大数据时代下的工业互联网信息安全研究

许应强
云南省工业和信息化厅信息中心　云南省昆明市　650000

摘　要：现如今已经全面进入互联网时代，大数据技术在各大行业得到了非常广泛的应用，给人们生活带来了更大的便利，有效推动了我国社会经济的快速发展。但与此同时也面临着更加严峻的网络信息安全挑战，如何做好工业互联网信息安全防范与控制工作是新时代全社会需要共同克服的一个问题。鉴于此，本文就基于大数据时代背景，分析工业大数据特征和现状，进一步研究大数据时代工业互联网信息安全影响因素及相应的控制措施，以期能够为工业互联网信息安全保障工作提供一定的借鉴。

关键词：大数据时代；工业互联网；信息安全；防护措施

引言：

新时代网络飞速发展，计算机技术信息处理方式越来越完善，为信息的快速传递创造了良好的基础条件。但信息安全性却受到了较大的威胁，信息泄漏问题时常发生，这就要求加强网络信息安全防护措施，营造良好的网络环境。下文就大数据时代工业互联网信息安全相关内容进行详细论述。

1　研究背景

1.1 大数据时代概述

大数据即对特定领域范围内各类数据的有效挖掘和分享，这一概念最早在2013年被提出，现如今已经广泛应用于各行业中。比如：对于企业来说，大数据主要是指企业在日常运营中所产生的结构化和半结构化数据。借助云计算或者其他数据处理技术将企业运营过程中产生的各类数据导入数据库，通过对这些数据的分析，从中挖掘出对企业经营发展具有一定指导意义的信息，进一步利用有价值的信息不断改善和优化企业的管理模式、产品制造及业务流程等，快速提升企业在行业中的市场竞争力。通过对大数据技术的合理运用，还能够快速准确定位企业的目标客户群，增强企业营销成果[1]。

1.2 大数据时代发展

众所周知，大数据时代的到来给人们日常生活和企业的运营发展都带来了巨大的改变，提供了更大的便利，但实践发现同时也存在较大的网络信息安全隐患，所以还需要不断完善网络安全问题。由于大数据时代给全社会带来的巨大改变和利好，现如今国家和各级政府部门对其发展尤为重视，同时为更好地推动大数据的良好发展制定了一系列扶持政策。由于我国大数据时代较欧美发达国家稍晚一些，所以实际发展过程中可以适当借鉴一些他们的成功经验。目前我国大数据已经实现了线上和线下产业的融合发展，相关软件和硬件也都取得了较好的发展。

2　工业大数据特征和工业互联网的概念及现状

2.1 工业大数据的特征

工业大数据其实就是指工业领域内围绕智能化制造模式，对工业产品的设计、制造、销售、存货、运维、回收及服务等所有环节产生的数据和应用技术的总称。大体可以分为设备物联数据、运营管理业务数据及外部数据三大类。工业大数据不仅具备了大数据的基本特征（大容量、多样化、实时性及价值密度低），另外还体现出较强的关联性、时序性、闭环性和准确性特征。下面就针对这些特征进行逐一介绍。

大数据容量（Volume）。随着科学技术的快速发展，特别是感知技术和传感器在工业领域的融入，工业数据大幅度增加，部分大型企业甚至可以达到EB级别。

多样性（Variety）。工业数据不仅结构复杂，而且分布也更广，在工业生产过程、管理及设备的运用等诸多环节都存在大量的数据。

实时性（Velocity）。工业生产现场要求数据具备较好的实时性，无论是数据的生成还是处理过程速度都非常快，通常情况下数据的分析速度要以毫秒来计算。

价值密度低（Value）。上面已经提到过，工业大数据结构较为复杂，其中包含了大量的非结构化数据，这

作者简介：许应强（1963-），男，汉族，云南省红河州石屏县，电子工程高级工程师，云南大学软件学院软件工程硕士，云南省享受政府特殊津贴专家，从事信息管理、电子政务、工业经济数据分析、两化融化、信息技术应用工作，就职云南省工业和信息化厅信息中心主任，单位所在地：云南省昆明市。

些数据通常体现出价值密度偏低的特征。可是数据价值是相对的，这就要对海量数据进行深入挖掘和分析[2]。

时序性（Sequence）。时序性主要是指工业大数据的处理在时间上体现出一定的先后顺序。

强关联性（Strong-Relevence）。工业生产过程中，同一时段所生产的产品相关数据之间存在紧密的关联，即使不同时段所生产的产品数据也体现出一定的关联性。

准确性（Accuracy）。工业大数据强调数据的高质量，对数据的完整性和真实性要求比较高。保证所有数据收集过程的可靠性，只有保证数据的真实性和可靠性才能为后续数据的挖掘和分析工作质量提供基础保障。

