研究工业互联网隐私与安全等保测评

廖晓琴
（广西壮族自治区信息安全测评中心，广西 南宁 530000）

摘　要：为了解决工业互联网安全问题，本文对工业互联网隐私与安全等保测评进行研究，分析了工业互联网体系架构及安全问题，并提出了网络安全等保2.0版本的相关要求，希望可以为有关人员提供参考。

关键词：工业互联网；隐私；安全等保测评
中图分类号：TP393　　**文献标识码：**A　　**文章编号：**1004-7344(2022)04-0167-02

工业互联网中综合应用了多种技术，如云计算技术、工业控制系统、移动互联网、物联网技术、大数据技术等。是工业企业发展的主要方向，是民族工业实现网络化、集约化、智能化的渠道，关系到“中国制造2025”目标的达成。随着国内基础设施网络化的发展，工业互联网的运用得到了进一步的拓展，同时网络安全问题也引起了广泛的重视，网络攻击行为从以往的IT层渗透到运营技术层，工业企业在促进工业互联网发展中，产生了较多的网络安全问题，如果计算机系统和工业控制系统受到攻击，就会给企业及国家带来严重的损失，因此，网络空间安全已经提升到国家战略层面。

1 工业互联网安全问题

1.1 体系架构

工业互联网体系主要可以分成两个方面：①工厂内部网络。②工厂外部网络。前者主要用在连接在制品、智能机器、人、工业控制系统等，包括工厂运营技术及工厂IT网络，运营技术网络用来连接生产现场的相关部件；IT网络主要构成是以太网，基于网关设备和互联网与工厂运营技术网络进行互联及安全隔离。后者用来连接相关的主体，工业云平台中有多样化的工业应用[1]。可见，工业互联网基于以往的工业控制上，有效地应用多种技术，包括虚拟技术、云存储技术、大数据分析、云计算计算，能够将数据、设备、人以及智能资产进行结合，借助先进的技术，提升生产效率，减少资源成本，推动工业革命发展。

1.2 具有代表性的安全问题

工业领域安全主要分成3种类型，如图1所示。

以往的工业控制系统主要重视物理安全以及功能安全，也就是防止安全设备或系统失去效用，如果失效或出现故障，确保系统或设备依然能处于安全状态或进入安全状态。工业互联网背景下，安全挑战更加严峻。首先，工业互联网的安全打破了之前比较明确的责任边界，在复杂性、风险性的影响、范围上得到了扩大，各种安全问题突出。其次，工业互联网的安全工作需要立足于全局的层面上进行安排，如国家能力、制度建设以及产业支

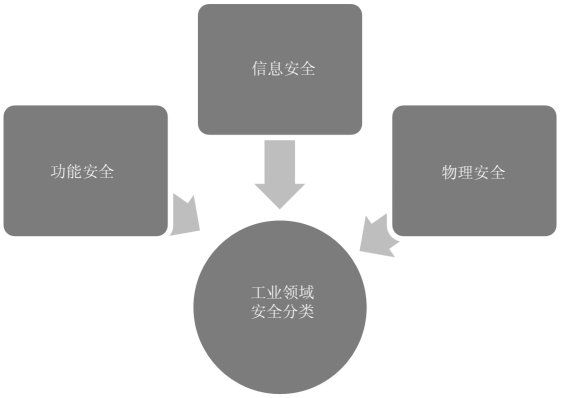

图1 工业安全分类

持等，现阶段，还有较多的企业并未认识到安全部署的重要意义，安全管理及风险防控方面存在不足[2]。

对此，安全框架应该综合的考虑功能、物理及信息安全，侧重于信息安全，解决各种新型风险，同时思考信息安全防护措施的安排对于物理及功能安全的影响。

工业互联网典型安全问题主要包括以下5个方面。

(1)设备安全问题。以往的生产设备主要是机械设备，强调功能及物理安全，未来的生产产品及装备强调集成通用嵌入式操作系统及APP，很多的设备会暴露在攻击下，木马病毒在设备间高速地传播扩散。

(2)网络安全问题。当前工厂网络的发展趋势为“三化+灵活组网”，面临的安全挑战更多。享有针对TCP/IP协议的攻击方法及手段很成熟，能够直接用来攻击工厂网络。

(3)控制安全问题。现阶段工厂控制安全侧重于控制过程的功能安全，缺乏较强的信息安全防护能力。IT及运营技术的结合，让安全的控制环境被破坏，网络攻击也延伸到运营技术层及工厂内。

(4)应用安全问题。工业应用的复杂性较高，有很多的安全需求，这就对网络安全保障能力及隔离能力提出了更高的要求。

(5)数据安全问题。工业数据呈现多维、大量、双向的趋势，主

要体现在互联网数据体量大、结构较为复杂、包含较多的种类、同时在IT及运营技术层、工厂内外双向流动共享，使数据保护变得更困难。

2 等保2.0有效保护工业互联网安全

等级保护2.0得到了进一步的推展，立足于横向角度来说，其中加入了一些新的元素，如大数据、基础信息网络等，立足于纵向角度来说，对保护对象进行拓展，移动互联网、云计算平台、物联网以及工控等系统都被包含在内。从表1中可以看到等级保护2.0的基本要求框架，对于新加入的等级保护对象，基本要求主要划分为安全通用管理及技术要求，还有安全扩展要求。

