DOI: 10.3969/j.issn.1009-6868.2016.05.008
网络出版地址：http://www.cnki.net/kcms/detail/34.1228.TN.20160905.1608.002.html

工业互联网的安全挑战及应对策略

Security Challenges and Countermeasures of the Industrial Internet

陶耀东/TAO Yaodong [1]
李 强/LI Qiang [1]
李 宁/LI Ning [2]
（1. 360企业安全集团，北京 100015；
2. 中国科学院大学 沈阳计算技术研究所，辽宁 沈阳 100168）
(1. 360 Enterprise Security Group, Beijing 100015, China;
2. Shenyang Institute of Computing Technology, University of Chinese Academy of Sciences, Shenyang 100168, China)

中图分类号：TN929.5 文献标志码：A 文章编号：1009-6868 (2016) 05-0036-006

摘要： 从设备、网络、控制、应用、数据、人员等方面全面分析了工业互联网面临的挑战，提出了应对安全挑战的10项策略，并创新性地出了整体建议和指导日常安全运营的PC4R自适应防护框架。指出工业互联网应用企业、安全服务企业、监管部门，需要采取提出的应对措施，形成联动的机制，从体制改革、管理流程优化、人员意识培养、技术创新等方面着手，构建PC4R的自适应防御架构，共同打造安全的工业互联网。

关键词： 工业互联网；安全挑战；应对策略；PC4R自适应防护框架

Abstract: In this paper, we analyze the challenges faced by the industrial Internet, and put forward 10 strategies from the aspects of equipment, network, control, application, data, personnel and so on. The PC4R adaptive protection framework is also proposed in this paper, which guides the daily safety operation of the industrial Internet enterprise. The industrial Internet companies, security services companies, network regulators should take measures to form linkage mechanism, and construct the PC4R adaptive defense framework from the aspects of the system reform, management process optimization, personnel training, technological innovation and so on. In this way, the secure Internet industry can be built.

Key words: industrial Internet; security challenges; strategies; PC4R adaptive protection framework

1 工业互联网概况

工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，中国工业互联网产业联盟（AII）提出的工业互联网参考体系架构[1]如图1所示。其中，“网络”是工业数据传输交换的支撑基础；“数据”是工业智能化的核心驱动；保障网络与数据的“安全”是工业互联网稳定运行、创造价值的前提。工业互联网的安全可以分为：设备安全、网络安全、控制安全、数据安全、应用安全和参与全程的人员安全。

工业互联网包含了工业控制系统、工业网络，同时也包含了大数据存储分析、云计算、商业系统、客户网络等商业网络基础设施，如图2所示。其中，工业控制系统（ICS）是指用于操作、控制、辅助自动化工业生产过程的设备、系统、网络以及控制器的集合[2]，包括：数据监测控制与采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、智能终端、人机交互接口（HMI）等一系

