缺乏系统操作人员的角色定位、授权流程及操作规程（可能会带来越权或非授权操作的威胁）；缺乏相应的操作行为审计机制；缺乏系统数据备份（可能会因系统故障丢失重要数据）等。

综合上述，防范非授权的违规操作与恶意代码威胁以及健全安全管理制度、提升行业人员的安全意识将是该行业亟待解决主要问题。

5.2 虚拟攻击场景分析

某地一个自来水厂，负责为方圆 20 公里以内区域的企事业单位和居民供水。A 在自来水公司工作多年，对于自来水的控制系统非常熟悉。最近由于与新任领导关系紧张，工作上一直不顺心，涨工资、升职更是没份，因此想通过制造自来水控制系统事故，报复一下新领导。

虽然自来水公司对控制系统的运维有管理规定，但是运维人员为了工作便利还是经常使用普通移动介质，并且使用操作员工作站为手机充电的情况也非常普遍。

A 实施攻击的过程如图 5.2 所示：

1) 通过周密计划后，在一次例行维护中，A 假装使用操作员工作站为手机充电，实际上是通过手机向操作员工作站注入经过精心准备的恶意程序，恶意程序通过缓冲区溢出取得控制系统程序的 ROOT 权限。

2) 正常情况下，控制中心只接收自来水厂发送的状态变化信息，所有的控制指令的下发都是由自来水厂本地完成的。但控制中心具备下发功能，此功能只有系统管理员有权限启动。恶意程序在取得系统管理员权限后，在预先设定用水高峰启动控制进程。

3) 通过修改水处理过程中投放的各种过滤剂配比度，来影响自来水的质量，因为水厂的水质监测系统在发现水质情况超过预先设定的安全限度后会进行报警，在设定的程序中，为了第一时间减少水问题引起的安全事故，通常会在监测到水质出现问题时，会立即启动紧急闭闸，因紧急闭闸导致部分区域出现用水中断，引起相关企业的经济损失。

A 选定恶意程序的执行时间是自己的非当值时间，并且恶意程序在下发控制指令，并监测到已经完成相关的操作后，自动关闭了控制通道。自来水公司通过现有的技术力量无法定位出产生问题的具体原因，但事故已经发生，只能定性为一起安全责任事故，当值人员和新进的领导都受到处罚，新进领导承担管理责任，被调离此岗位。

