Pisco Med Publishing
ISSN:2705-0963（Print） ISSN:2705-0955（Online）

工业互联网安全体系分析与对策

邹少军

江门职业技术学院 广东 江门 529090

摘 要：本文就工业互联网安全体系在工业实际应用中的一些安全问题进行分析，提出在平台安全、网络安全、数据安全、设备安全、安全标准五方面的一些对策及建议，旨在增强工业互联网中平台、设备、网络、控制、应用和数据的安全保障能力，有效识别和抵御各类安全威胁，化解各种安全风险，保障工业智能化的实现。

关键词：工业互联网；数据安全；平台安全；设备安全

一、引言

安全体系是工业互联网的保障，通过构建涵盖工业全系统的安全防护体系，构建工业智能化发展的安全可信环境，是工业互联网健康发展的保障[1]。2018 年工信部《加强工业互联网安全工作的指导意见》提出到 2020 年底初步建立工业互联网安全保障体系[2]。工信部 2020 年 3 月 20 日发布 20 条支持举措，加快健全安全保障体系[3]。建立企业分级安全管理制度，出台工业互联网企业网络安全分类分级指南，制定安全防护制度标准，开展工业互联网企业分类分级试点，形成重点企业清单，实施差异化管理。因此，建立工业互联网安全保障体系，使工业安全防护体系贯穿平台所有层级，全方位保障设备、网络、控制、应用和数据的安全，有效识别和抵御各类安全威胁。

二、目前工业互联网安全体系形势

目前众多企业和机构加入到工业互联网建设中来，大力促进了工业互联网网络、平台、安全三要素的共同发展。我国目前工业互联网网络、安全体系尚未构建完整，为了保障工业互联网平台数据安全，进一步加强工业互联网安全防护体系建设，是抢占新一轮工业革命发展制高点，是应对日益复杂网络安全形势、筑牢网络安全防线的必然要求。

（一）工业互联网平台安全问题

平台安全和平台标准化问题仍是局限世界范围内工业互联网平台发展的主要因素，由于国外工业互联网平台发展呈现大企业主导、政府引导的自下而上的特点，导致平台的标准制定倾向于部分大型企业，不能形成统一的国家标准和世界标准。平台安全问题主要体现于两个方面，一是数据传输中的网络安全问题，二是工业无线通信网络的安全问题；工业互联网平台标准化问题使平台建设和应用推广面临困难。

（二）网络安全问题

网络安全指承载工业智能生产和应用的工厂内部网络、外部网络及标识解析系统等的安全[4]。安全威胁主要源自传递网络数据过程中出现的拒绝服务以及中间人攻击等比较常见的网络威胁，软件漏洞以及配置不合理等传输链路上存在的软硬件安全等因素，使用无线网通讯技术过程中出现的边界防护模糊等安全隐患。

（三）数据安全问题

数据安全包括涉及采集、传输、存储、处理等各个环节的数据以及用户信息的安全。比如工业内部、外部各类数据的综合，如内部的管理数据、生产操作数据以及外部的工厂数据等，各类数据无论是集中存储于大数据平台，还是散存于设计服务器、生产终端或者用户设备上，难以计数的大量数据都存在着被篡改以及丢失等潜在的安全威胁。又如异构数据的存在导致工业数据难以实现信息流通，难以发挥工业互联平台价值，因此工业互联网平台数据安全是工业互联网安全建设的重要保障，数据防泄漏，防攻击是保护企业、城市、国家工业信息秘密避免泄露的关键所在。

（四）设备安全问题

设备安全包括工业智能装备安全，比如工厂内单点智能器件、成套智能终端等智能设备的安全，以及智能产品的安全，具体涉及操作系统 / 应用软件安全与硬件安全两方面。工业互联网中的工业物联网控制着大量的设备，倘若存在安全问题的设备连接到工业互联网中，可能导致这些采用嵌入式技术的物联网终端设备被利用，进而造成 DDoS 攻击甚至僵尸网络等问题。

（五）安全标准仍未统一或制定

工业互联网安全标准主要包括设备安全、控制系统安全、网络安全、数据安全、平台安全、应用程序安全、安全管理等标准。我国目前在在网络化制造、智能化生产、供应链管理等安全方面制定了少量的标准，主要涵盖工业互联网典型应用方面，但面向重点行业领域的安全标准仍未制定，没有统一的安全标准或没有制定标准，给工业互联网体系安全多个环节带来严峻的威胁及挑战。

