工业互联网网络安全技术浅析

Analysis of Industrial Internet Network Security Technology

吴　涛[1]，黄　健[2]，郭钰璐[2]，杨　飞[1]，赵　通[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Wu Tao[1], Huang Jian[2], Guo YuLu[2], Yang Fei[1], Zhao Tong[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

工业互联网的连接逐步打破了传统工业相对封闭可信的生产环境，针对近年工业互联网安全事件频发的严峻形态，对工业互联网的相关网络安全技术进行分析研究。从工业互联网的安全体系架构出发，针对工业互联网安全架构中网络安全的模块，识别出相关的安全风险，并针对识别出的风险进行分析研究，依靠现有的安全技术提出了相应的解决方案与规避措施，并对落地实施方案做了简要介绍；同时对于工业互联网的安全技术发展趋势做了简要分析。

关键词：

工业互联网；网络安全；数据安全

doi：10.12045/j.issn.1007-3043.2022.09.003

文章编号：1007-3043（2022）09-0009-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

The connection of industrial internet has gradually broken the relatively closed and reliable production environment of traditional industry. In view of the severe situation of frequent industrial Internet security incidents in recent years, it analyzes and studies the relevant network security technologies of industrial internet. Based on the security architecture of the industrial internet, in view of the network security modules in the security architecture of the industrial Internet, the relevant security risks are identified, and the identified risks are analyzed and studied. Based on the existing security technologies, the corresponding solutions and avoidance measures are proposed, and the implementation scheme is briefly introduced. At the same time, the development trend of industrial Internet security technology is analyzed.

Keywords：

Industrial internet; Network security; Data security

引用格式：吴涛，黄健，郭钰璐，等. 工业互联网网络安全技术浅析[J]. 邮电设计技术，2022（9）：9-12.

0　前言

在“新基建”背景下，数字化驱动的工业互联网技术加速了信息空间与物理空间的融合，“键盘鼠标”与“大国重器”之间界面的逐步打破将导致工业互联网暴露在互联网“炮火”攻击之下，不可避免地成为恶意势力攻击破坏的首要目标。近年来，工业互联网安全形势严峻，工业安全事件频发。

自2010年伊朗核电站Stuxnet震网病毒攻击事件起，针对工业互联网的攻击事件愈发频繁，如2015年乌克兰电力公司遭到黑客攻击，导致大规模停电；2017年美国水务公司遭受黑客入侵，导致大量用户信息泄露；2017年的“魔窟”勒索病毒感染全球百余个国家和地区；近日委内瑞拉一大型水电站系统遭“黑客攻击”，影响21个州的供电事件。工业互联网安全已经成为了世界性难题，没有安全保障的工业互联网，其后续的发展将寸步难行。加强工业互联网安全关键技术研究，推进工业互联网安全技术发展已经刻不容缓。

收稿日期：2022-07-11

1　工业互联网体系结构

工业互联网体系包含网络、平台、安全三大功能

体系,实现人、机、物全面互联的新型网络,图1所示为工业互联网体系结构示意。

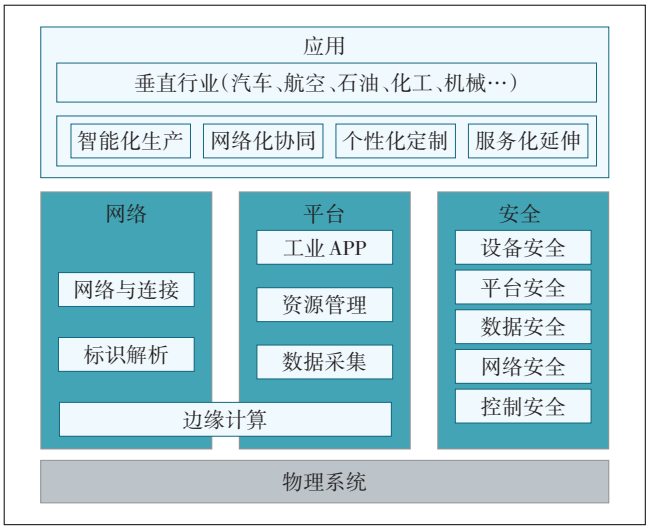

图1 工业互联网体系结构

a)网络。网络是工业互联网的基础,实现工业体系内各系统、产业链、价值链泛在互联。

b)平台。平台是工业互联网的核心,构建基于海量数据采集、汇聚、分析的平台能力。

c)安全。安全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,增强设备、网络、控制、应用和数据的安全保障能力,识别和抵御安全威胁,化解各种安全风险,构建工业智能化发展的安全可信环境。

2 工业互联网的安全体系架构

工业互联网的安全与传统信息安全及生产物理安全有根本性的区别,工业互联网所面临的复杂安全挑战,需要一套体系化的安全方案来应对,图2所示为我国当前主流的工业互联网安全体系架构示意。