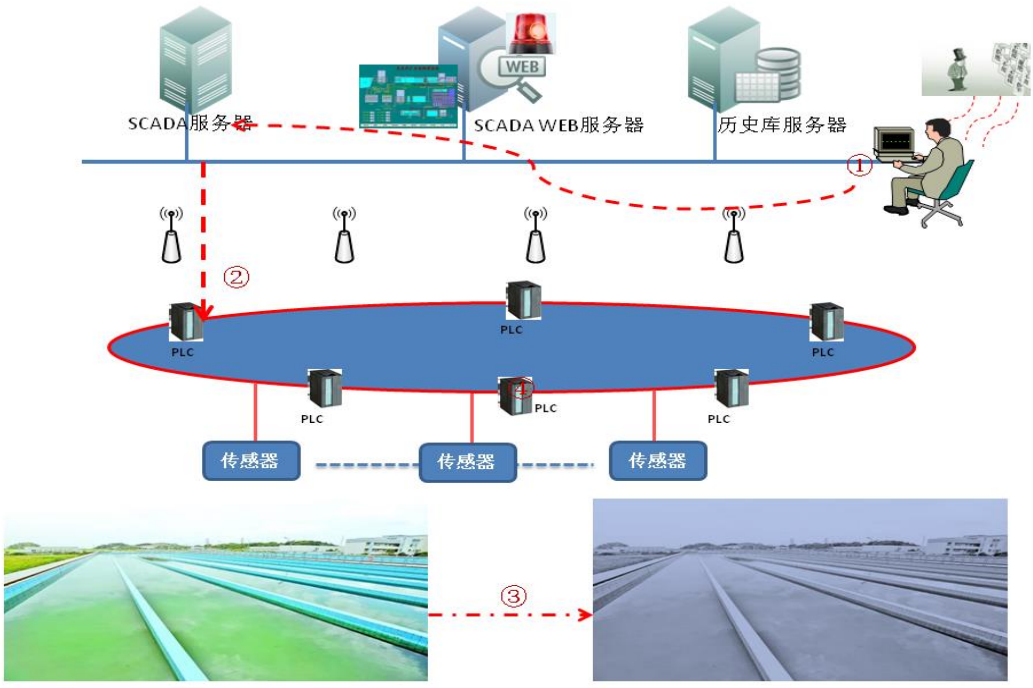

图 5.2 虚拟攻击过程示意图

六. 建议与展望

6.1 工业控制系统安全的发展建议与展望

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，如图 6-1 所示。

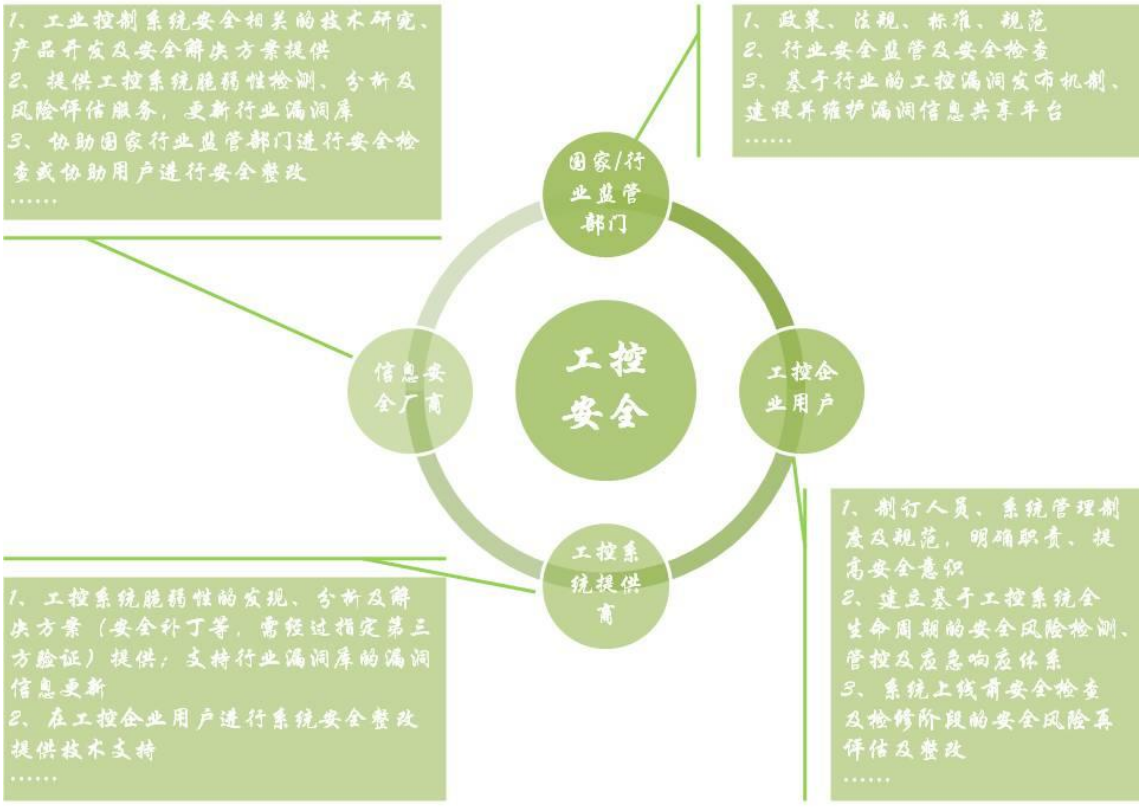

图 6.1　工业控制系统安全的生态环境

在国家的层面，可通过出台工业控制系统安全相关的政策、法规等可落地的指导性文件，从确保国家安全战略、应对网络战的威胁的角度明确国家各行业的战略目标和任务。进一步需要组织、协调行业监管部门、研究机构、工业控制系统的企业（用户）、信息安全厂商等共同参与的合作，建立工业控制系统安全相关的管理要求及技术标准与规范。明确行业监管部门的安全检查及督促企业进行安全整改的职责。建立国家层面的工业控制系统漏洞发布机制及漏洞信息共享平台。

在行业监管部门层面，可在行业内部建立起有效的工业控制系统安全监管机制及行业内部的安全通告机制；基于国家层面的安全管理要求与标准规范构建适用于本行业的安全防护体系、标准及规范；建立适用于行业的风险评估与安全检查机制，定期对工业控制系统的企业（用户）进行合规性安全检查并督促不合格企业进行安全整改。从国家政策落实的角度，通过安全检查促进工业控制系统的企业（用户）加强对工业控制系统安全的重视，并提升工业控制系统管理人员的安全意识。