表1 等级保护2.0基本要求

测评要求	包含内容
技术要求	物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全
安全扩展要求	云计算、移动互联、物联网、工业控制系统、大数据应用安全扩展要求
管理要求	安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理

新技术促进了工业互联网的产生，不仅可以促进工业生产的高效开展，还对互联网安全提出了更高的要求。其运行需要建立在多样化的基础上，互联网安全威胁同样会威胁到工业互联网。对此，2.0标准不仅对以往的信息系统安全条款进行补充及调整，还提出了对于有关技术的安全扩展要求，为等级保护测评奠定基础。

3 云计算平台等级保护测评和存在的安全问题

编制测评指导书。云计算平台的构成部分较多，如虚拟化计算资源、设施、应用软件、硬件、资源抽象控制层等。服务模式包括基础设施、平台、软件即服务。

针对应用云计算模式的信息系统，需要组合应用《信息安全技术网络安全等级保护基本要求》(GB/T 22239—2019)中的云计算扩展要求和安全基本要求，调查研究信息系统，按照测评对象所处的角色，有目的性地选择测评要求，在此基础上，制定云计算等级保护测评指导书，为测评提供依据。

一般可以对系统中的特定高维度及低维度同时进行测评[3]。云计算的应用对安全测评工具以及技术有更高的要求，除了传统的检测工具，还要运用云安全审计、虚拟化漏洞扫描、APP云端安全检测工具等。结合具体的被测对象，选择相应的测评项。

对平台进行测评之后，归纳常见的问题，主要体现以下4个方面。

(1)架构安全问题。平台就像是一套虚拟的基础设施平台。立足于广义层面上而言，其属于软件，也就是信息系统，承载的业务应用安全等级若是比平台安全等级高，因为其是底层平台，对于业务应用具备完全控制权，如果云平台被攻击，高级业务应用同样会受到影响。大多数云租户在选择云服务时并未注重自身应用和选择平台安全等级的关系，且云服务商并未掌握租户应用安全等级情况，使等级存在不匹配的问题，产生架构安全问题。

(2)数据保护问题。当前一些云计算服务商数据安全保护能力的评估不到位，在对虚拟资源实施备份或是迁移时，可能产生错误或丢失的情况。一些服务商对于用户隐私数据的保护不到位，如缺乏健全的残余数据清除机制，导致用户信息有泄露的风险。还有一些厂商并未设置预防越权访问隐私数据的技术或制度。

(3)访问控制问题。在云计算服务模式中，计算资源主要在云平台中，公有云服务需要支持大量用户认证和接入，对于这方面的自动化管理具有更高的要求。为了优化认证接入管理体验，就要对用户认证过程进行完善，例如提供业务统一认证和权限管理平台，导致用户认证管理及访问控制的难度提升，若是认证模块被攻击，就会影响到平台中的资源，进而影响到租户的利益[4]。入侵者一般通过虚拟机进行攻击，或攻击虚拟化管理平台，通过网页或操作系统中存在的漏洞，获取用户的相关信息。这就需要设置访问控制机制，合理地制定规则。

(4)共享漏洞问题。在云计算服务中，云计算环境中的大多数资源都共同运用一套模板，也就是运用通用配置信息，如果产生配置错误会影响到系统的功能，业务稳定运行是云服务的一个重要作用，这就需要给网络及主机配置相关的制度，包括预警、告警或应急响应，保证供应商有效地安装补丁，对云计算服务进行优化。

4 结语

综上所述，工业互联网基于传统互联网产业基础上，融入了新的信息技术和工业控制技术，可以为工业智能化发展提供保障；建立工业互联网环境，需要对相关的系统、客户、管理及生产运维人员等进行互联互通，基于深度感知、实时传输交互、高效计算处理数据，实施建模，可以改善能源管控的效果，智能地进行调度，促进生产经营发展。虽然其具有显著的优势，但是应用中的安全问题不容忽视。其中的典型安全问题也为等级保护2.0制度的修订提供依据，当前信息安全等级保护制度在不断地丰富及调整，新的2.0测评对象范围可以全面覆盖所有的应用场景，因此，应该按照等级保护2.0评估工业互联网安全状况。

参考文献

[1] 孙俊杰.长扬科技：打造“技+管”安全工业互联网[J].中国工业和信息化，2021(10)：88-93.

[2] 浦巳怡.工业互联网隐私与安全等保测评[J].上海信息化，2021(10)：22-27.

[3] 彭磊.新基建时代如何保障工业互联网数据安全[J].中国工业和信息化，2021(8)：38-44.

[4] 齐云菲，李政，杨倩文，等.工业互联网安全与等级保护测评研究[J].信息系统工程，2019(6)：60-63.

收稿日期：2021-12-18

作者简介：廖晓琴(1991—)，女，汉族，广西贵港人，本科，主要从事等保测评(测评师)的工作。