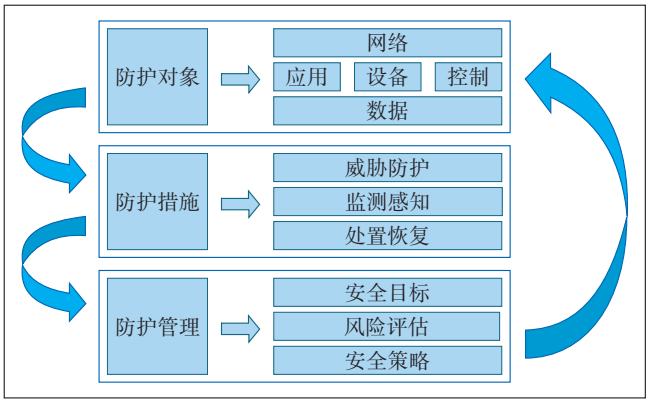

图2 工业互联网安全框架示意图

安全框架充分借鉴传统网络安全框架和国外成功实践,包含了防护对象、防护措施及防护管理3个部分,3个部分相辅相成、互为补充,形成一个完整、动态、持续的防护体系。

3 工业互联网的网络安全隐患分析

工业互联网子系统按照功能分为车间、企业、产业、平台等模块。各模块具有大规模连接、设备多样性、系统接口多等特征,其安全风险隐患主要表现在威胁对象广、危险类型多、安全风险因素多、攻击模式复杂几个方面。

按照安全框架的防护对象,工业互联网的安全工作主要聚焦在设备、控制、网络、应用和数据五大领域,本文主要对工业互联网中的网络安全领域的关键技术进行研究。

工业互联网领域中的网络安全主要指工厂内部网络和工厂外部网络的安全,其网络示意如图3所示。

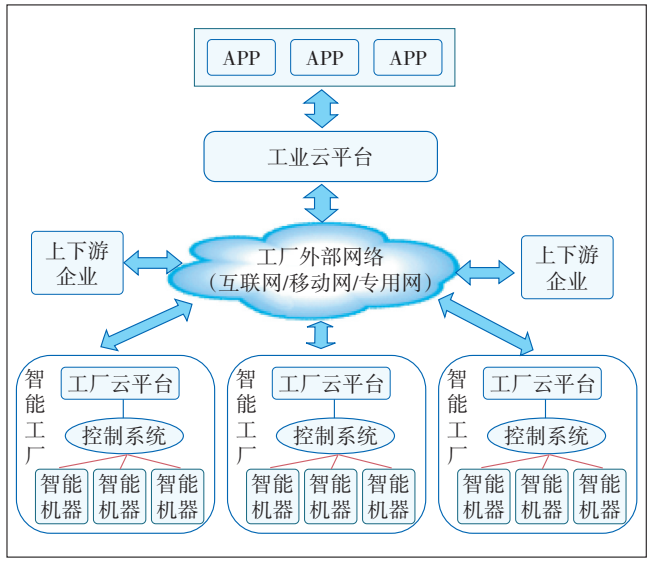

图3 工业互联网网络示意图

根据对工业互联网的网络架构及网络安全相关工作内容的分解与分析,工业互联网网络主要存在如下安全风险。

a)工厂原有的内部网络为封闭网络,原生产区域及各个设备之间未做严格的权限管控及区域隔离,在接入互联网后,带来攻击风险。

b)工业互联网包含了IT、CT、OT相关技术,其安全体系所涉及到工业互联网的攻击形态、攻击手段还未被完全掌握,基于现有的防火墙技术很难精确地定位与应对。

c）目前部分工控系统仍然使用微软 Windows 系统，由于原有的封闭网络特性导致其部分系统存在长期未升级、版本停止服务、安全漏洞无法修复等风险。

d）工业互联网的网络中传输大量的 OT 侧的控制数据，如果该类数据被劫持或者破解，将会给生产带来极大破坏的风险。

4 工业互联网网络安全防护技术

根据对工业互联网面临的网络安全风险的分析，建议将网络隔离技术、入侵检测技术、网关防病毒技术、数据加密技术应用于工业互联网的网络安全管控工作中，应对其安全风险，技术应用示意如图 4 所示。