对工业控制系统的企业（用户）来说，信息管理部门将被赋予更多的信息安全管理职责。首先需要和生产部门及信息安全厂商协同构建企业工业控制系统安全管理与技术防护体系；建立工业控制系统环境、人员管理安全相关的制度、规范。依据工业控制系统的重要性及潜在风险制订分级分域的管控与安全防护策略。明确操作管理人员的角色定义、职责及访问授权。其次，逐步加强对工业控制系统的安全运维管理。通过在工业控制系统上线前的漏洞扫描、配置核查与风险评估；运行阶段的安全管理、合规性监测以及维护阶段的安全检测与风险控制，形成完善的基于工业控制系统全生命周期的安全管控体系。第三，建立有效的安全应急体系，对于发现的攻击或违规行为，能够快速上报并及时地处理。同时，加强企业内部人员的安全意识和管理制度的培训则是当前企业提升工业控制系统安全防护能力的首要任务。

对工业控制系统提供商来说，因其重视工业控制系统的功能性实现、忽视安全性开发的历史原因，导致工业控制系统存在不少的安全脆弱性问题。又因为工业控制系统的专业性，信息安全厂商虽然有时能够发现工业控制系统存在的脆弱性，但因缺乏相应的实验环境、缺乏相应的知识等多种原因，而难以提供相应的经过验证的补丁程序。因此，这些关于工业控制系统脆弱性问题的解决以及相应的安全防护产品与工业控制系统间的协同离不开工业控制系统提供商的积极参与。

对信息安全厂商来说，工业控制系统安全将是一个新的战略发展方向。在复杂多变的互联网空间攻防对抗的经验、技术、产品和最佳实践的积累将是其进军工业控制系统安全的最

大优势。但也存在不熟悉工业控制系统环境、缺乏对工业控制协议的深入研究和积累、缺乏对工业控制系统控制原理及业务流程的深度理解；且存在因缺乏工业控制系统实验环境，难以进行脆弱性分析研究等等现实的不足，造成了信息安全厂商必须和行业监管部门、工业控制系统的企业（用户）以及工业控制系统提供商建立相对紧密的合作关系，成立联合实验室、参与构建行业级漏洞信息分享平台，建立专业的、关于工业控制系统的攻防研究团队，以提供针对性的、个性化安全服务才能有效地解决用户的安全需求。

6.2 工业控制系统安全产品及服务的发展建议与展望

依据我们的调研分析 [LW2013]：用户当前最为关注的工业控制系统安全问题为业务中断、违规外联、违规操作以及系统配置的不安全；并期望通过部署“违规操作的检测及预警”、“ 漏洞扫描及系统配置核查”、“审计系统”、“接入控制与身份鉴别”、“网络隔离设备”以及“防病毒”等安全机制或产品来防范其工业控制系统所面临的安全威胁。

基于用户的客观需求与信息安全厂商的现实基础，图 6.2 针对信息安全厂商给出了一些关于工业控制系统安全的研究、产品开发、安全服务以及对外合作的发展建议。建议信息安全厂商可从工业控制系统的脆弱性（漏洞）的挖掘分析入手：

- 首先提供针对工业控制系统的漏洞扫描及配置核查类产品及相应的产品上线前评估服务，随着对工业控制系统的进一步熟悉和经验的积累，推出基于行业应用的安全风险评估基线提高安全风险的评估服务能力。
- 其次，展开对工业协议的分析研究（因多数工业控制系统个性化强、生命周期长、通信协议种类繁多，这需要长时间的积累才行。），只有在具有足够的工业控制协议识别及解析能力的基础之上，才能够逐步开发基于工业控制协议识别、深度分析及合规性审核的工控防火墙、工控 IDS、工控审计系统等相关产品（即使漏洞扫描及配置核查类产品也需要工业控制协议的支持）。
- 第三，通过大量行业项目的积累以及与用户合作的进展，了解分析工业控制系统的业务逻辑和操作规程，开发操作行为监管类产品。因为工业控制系统的操作相对规范，结合操作人员的角色管理、认证及授权机制，可以构建有效的用户业务行为相关的‘白环境’— 合规性操作行为的集合[LHP2013]，在此基础上结合异常行为检测机

制可以大大提高发现工业控制系统内违规行为或未知攻击威胁的可能性，增强防范 APT 等新型入侵攻击的能力。

- 在上述工业控制系统安全产品开发的基础上，进一步加强工业控制系统安全的威胁情报分析，及时了解工业控制系统相关的安全情报信息，比如安全事件、漏洞信息、新型的入侵攻击技术以及当前流行的恶意代码（蠕虫、木马、病毒等）；提供行业工业控制系统安全态势感知能力，并结合相应的安全产品和安全防护技术提供相应的攻击检测及安全防护方案；进而增强针对工业控制系统的安全服务能力。