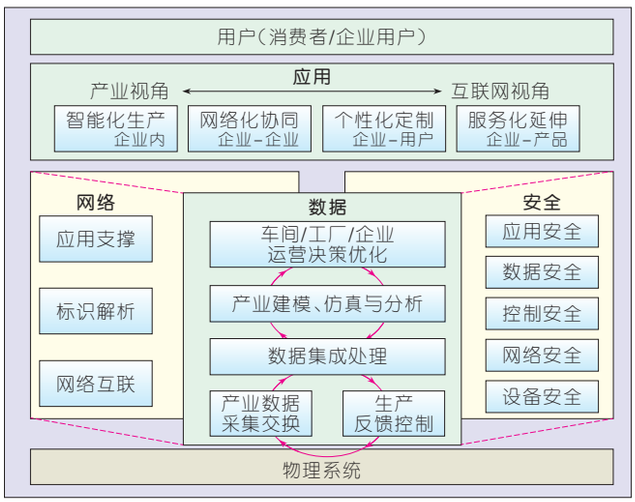
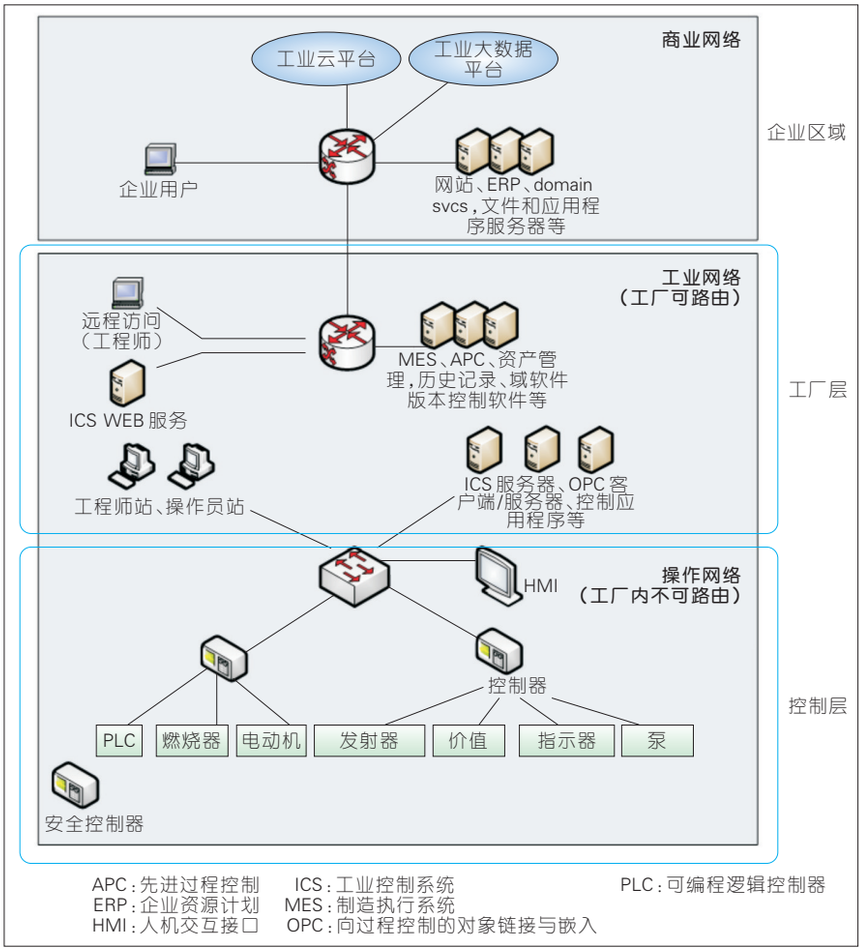


图1▶ 工业互联网体系架构

收稿时间：2016-07-20
网络出版时间：2016-09-05



▲图2 工业互联网的典型组成

列系统[3]。

文章中，我们将分析工业互联网的安全挑战，并提出应对措施、整体防御建议。

2 工业互联网的安全挑战

2.1 工业互联网的安全现状

在中国提出《中国制造2025行动纲要》后，工业互联网已经是国家战略组成，工业互联网安全关系国家战略安全。工业互联网中工业网络与采用Internet技术的商业网络的打通，标准Internet的威胁也随之而来——病毒和黑客。原本认为不容易被攻击的工业网络，也因存在设备同时连接到企业网络，而使该设备成为攻击跳板，最后工业网络受到攻击。近年来全球工业互联网安全事件频发，如：2006年8月，美国BrownsFerry核电站受到网络攻击事件；2011年5月，Duqu病毒（Stuxnet变种）出现；2012年12月，震网病毒攻击美国ChevronStuxnet等4家石油公司。根据RISI数据库统计，发生在工控领域的安全事件与涉及的工业行业，数量明显增多[4]，如图3所示。

2.2 工业互联网的各层次安全挑战

工业互联网安全主要受到来自图1所示的5个层次安全挑战，同时也包括可能参与到各个层面的人员因素，以及覆盖多个层面的高级持续性威胁（APT）。

（1）设备层安全挑战，指工业互联网中工业智能设备和智能产品的安全挑战，包括所用芯片安全、嵌入式操作系统安全、编码规范安全、第三方应用软件安全以及功能安全等，均存在漏洞、缺陷、规范使用、后门等安全挑战。