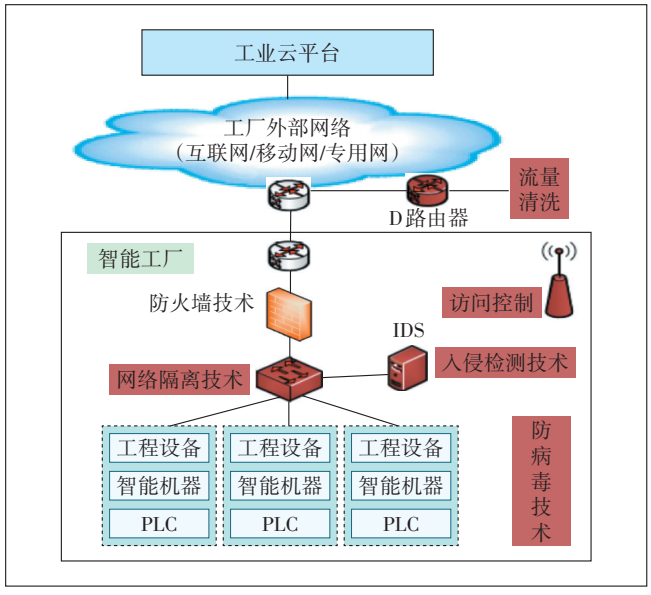

图 4　工业互联网网络安全技术应用示意图

4.1 网络隔离技术

网络隔离可以有效防止网络信息无序流转，根据系统安全等级的不同，分区域、分设备、分用户多维度隔离，当前主要有物理隔离、协议隔离和应用隔离 3 种隔离技术。

a）物理隔离。物理隔离技术主要在 OT 区域实施，可以通过网络规划进行完全的物理隔离，也可以使用网闸技术来完成物理隔离。

b）协议隔离。该类隔离技术依靠 TCP/IP 协议原理实现，如基于二层的 MAC 地址访问控制技术，基于 VLAN 的广播域控制技术，基于隧道协议（IPSec、GRE 等）的 VPN 技术。

c）应用隔离。该技术主要指在工业互联网的云平台的 SDN 的网络环境中，如容器、虚拟机、沙箱虚拟化隔离技术等。

4.2 入侵检测技术

入侵检测技术（IDS）相对于防火墙的静态防御技术，是一种主动保护自己免受攻击的一种网络安全技术，其提供了动态防御能力，整体提升了网络安全防护体系的防御能力。

在工业互联网中，很多工业控制设备在设计之初就未考虑过自己会暴露在工业互联网上，缺乏防护设计，存在很大的漏洞隐患，一旦在线运行极易被攻击，直接威胁网络安全。同时数据安全方面，因工业互联网发展产生的数据采集、汇聚，也会增加数据被泄露、被勒索攻击和被滥用的风险。工业互联网中设备众多、网络通信复杂，很难全面掌握网络中所必须的业务通信需求，防火墙的静态配置技术无法全面解决其安全风险，入侵检测技术将作为防火墙技术的有效补充，整体提升工业互联网的安全。

入侵检测技术对网络进行检测，提供对内部攻击、外部攻击和误操作的实时监控，对网络安全提供动态保护，其具有事前警告、事中防御、事后取证的特点，很好地弥补了防火墙只能作为静态防御的不足。对缓冲区溢出、SQL 注入、暴力猜测、DOS 攻击、扫描探测、木马后门等各类黑客攻击和恶意流量进行实时检测及报警。

入侵检测系统的部署示意如图 5 所示。

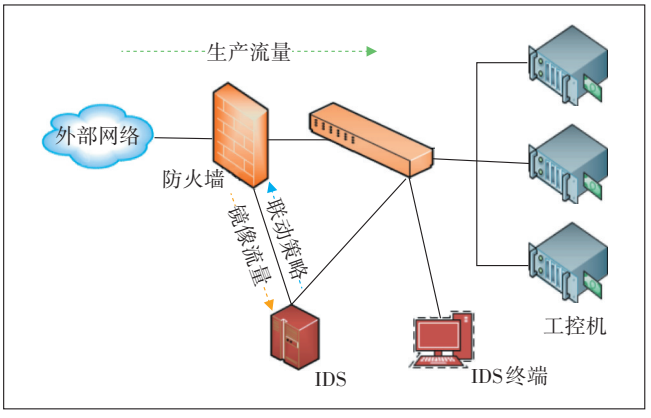

图 5　入侵检测部署示意图

部署方式采用旁路方式，从防火墙上将流量镜像到 IDS 设备，这样可以使用防火墙与 IDS 进行联动配置，提高系统整体安全。

4.3 网关式防病毒技术

传统的主机侧的防病毒系统如果在工业互联网上实施需要部署在每一台工控设备即服务器上，由于

工业系统对软件的兼容性、可靠性、稳定性要求非常高,其防病毒产品必须经过严格的测试后才能安装,因此带来适配周期长、测试样例复杂、改造成本高等诸多难以短时解决的困难,如果采用网关式防病毒技术就能够很好地规避工业互联网中防病毒软件部署困难的问题,网关防病毒示意如图6所示。