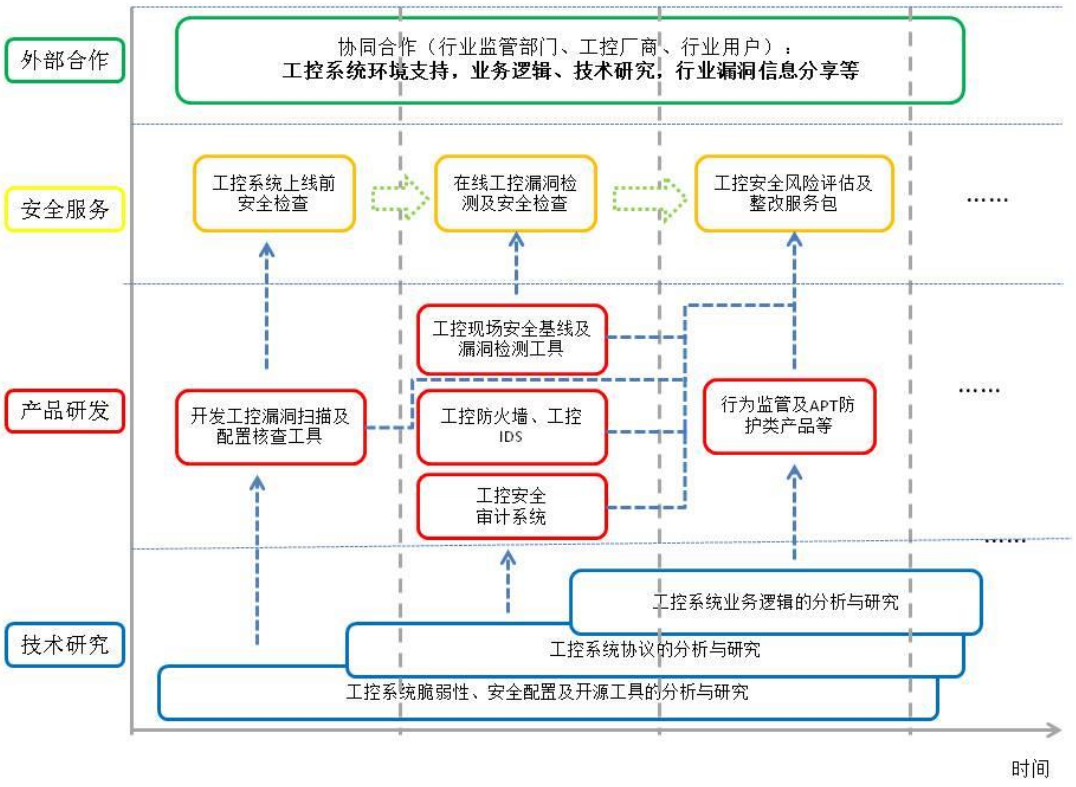

图 6.2　工业控制系统安全相关研究、产品、服务及合作的发展建议

6.3 小结

综上所述，工业控制系统安全作为一个新的、战略性的安全领域，需要国家、行业主管部门、工业控制系统的企业（用户）、工业控制系统提供商、信息安全提供商等跨领域、跨行业的多方位的合作才能够促进工业控制系统安全领域的发展。**以国家政策、标准为导向，行业安全检查、用户安全意识培训、工业控制系统风险评估及相应的安全产品、安全解决方**

案等的逐步推进将是工业控制系统安全领域的发展主线。其中，工业控制系统的企业（用户）的安全意识培训、工业控制系统的安全状况调查及系统脆弱性评估与整改将是近期的主要工作任务。这就需要建立工业控制系统的安全性测评验证机制，提供系统漏洞信息及厂商的漏洞修补方案及安全补丁的及时通报、分享及可用性验证机制。

2013 年国内政策、标准制订，工信部的安全检查工作及工业控制系统安全市场预测报告[GK2013]的发布，国家发改委工业控制系统安全专项基金的支持计划，电力、石化、烟草、市政等重要行业用户的积极响应以及国内主流工业控制系统提供商、信息安全厂商在工业控制领域的积极投入都表明：工业控制系统安全这一涉及国家安全战略的国内新市场正在快速的启动，在多方的合力推动下必将具有良好的发展前景。

附录 缩略语中英文对照

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

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

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”