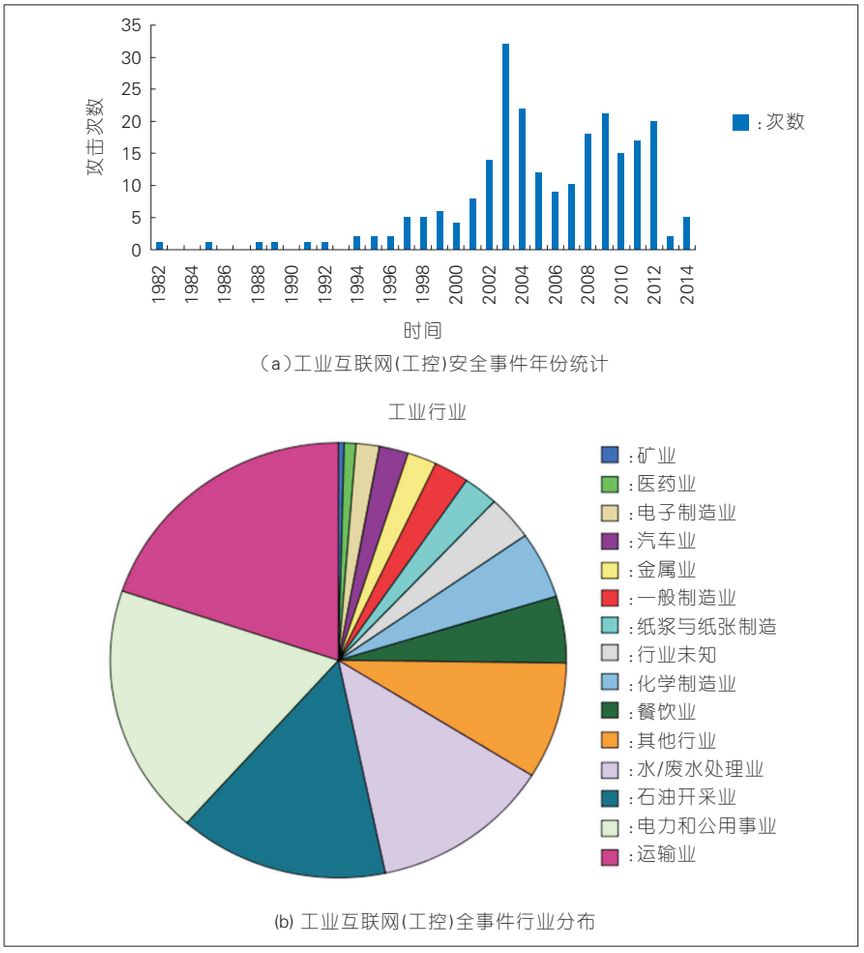
（2）网络层安全挑战，主要来自3方面：工业网络、无线网络、商业网络。主要挑战包括：网络数据传递过程的常见网络威胁（如拒绝服务、中间人攻击等），网络传输链路上的硬件和软件安全（如软件漏洞、配置不合理等），无线网络技术使用带来的网络防护边界模糊等[5]。

（3）控制层安全挑战，主要来自控制协议、控制平台、控制软件等方面，其在设计之初可能未考虑完整性、身份校验等安全需求，存在输入验证，许可、授权与访问控制不严格，不当身份验证，配置维护不足，凭证管理不严等安全挑战。

（4）应用层安全挑战，指支撑工业互联网业务运行的应用软件及平台的安全，如：WEB、企业资源计划（ERP）、产品数据管理（PDM）、客户关系管理（CRM）以及正越来越多企业使用的云平台及服务等。应用软件将持续面临病毒、木马、漏洞等传统安全挑战；云平台及服务也面临着虚拟化中常见的违规接入、内部入侵、多租户风险、跳板入侵、内部外联、社工攻击等内外部安全挑战。

（5）数据层安全挑战，是指工厂内部生产管理数据、生产操作数据以及工厂外部数据等各类数据的安全问题，不管数据是通过大数据平台存储，还是分布在用户、生产终端、设计服务器等多种设备上，海量数据都将面临数据丢失、泄露、篡改等一些安全威胁。

（6）人员管理的挑战，随着工业与IT的融合，企业内部人员，如：工程师、管理人员、现场操作员、企业高层管理人员等，其“有意识”或“无意识”的行为，可能破坏工业系统、传播恶意软件、忽略工作异常等，而针对人的社会工程学、钓鱼攻击、邮件扫



▲图3 工业互联网(工控)安全事件统计

描攻击等大量攻击都利用了员工无意泄露的敏感信息。因此,在工业互联网中,人员管理的也面临过巨大安全挑战。

(7)APT,工业互联网中的APT是以上6个方面各种挑战组合,是最难应对、后果最严重的威胁。攻击者精心策划,为了达成既定目标,所长期持续地进行攻击,其攻击过程包括收集各类信息收集、入侵技术准备、渗透准备、入侵攻击、长期潜伏和等待、深度渗透、痕迹消除等一系列精密攻击环节[6-7]。

3 工业互联网安全的应对措施

针对第2节提到了工业互联网所面临过的威胁,我们可从以下几方面进行系统应对。

3.1 知己知彼

(1)知己——安全的前提

制作工业互联网中企业内网的设备清单,保证任何一件设备都处在安全的状态。理解并且登记在企业网络环境中的工控系统设备及其安全状态,是工控安全管理的基础。工控资产清单包括硬件清单、软件清单、软硬件配置清单、网络拓扑图等。

(2)知彼——主动防御

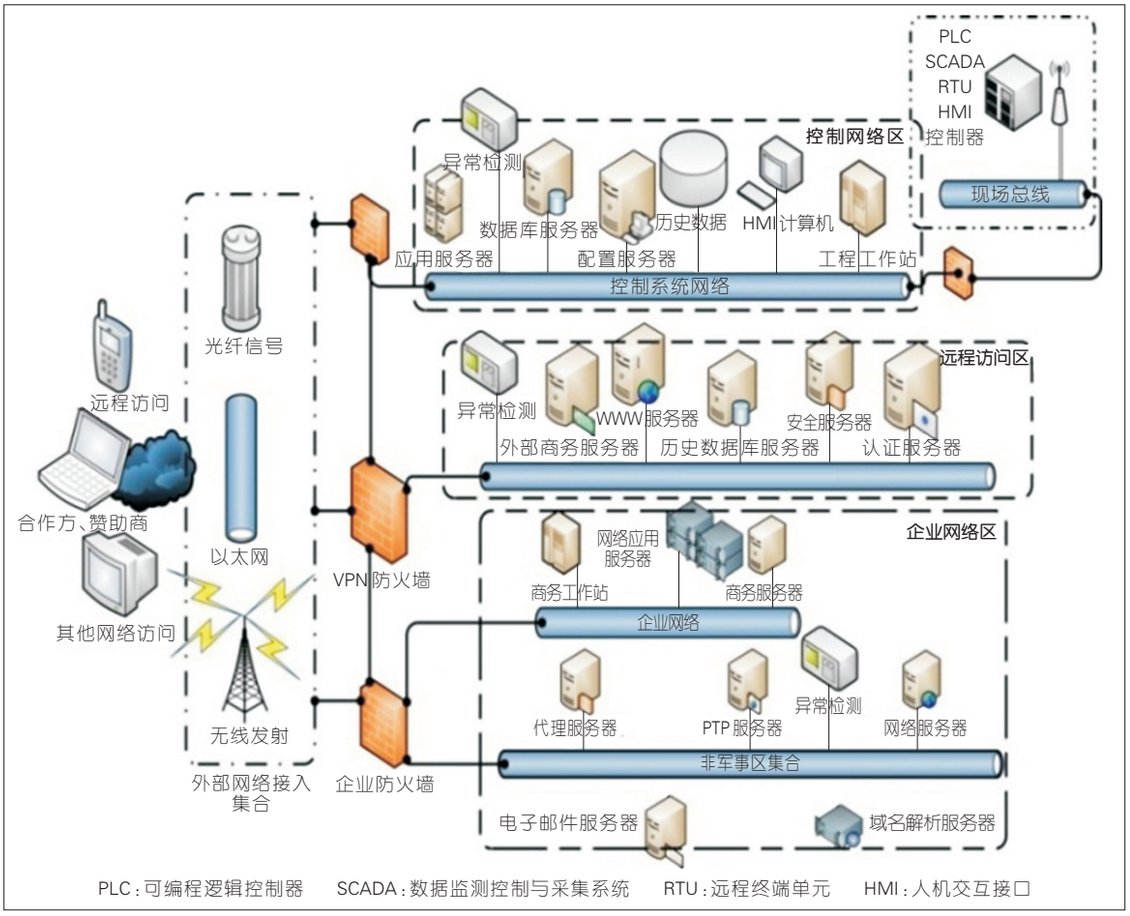
采用蜜罐系统对入侵行为进行捕获,分析相关行为后,并采取更新防火墙、服务器、工作站等安全略策,进行主动防御,使得入侵无功而返。如Conpot[7]在GitHub发布开源工控蜜罐系统Conpot,该系统是工业控制系统服务器端的低交互的蜜罐技术,设计易于布置、修改和扩展,通过提供各种通用的工业控制协议,可以构建需要的系统,并且能够模拟构建基础设施[8]。目前,其他一些国家将蜜罐技术用于研究工业互联网的威胁源,攻击途径以及探索防御手段,技术应用成熟,取得了很多成功,中国部分企业已开始尝试使用。

3.2 网络分区防护

图4为参考NIST SP 800-82、IEC62443等国际工控领域指导性文献的深度防御架构,该架构将工业互联网划分为外部区域集合、控制网络区、企业网络区、远程访问区与生产现场。在相应边界设置防火墙,可保护整个的内部系统免受外部的攻击,隔离企业网络与远程访问区,控制系统网络与其他网络隔离,生产区与控制网络隔离。为进行工业互联网保护,网络分区与应用防火墙可按4个阶段改进:第1阶段双宿主机防火墙;第2阶段在企业网络和控制网络之间构建防火墙[3];第3阶段添加路由的企业与控制网络间的防火墙策略;第4阶段添加非军事区(DMZ)防火墙;最后是按照深度防御体系的布置防火墙,并采用基于行为感知的动态分区技术[9]、特殊分区间的单项传输策略和基于威胁情报的非白即黑策略等。

3.3 安全的远程访问

远程接入设备和移动设备安全的远程访问是工业互联网开放的基础。首先,对于企业工作人员移动设备管理策略应该至少要求远程访问人员不得在公共网络、私人WiFi、其他单位局域网中登录,需要使用安全的网络登录,例如虚拟专用网络(VPN)登录,登录需要使用强口令,并且口令、文件应加密传输[10],企业外部客户远程访问要做好访问域、访问权限控制等;再次,使用VPN技术保证远程访问过程安全,也被列入到



◀图4
ICS深度防御架构

美国国土安全部发布的工业控制系统远程访问的指导性文献[11]；另外，工业控制网络网关无需对工控设备做任何改造或配置，便可完成数据包的转发工作，不依赖任何硬件环境和软件环境，适用于各种SCADA系统防护，也具有较强的适用性[12]。

3.4 漏洞和补丁管理

入侵者或黑客用漏洞对工业互联网中的商业网络和工控系统展开攻击，如零日漏洞攻击。科学地检测各类服务器、终端和工控系统漏洞，并合理更新补丁是工业互联网防御的重要组成。CVE、中国国家信息安全漏洞库、国家信息安全漏洞共享平台等权威机构漏洞库统计出现的包括工控系统在内的各类漏洞，可作为漏洞扫描的参考。同时，企业用户在自己的工业网络中，主动利用漏洞扫描技术提前检测主机、网络、工控系统的安全脆弱性，这也是一种主动防御技术。针对工业互联网中的工控系统，因其是实时连续运行的系统，更新补丁需要科学的策略，工信部451号文件也明确了对补丁安全管理提出了要求。