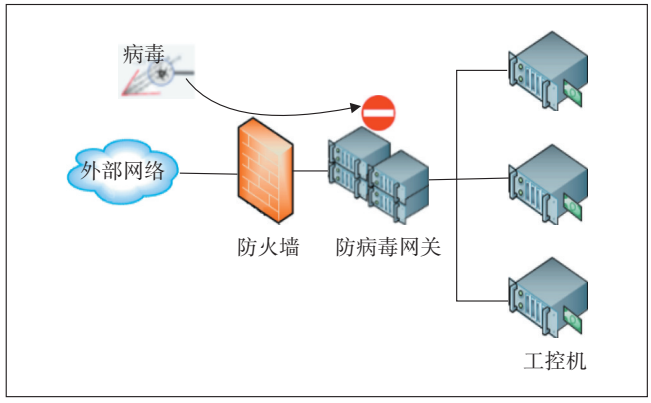

图6 网关防病毒示意图

网关防病毒技术依靠病毒特征码匹配,在网关处将数据包还原成文件进行病毒处理。该种方案将原有的分布式的主机查杀毒方式转变为集中式的网关病毒防范,对于原有工业互联网因设备老旧,系统版本厂家已经停止服务无法适配病毒软件,软件因病毒软件兼容性带来的附加改造成本均能得到很好的改善,既降低了防病毒方案的技术实现,同时也降低了防病毒系统实施的成本。

在工业互联网的系统中,防病毒网关的部署方式主要有如下3种。

a)透明模式。该模式部署简单,所有流量均进行病毒查杀,但存在单点隐患。

b)旁路代理模式。只针对引入特定协议的流量进行病毒查杀,合理配置下,成本与收益最佳。

c)旁路模式。与旁路代理模式一致,该模式只做检测,不做病毒查收,该模式更多作为已有的主机侧病毒的补充方式。

4.4 数据安全传输技术

工业互联网的网络中会传递大量OT侧控制数据,数据的密级很高,数据安全传输是非常重要的需求,可采用隧道技术方案来解决数据安全传输问题。

根据技术特点、应用场景、安全特性和工作原理对隧道技术进行分类及对比,如表1所示。

考虑到各个企业内部、外部的安全传输需求,推荐使用IPSec技术作为工业互联网的安全传输解决方案,既提供了身份认证功能,又提供了数据加密功能。

表1 隧道协议对比表

隧道协议	工作层面	身份认证	加密
SSL VPN	应用层	支持多种身份认证	支持
Sangfor VPN	传输层	支持多种身份认证	支持
GRE	网络层	不支持	简单的关键子验证
IPSec	网络层	预共享密钥;IKEV2的EAP认证	支持
L2TP	数据链路层	CHAP、PAP、EAP	不支持

5 工业互联网的网络安全技术趋势

5.1 原生安全的持续完善

在现有的工业互联网的安全实践中,由于OT网络从原有的封闭特性向开放型网络演进,其原生的网络安全设计不足的缺陷会被逐步放大,要从根本上提高工业互联网的安全基础,需要从系统的设计阶段就将系统安全性、网络安全性等综合考虑进去。

5.2 智能动态防护

工业互联网的防护对象多,防护环节长,如果整个安全体系都是依靠被动的响应防守,整个安全体系设计将庞大而冗杂,且无法做到安全事件的精准防控,因此,对于工业互联网的防护体系,未来目标需要向动态均衡、自我学习的智能动态防护体系发展,从而保障工业互联网的安全运行。

参考文献:

[1] 陈礼波,宋明泽.面向工业互联网的传输网络安全研究[J].网络安全技术与应用,2021(8):114-116.

[2] 魏强,王文海,程鹏.工业互联网安全[M].北京:机械工业出版社,2021.

[3] 田竹娟.探析工业互联网设备的网络安全管理与防护[J].互联网周刊,2021(19):40-42.

[4] 贾玉雷,韦盛中.工业互联网下的智慧电厂网络安全[J].消费导刊,2021(26):296-297.

[5] 胡佳杰.工业互联网领域网络安全服务的思考[J].IT经理世界,2019,22(12):90,92.

[6] 李崇汉,张恒.工业互联网时代的网络安全[J].现代制造,2018(27):52-53.

作者简介:
吴涛,毕业于天津大学,学士,主要从事IT运维安全管理工作;黄健,毕业于武汉理工大学,高级工程师,硕士,主要从事网络安全相关工作;郭钰璐,毕业于大连海事大学,助理工程师,硕士,主要从事网络安全技术需求分析与安全产品运营工作;杨飞,毕业于合肥学院,高级工程师,学士,主要从事网络安全技术的研究工作;赵通,毕业于中国农业大学,硕士,主要从事网络安全产品及安全技术方向的研究工作。