闭环性（Closed-Loop）。工业大数据的闭环性特征主要体现在，产品生产全过程各类数据的采集和处理都处于封闭的状态，该过程的顺利完成还需要对闭环场景下的状态感知、信息反馈及分析等工作进行不断完善和优化处理。

2.2 工业互联网的概念及现状

工业互联网是集人、机械设备、产品及计算机于一体的互联网，其通过对现代化数据分析法的科学运用，为工业智能化操作提供了很大的支持，进一步改变商业产出，提高企业的综合效益。也可以说工业互联网其实就是对工业诸多域的有效整合，利用互联网将工厂、生产线、产品、客户及供应商紧密联系在一起，从而形成一个跨区域和跨时间的信息互联产业链，工业互联网的有效应用有效推动了现代化智能工厂、智能制造和智慧城市的快速形成与发展，促使我国工业经济水平的快速提升[3]。

随着时代的发展和智能化、数字化以及网络化工业场景的出现，目前我国工业互联网已经进入到高速发展时期，互联网当中涌现出越来越多的工业系统和生产设备，同时也面临着一定的网络风险，如何抵御互联网安全风险也成了近些年社会各界广泛关注的一个问题。部分欧美国家针对互联网安全问题出台了一系列法律法规，比如：美国的《国家安全与个人数据保护法提案》，德国的《联邦数据保护法》等，我国在2020年也出台了《工业互联网数据安全防护指南》。

3 大数据时代下工业互联网信息安全影响因素

3.1 工业网络逐渐开放

传统网络和工业互联网设计的时候，首先要考虑的就是其开放性，由于网络终端存在一定的不确定性，所以开放性网络就为一些不法分子提供了可乘之机，他们会从中窃取一些自己需要的信息，甚至还会破坏工业级的物理实体。工业互联网其实和传统网络之间存在密切的关联，其需要借助传统互联网技术实现自身的良性运行，通信工作同样也依赖于传统网络基础设施和协议，这就使传统网络当中的漏洞给工业互联网造成了严重的威胁，而且网络攻击形式越来越多样化，只是采用传统的网络信息安全防护措施根本无法保证工业互联网信息的安全性，所以工业网络安全防护措施还需紧跟时代发展步伐不断更新和完善[4]。

3.2 工业设施操作不当

随着互联网时代的带来，企业的发展要求保证信息的畅通性和及时性，在此背景下越来越多的企业构建工业网络，以实现和其他企业之间信息的及时沟通和资源的共享，工业网络使用者持续增加，但由于部分工作者对工业网络系统的操作不够熟练，在实际操作中存在不规范行为，导致相关信息安全受到了严重的威胁。造成这一问题出现的主要原因是各操作人员的计算机使用习惯有所不同，实践中出现了一定的失误。例如，部分使用者习惯于在网络上登录个人账号的时候选择记住密码，这样就存在一定的安全隐患，容易泄漏个人信息。

3.3 互联网直接攻击

工业互联网信息安全受到最大的威胁来自于互联网的直接攻击，也就是人们经常所说的黑客攻击，他们的工业攻击目标主要包括主动性和被动性攻击两种模式。主动性攻击不仅会给工业网络信息的有效性和完整性造成严重的不良影响，而且还会在一定程度上影响工业实体的实践操作。被动性攻击只会影响工业网络信息的有效性和完整性，但工业实体操作不会受到影响。相比较而言，主动恶意攻击对工业互联网所造成的伤害更大一些[5]。各大工业生产企业在优化升级互联网软件的时候，应融入更为先进的新型技术，保证自身信息处于安全的环境当中。

3.4 工业内网病毒攻击

工业内网病毒同样来自于互联网，因为其攻击目标存在定向性，所以在互联网中的传播没有体现出攻击特征，但当其渗入工业企业内部网络之后，便可以主动探索查找一些定向目标，并对其实施工业实体攻击。这类病毒依靠传统的流过滤等常规手段根本无法查找和杀灭，而是需要结合其对工业实体的具体操作行为进行相应的模型化分析，深入分析其恶意行为并做出针对性的阻断，只有这样才能避免工业内网病毒的侵害，保护好工业实体。

4 大数据时代下工业互联网信息安全防护措施

4.1 构建大数据安全信息管理平台

大数据时代下想要保证工业互联网信息的安全性，必须构建大数据安全信息管理平台，具体可以从以下三

个方面进行着手：

首先，数据类型标准化。工业互联网信息安全管理人员需对工业生产中所产生的所有信息进行收集与整理，并根据统一的标准将标准化数据信息存储到中央处理系统当中，如此一来无论是哪种类型的信息都可以快速引擎查找，同时还实现了对信息的安全存储。其次，数据分类标准化。结合企业生产运营实际情况构建一套完善的数据标准化分类体系，从而实现对数据信息的批量化处理，提高数据分析处理效率。再次，创新信息安全管理举措。根据自身发展需求，不断研发更为先进的信息安全管理工具，丰富其使用功能，提升其集成度，为工业互联网信息管理提供安全可靠的保障。

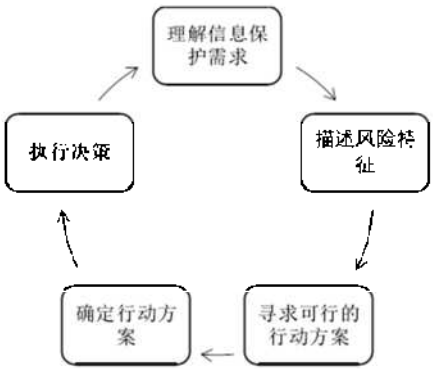

图1　风险管理过程示意图

4.2完善工业企业自身安全防御体系

进入全球互联网时代以来，各行业及企业之间的信息沟通更加畅通，为企业快速发展提供了全新的机遇，但也面临这更加严峻的网络信息安全风险，这就要求工业企业应不断建立健全自身的信息安全防御体系，可以在企业内部网络系统中安装网络安全滑动标尺模型，通过对其的合理运用提升企业网络的安全性。该模型作为现如今一种主要的工业互联网防御方式，其实际应用中可以分为五大类别：

（1）架构安全。其对工业互联网系统的规划、构建以及后期维护都有着很好的保护作用。（2）积极防御。实现对工业互联网系统各类威胁的全面分析和实时监控。（3）被动防御。在无人值守情况下做到对工业互联网的持续性防御和自动化维修。（4）情报。将数据顺利转换成系统能够识别的信息，通过对信息的进一步加工处理，很好地弥补系统中存在的缺口。（5）进攻。利用法律手段反击工业互联网中出现的一些网络攻击行为。

4.3基于威胁情报的工业互联网安全态势感知

（1）广泛收集数据信息，这是生成威胁情报最基础且最关键的一步。（2）仔细分析研究已经收集到的各类数据信息，剔除其中一些不可信的数据。（3）整理不同类型的数据，并梳理好各类数据之间的关系，明确他们之间存在的关联性。（4）利用机器学习法对情报的可靠性进行验证，为系统筛选出可信度比较高的数据。（5）情报报警内容需包含有攻击团队、攻击类型和攻击目标等相关信息。（6）根据情报进一步明确报警优先等级信息[6]。（7）按照特定格式输出情报信息，比如：PDF、STIX或者Word等。（8）根据情报类型用途，为工业互联网自主推送打包下载和安全产品等服务功能。

4.4实现工业内网安全管理可视化

大数据时代工业互联网信息安全管理过程中，促使安全管理工作可视化非常关键，其不仅能够提高系统安全分析工作人员的专业技能，而且还有效提升了情报分析效率。想要实现工业内网安全的可视化管理，具体可以从以下两个方面进行着手：

一方面，数据结构化。利用安全管理可视化技术，结构化系统中繁杂的碎片数据，像异常行为警告和威胁类警告等，逐步形成更加完善的可视化管理方案，对用户理解也具有一定的帮助作用。另一方面，实现有机结合。利用可视化技术将企业内部相关业务和威胁事件结合在一起，从而使安全态势的呈现更加直观清晰，促使所有的威胁和信息安全隐患都从以往的不可见转变成了可见的，有助于工业互联网信息的安全保护。

5　结束语

总而言之，大数据已经成为现如今社会的必然发展趋势，且在各大领域的应用越来越广泛。在此大环境下网络信息安全问题受到了人们的高度重视，只有加强信息安全保护工作，利用多样化的防护手段保护好用户的隐私，为人们提供一个良好的网络环境，才能保证工业企业的综合效益最大化，促使工业互联网的稳健发展。

参考文献：

[1]陈祥谦.互联网金融风险浅析与监管建议[J].财经界，2020（31）：37-38.

[2]贺兆林.互联网环境下计算机信息处理技术安全性研究[J].信息与电脑（理论版），2020，32（20）：11-13.

[3]徐向艺，张国平.大数据时代下计算机软件技术的应用[J].电脑编程技巧与维护，2020（10）：42-43+68.

[4]董悦，李艺，秦国英，李姗.工业互联网数据安全技术研究[J].信息通信技术与政策，2020（10）：38-41.

[5]张天明.探讨计算机网络安全[J].计算机产品与流通，2020（11）：90.

[6]罗力.新兴信息技术背景下我国个人信息安全保护体系研究[M].上海社会科学院出版社：智库论策，202011.176.