3.5 攻击检测与应急响应

异常检查是对防火墙的补充，可检查内部的攻击、异常，并可检测跨防火墙攻击。异常检查包括入侵检测、病毒查杀、异常代码检测等。业界已提出一些入侵检测模型、异常检测方法，如：非参数累积和（CUSUM）模型、基于多分类支持向量机（SVM）的入侵检测方法[13]，以及基于系统级行为特征的ICS场景指纹异常检查方法[14]。业界也通过对工业网络中的流量进行被动监测控制，进行分析检测异常，如对工业网络用差分自回归移动平均模型（ARIMA）方法对正常流量建模后检测异常[15]。工业大数据现在已开始应用在工业系统和工业网络健康预测性管理（PHM）[16]，通过对工业网络、控制系统、设备上提取关键信息，经过大数据建模、分析、预测，提前预测工业系统的状态和可能存在的异常，布置相关预案。将工业大数据用于工业互联网的异常检测和应急响应，将有机会提前发现由于工业互联网入侵引起的安全事件，抓住先机[17]。

工业互联网受到攻击是不可避免事件，优秀的安全策略的一个重要指标是能在尽可能短的时间内检测到入侵事件，做出响应动作，使系统回复正常的生产过程，这需要对应急响应包括对入侵事件分类、针对不同类型的入侵事件执行不同的响应动

作，最后采取恢复系统的动作，制订面向网络的故障维修事件应急响应策略，进一步优化响应时间。

3.6 态势感知

态势感知指综合分析工业互联网安全要素，结合企业、商业网络和工业网络状态，评估工业互联网的安全状况，预测其变化趋势，以可视化的方式展现给用户，并给出相应的应对措施和报表。在中国，将态势感知技术用于互联网、企业内网已经出现了解决方案，如360公司的天眼下一代态势感知和未知威胁发现平台，但是将态势感知用于工业互联网还是比较少。其他一些国家提出专门应用于ICS的态势感知参考架构（SARA），并提出构建网络入侵自动响应和策略管理系统（CAMPS）[19-20]。

从技术发展趋势来看，只要解决了工业网络中的协议多样性、应用多样性的问题，互联网态势感知和未知威胁发现的方法就同样能够适用于工业互联网中，那么态势感知和未知威胁发现将是工业互联网应对安全挑战的重要策略选项。

3.7 用户与实体行为分析

如何确定有效特权账户是否被盗用，应用是否被攻破，设备是否因攻击进入异常状态也是工业互联网用户最棘手的问题之一，解决该问题的最新安全对策是用户与实体行为分析（UEBA）方案。

UEBA方案从物理传感器、网络设备、系统、应用、数据库和用户处收集数据，利用这些数据创建一条基线，以确定在各种不同情况下，什么状态是正常状态。建立基准线后，通过聚合数据、机器学习，发现非正常的模式。用户行为分析管理员也可以创建自定义规则来定制解决方案，以便更贴合工业互联网用户及其特定服务、数据和过程的需求，未来部署了UEBA方案的工业互联网用户，准确率命中异常事件的速度将远快于传统的安全信息和事件管理（SIEM）系统，可防御80%复杂攻击。

3.8 打造安全的产品

工业互联网中运行了的服务器、终端、工业控制系统、传感器等，特别是工控系统、工业软件，其开发人员一般是控制领域的人员，其信息安全知识不足，往往存在开发环境过时，操作系统版本过时并没有补丁，编码规范不严格，所引入的开源组件代码安全性未知等情况，所完成的产品可能在出厂时就带有各种开发人员未知的缺陷、漏洞等，在进入应用现场后，才开始考虑产品的安全，导致后期修复、升级、防护投入巨大，这也是工控系统安全事件频繁发生的根源之一。因此，我们需要转变思路，将产品进入使用后进行防护保证“产品的安全”这种通常模式，转变为产品进入使用前，先按安全规范，对问题排除，使其成为“安全的产品”。

各大工业互联网解决方案厂商，特别是工控产品厂商，可以联合信息安全厂商建立自己的产品的开发流程、编码规范、出厂标准等。工业互联网应用用户，在将系统投入使用前也请专业的安全服务商、第三方检测机构帮助发现、解决可能存在的问题。越早发现产品或整体网络安全问题，其修复成本越低。

3.9 安全即服务

在工业互联网中将广泛使用云计算、大数据技术，在云平台所面临的问题，如虚拟化安全问题、分布式拒绝服务（DDOS）攻击和挑战黑洞（CC）攻击等，采用传统硬件或设备已经无法防护，安全产品转化新的形势，即安全即服务。安全服务即以云服务的方式在云端为用户提供各种安全解决方案，包括：态势感知、DDOS防护、域名系统（DNS）劫持、IP攻击等；在安全运维管理方面，安全也正变成一种服务，被工业互联网企业采购；企业也不再维持一个庞大的信息安全维护人员，而是在工业互联网中布置响应感知探针，构建安全管理平台后，发现网络中的安全问题，自动对接专业的安全服务公司或安全专家，由安全专家根据所约定的安全事件级别，提供相应的响应服务，服务内容包括：网络安全评估、渗透测试、取证溯源、响应恢复等。

3.10 以人为中心的安全

在工业互联网中，以人为中心的安全策略（PCS）可以作为应对人员管理挑战的战略应对。在以PCS指导的安全策略中[20]，可以从问责、责任、即时性、自治、社区、比例、透明度等方面设计较好的安全制度和流程，建立人员的信任空间，包括人员的自治性、主动性、对话、查询等。这个策略实施过程中应强调个人的责任和信任，并强调限制性、预防性的安全控制。进一步地，工业互联网企业可以建立用户和实体行为分析UEBA的系统，并结合端点、网络和应用的情况，提供了围绕用户行为的、以用户为中心的分析。这种跨不同实体相关性分析使得分析结果更加准确，让威胁检测更加有效。

4 工业互联网安全挑战的整体防御建议

4.1 整体防御建议

（1）从“应急响应”转变为“持续响应”。假定工业互联网系统受到破坏并需要不断监测控制和修复，则需要建立多点防御、联合防御，与产业界合作开展防御响应。

（2）以“数据驱动安全”。对工业互联网中的所有层面构建进行全面持续的监测控制，通过全面的数据感知和分析，建立企业安全数据仓库，并结合云端威胁情报，实现对已知威胁、高级威胁、APT攻击的有效预防、发现、防御和过程回溯。

（3）开发安全运维中心，构建组织流程和人员团队，支持持续监测控

制并负责持续的威胁防护流程，规划好外部安全服务合作伙伴，保证“人在回路”，应对各类安全事件。

4.2 工业互联网的PC4R自适应防护架构

为帮助工业互联网用户应对工业物联网所面临的各种挑战，结合整体防御的3点建议，我们提出了可以工业互联网信息安全日常运作的自适应防护架构——PC4R，其由6个过程闭环组成，该6个过程均需要人在回路，全程参与，具体如图5所示。

（1）信息感知

工业互联网中，实现对工业网络中工业现场（压力、摩擦、振动、温度、电流等）关键物理量数字化感知、存储，为工业现场异常分析、预防性健康监测分析提供物理信息来源。

（2）数据汇集

对数控系统（CNC）/ PLC、分布式数控（DNC）、SCADA、制造执行系统（MES）、ERP等工业控制系统及应用系统所运行的关键工业数据进行汇聚，该过程不是简单的数据采集，是产品全生命周期的各类要素信息的同步采集、管理、存储、查询，为后续过程提供控制信息来源。在网络方面，进行全网流量的被动存储等，为工业互联网企业建立安全数据仓库。

（3）转化分析

数据特征提取、筛选、分类、优先级排序、可读，可以实现从数据到信息的过程，使得数据具有信息安全意义。信息主要包括内容和情景两方面，内容指工业互联网中的设备信号处理结果、性能曲线、健康状况、报警信息、DNC及SCADA网络流量等；情景指设备的运行工况、维护保养记录、人员操作指令、人员访问状态、生产商务任务目标、生产销售机理等；该过程针对单个设备或单个网络做纵向的数据分析，计算相对来说比较简单。

（4）网络融合

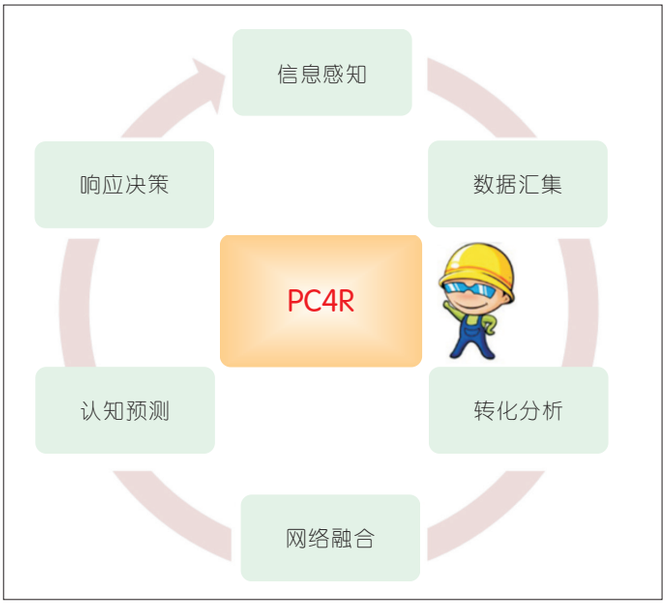
该过程面向工业互联网中的设备集群和企业跨域运维和经营活动的关联，将机理、环境、群体、操作、外部威胁情报有机结合，基于大数据进行横向大数据分析和多维分析，利用群体经验预测单个设备的安全情况；并建立虚拟网络与实体系统相互映射，实现综合模型的应用，如蜜罐、入侵检测等；也可以根据历史状况和当前状态差异化的发现网络及工控系统异常。

（5）认知预测

该过程在网络层的基础上，加入人的职责，人在回路，对企业的工业互联网规律、异常、目标、态势、背景等完成认知，确定安全基线，结合大数据可视化平台，发现看不见的威胁，预测黑客攻击。

（6）响应决策

根据认知预测的结果，一旦完成了对事件的识别并确认优先级排序后，人在回路的决策、部署、优化、响应，可实现安全价值，而启动相关响应策略，如隔离受损系统或账户，使其无法访问其他系统，从而遏制威胁。同理，人在回路也可以在决策之后，形成团队，一旦受损系统或账户得以遏制，并利用持续监测控制所收集的数据来源确定根本原因和所有违规行为。



◀图5
工业互联网的PC4R自适应防护架构

5 结束语

工业互联网打通了商业网络与工业网络的边界，传统的网络边界概念正在逐渐模糊，网络环境的复杂性、多变性、信息系统和工业控制系统的脆弱性，给工业互联网带来了设备、网络、控制、应用、数据、人员等多方面安全挑战。工业互联网应用企业、安全服务企业、监管部门，需要采取文章所提出的应对措施，形成联动的机制，从体制改革、管理流程优化、人员意识培养、技术创新着手，构建PC4R的自适应防御架构，并通过内外部大数据、威胁情报驱动安全防御，全程人在回路，利用用户本身、专业安全服务机构的力量，进行预测、防护、检测、响应，并根据不断出现的、新的威胁形式，完善应对策略，共同打造安全的工业互联网。

参考文献
[1] 工业互联网产业联盟(AII). 工业互联网体系架构[R]. 北京:工业互联网产业联盟, 2016
[2] WILHIOT K. Who's Really Attacking YourICS

➡下转第46页