三、工业互联网安全体系防护对策

鉴于上面提到工业互联网存在的一些安全问题，提出以下几点安全防护对策及建议：

（一）平台安全防护策略

首先建立平台统一的访问机制，限制用户的访问权限和所能使用的计算资源和网络资源实现对平台重要资源的访问控制和管理，防止非法访问。其次通过平台入侵实时检测、恶意代码防护等技术实现平台的代码、数据、网站及应用的安全。另外也建议我国应建立工业互联网安全监测与态势感知平台，在采集多维度、多层次数据的基础上，通过对安全信息分类、归并、建立数据模型、分析等手段进行融合、分析，得到网络的整体安全状况及其应对措施，并对网络安全状况的发展趋势进行预测，从而为工业互联网安全体系提供重要保障。

目前国家工业信息安全发展研究中心等研究机构和浙江中控、湖南创发等企业在工业数据的安全监测与态势感知方面已取得显著成果。

ISSN:2705-0963（Print）　　ISSN:2705-0955（Online）

（二）网络安全防护策略

建立网络安全防御系统，通过网站威胁防护、网页防篡改等技术建立网络结构优化、边界安全防护、接入认证、通信内容与通信设备防护、安全监测审计等安全机制。

（三）数据安全防护策略

工业互联网体系中的工业数据安全与企业隐私防护的面临严峻挑战，首先建立工业互联网云数据安全策略。云数据一般是生产工艺等核心数据，涉及企业核心利益，具有一定商业机密性。充分利用计算存储能力无限扩展、云数据快和成本低的明显优势，建立云安全通过机制流程，利用数据安全技术为云上数据、云上用户提供可靠保障。其次重点解决工业互联网云数据中的稳私安全问题。当前公有云在技术保障和法规规范层面已达到较高标准，但解决部分企业或个人对数据“上云”的安全隐私问题势在必行。

工业互联网数据安全防护主要通过工业防火墙技术、工业网闸技术和加密隧道传输等技术，防止数据泄漏、被侦听或篡改，保障数据在源头和传输过程中安全。

（四）设备安全防护策略

可采用的安全机制包括固件安全增强、恶意软件防护、设备身份鉴别与访问控制、漏洞修复等策略。采用的安全机制包括明示用途、数据加密、访问控制、业务隔离、接入认证、数据脱敏等[5]。

（五）控制及应用安全防护策略

控制及应用安全，包括控制协议安全、控制软件、功能安全及支撑工业互联网业务运行的工业应用程序安全。可采用的安全机制包括协议安全加固、软件安全加固、恶意软件防护、补丁升级、漏洞修复、安全监测审计等。应用程序安全防护策略主要采用包括安全审计、认证授权、DDOS 攻击防护、漏洞排查、应用程序行为监测等安全机制。

（六）完善工业互联网各项安全标准

工业互联网产业联盟（AII）2019 年 2 月发布《工业互联网标准体系（版本 2.0）》[6]，修订了工业互联网标准体系框架及重点标准化方向，其中安全标准化工作应紧密围绕工业互联网各安全防护对象，防护措施和防护管理三个维度来开展。目前已发布《工业互联网安全总体要求》和《工业互联网平台安全防护要求》两项联盟标准，但从标准明细表中仍有待制定的标准 141 项[6]，制定并完善工业互联网各项安全标准，才能减少安全威胁，保障工业互联网体系的安全。

四、总结

综上所述，建立完整的工业互联网安全防护体系，必须从工业互联网平台、网络、工业数据、设备及统一安全标准等多方面进行分析研究，结合工业互联网应用建立具体对应的安全防护策略，加强工业互联网网络及平台数据安全防护，加大力度建设数据防泄露、防篡改等安全防护体系，制定并完善各项安全标准，全面保障工业互联网设备、网络、控制、应用和数据的安全，从而加快我国制造业转型升级，推动实体经济高质量发展。

参考文献：

［1］陶耀东等 工业互联网的安全挑战及应对策略 中兴通讯技术 OI：10.3969/j.issn.1009-6868.2016.05.008

［2］工业互联网产业联盟 . 工业互联网平台白皮书（2017）［R］, 2017.

［3］工业和信息化部办公厅关于推动工业互联网加快发展的通知 工信厅信管〔2020〕8 号

［4］程月平 分析工业互联网安全问题面临的挑战与应对措施 仪表技术 1006 — 2394（2020）10 — 0037 — 04

［5］李志博 曾鹏 李栋 工业互联网架构与关键技术 仪器仪表标准化与计量 CNKI：SUN：YQBJ.0.2020-01-013

［6］工业互联网产业联盟 . 工业互联网标准体系（版本 2.0）工业和信息化部 2019.2 发布