Cyberwar， 网络战

Cybercrime， 网络犯罪

DCS，Distributed Control Systems，集散控制系统

DHS，The U.S. Department of Homeland Securty，美国国土安全部

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

FCS，Fieldbus Control System，现场总线控制系统

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

ICS，Industrial Control Systems，工业控制系统

NIST，National Institute of Standards and Technology，美国国家标准与技术研究院

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

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

RTU，Remote Terminal Unit，远程终端

RAT，Remote Access Terminator，远程访问终端

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

参考文献

1. [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。
2. [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》
3. [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》
4. [APT] http://en.wikipedia.org/wiki/Advanced_Persistent_Threat
5. [BL2013] 鲍旭华、李鸿培等，2012 年安全威胁态势报告，绿盟科技，技术报告，2013.1。 http://www.nsfocus.com/report/NSFOCUS_Threats_Report_2012.pdf
6. [BL2012]，鲍旭华、李鸿培等，2012 上半年 NSFOCUS 安全威胁态势报告，绿盟科技，技术报告，2012.8
7. [CVE] http://www.cve.mitre.org/
8. [CNVD] http://www.cnvd.org.cn/
9. [DHS2011] Common Cybersecurity Vulnerabilities in Industrial Control Systems，May，2011。
10. [Event2008] 南美某国电网被攻击，攻击者进行敲诈勒索，http://www.e-works.net.cn/report/fs/fs.html
11. [EW] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
12. [FP] http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack
13. [FL] http://www.crysys.hu/skywiper/skywiper.pdf
14. [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?code=cheminfo&action=detail&type=MRDynamic&infoId=2013080914124200001
15. [GXB451] 关于加强工业控制系统信息安全管理的通知，工信部协[2011]451 号。
16. [HL] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf
17. [ICSCERT1] ICS-CERT_Monitor_April-June2013_3
18. [ICSCERT2] ICS-CERT_Monitor_Jan-Mar2013
19. [IF] http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf

20. [LYHC2012] 李鸿培、于旸、忽朝俭、曹嘉，工业控制系统及其安全性研究报告，绿盟科技，技术报告，2012.12。 http://www.nsfocus.com/report/NSFOCUS_ICS_Security_Report_20130624.pdf.
21. [LHP2013] 李鸿培，下一代安全的概念与特性，绿盟科技，技术报告，2013.7。 http://www.nsfocus.com/report/Concept_and_characteristics_of_Next_Generation_Security.pdf.
22. [LHP2013-1] 李鸿培，工控系统的安全威胁离我们有多远？ 工控系统安全研讨会（PPT）,2013.10
23. [LYHC2013] 李鸿培、于旸、忽朝俭、曹嘉，工业控制系统的安全性研究，中国计算机学会通信，Vol.9，2013，pp37~42。
24. [LW2013] 李鸿培、王晓鹏，工业控制系统安全需求分析及产品规划研究，内部报告，2013.9。
25. [News2012] 天然气管道上的“苏美暗战”，中国海洋石油报,2012.11,http://www.cnooc.com.cn/data/html/news/2012-11-16/chinese/330655.html
26. [NIST-1] Guide to Industrial Control Systems (ICS) Security：NIST，SP800－82.,June,2011.
27. [NIST-2] Guide for Assessing the Security Controls in Federal Information Systems and Organizations：NIST，SP800－53A.,
28. [Nitro] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
29. [NS2013] 绿盟威胁分析系统产品白皮书，绿盟科技产品白皮书，2013。
30. [NVD] http://web.nvd.nist.gov/view/vuln/search
31. [RSA2013] Amol Sarwate，WHY IS ‘SCADA’ SECUIRTY AN UPHILL BATTLE?，Qualys Inc. 2013.
32. [SM] http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work
33. [Stuxnet1] http://www.anti-virus.by/en/tempo.shtml
34. [Stuxnet2] http://www.wilderssecurity.com/attachment.php?attachmentid=219888&d=1279012965
35. [USDE] 21 steps to improve cyber security of SCADA networks, The President’s critical infrastructure protection board, office of energy assurance, US department of Energy
36. [wooyun] http://www.wooyun.org.
37. [WP] http://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing
38. [wxp2013] 王晓鹏，工业控制系统安全之路，工控安全研讨会报告（PPT），2013.10.
39. [wxp2012] 王晓鹏，透过智能变电站看智能电网安全，绿盟科技内刊，Vol.19，2012.12.

作者信息

李鸿培

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。

忽朝俭

Email：huchaojian@nsfocus.com

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

王晓鹏

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。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS