数字化转型背景下工业数据安全风险防护研究

袁琨
新余钢铁集团有限公司

摘　要：数字化转型背景下，我国企业逐渐向着智能化、数字化方向发展。工业企业作为我国经济建设的重要组成部分，要积极响应时代号召，实现工业数据的数字化转型升级。但是，在工业数据数字化转型的同时，工业数据也正面临着安全风险。本文以钢铁行业的工业数据管理为例，简要阐述工业数据安全风险防护在数字化转型背景下产生的积极作用，分析现阶段我国工业数据安全风险防护存在的问题，提出四条发展策略，为我国工业高质量发展提供参考。

关键词：数字化；工业数据安全；风险防护；钢铁企业
【DOI】10.12252/j.issn.2096-6288.2023.03.224

引言

工业数据安全风险主要是由于虚拟世界和现实世界的边界被模糊化处理，使得虚拟世界的安全风险正在向着现实世界延伸，对于经济、社会、生态等都会产生不同程度的影响。笔者所在公司为钢铁公司，本文将会以钢铁行业的工业数据安全风险情况为例，进行工业数据安全风险分析，研究相应的解决对策，降低工业数据安全风险，以期保障本行业内的可持续发展，促进行业数据的数字化转型的平稳运行。

一、工业数据安全风险防护在数字化转型背景的影响下的重要性

（一）有利于保证工业产业安全

互联网的时代主题背景下，我国钢铁工业企业利用相关工业数据，搭建了相关工业行业的虚拟世界，利用数字化技术、人工智能技术、云计算技术、物联网技术等，使得钢铁工业企业与社会各领域衔接，强化工业生产、销售、服务等环节，促进钢铁工业企业实现了跨行业发展[1]。

为了保证钢铁工业企业跨行业的顺利开展，需要针对工业数据安全建立相应的安全风险防护体系，如图1所示。利用该工业数据安全风险防护体系，避免虚拟世界的技术攻击影响现实世界的钢铁工业生产安全，促进相关行业及其上下游产业链的高质量发展。

图1 工业数据安全风险防护体系

（二）有利于促进工业企业开拓国际市场

钢铁企业工业数据的安全风险防护有利于打破传统的工业数据安全管理思想束缚，形成更为成熟的工业安全生产体系，帮助钢铁工业企业了解国际市场形势，提高相关工业企业的国际市场份额。

目前，传统的钢铁企业由于工业数据安全风险管理存在问题，导致企业对于工业数据的信任度不足，不愿意进行数字化转型。而建立工业数据安全风险防护体系能够提高企业对于互联网的信任度，促进工业生产数据信息实现安全且高效的数据共享，助力我国钢铁企业数字化转型的发展，保证工业数据信息共享过程中数据的真实性、有效性。企业可以根据供给市场需求，进行钢铁产品的动态调整，增强钢铁产品的国际市场竞争力。

（三）有利于提高工业企业的经济效益

首先，工业发展过程中，在互联网的影响下极易出现数据泄漏。工业生产数据以及重要的客户隐私等相当于工业企业的命脉，一旦数据被泄漏，对于企业而言无疑是致命的打击。而工业数据安全风险防护，将会提高工业企业生产过程中的数据信息的安全性，保证企业的长久发展，助力工业企业开拓市场。

其次，工业安全风险数据防护能够促进工业企业的多维管理，促进企业转型升级。在钢铁工业生产过程中，工业安全风险数据防护是实现智能、机械设备、材料三者的有机结合的重要基础，促进管理制度多维度发展，保证钢铁生产指标的一致性，提高钢铁产品的质量及生产效率，促进钢铁工业企业经济效益的提升[2]。

最后，在工业企业进行数据管理过程中，相应的工作人员的技术水平不足，因此，可能导致我国工业企业数据管理过程中存在操作不当的情况，造成数据的泄漏或篡改，使得工业企业面临数据风险。工业数据安全风险防护能够通过对于工业数据访问控制技术的创新，控制相应的访问权限，保证技术操作的规范性、合理性，最大程度将企业内部人员操作不当的危害的影响降至最

低。

二、工业数据安全风险防护在数字化转型背景的影响下的发展现状

（一）工业数据安全管理体系存在问题

依据我国相应的工业数据安全管理法规，要求相应的钢铁企业建立工业数据安全风险管理部门，设立数据安全管理机构及负责人，实现网格化管理。但是，目前我国钢铁行业对于网络安全管理体系的重视度不足，并未依据相应的业务领域及企业布局建立工业数据安全组织。并且，各级部门的安全责任不清，相应的钢铁数据分类分级标准建立不完善。

（二）工业数据安全防护技术存在问题

钢铁企业的工业数据安全风险防护要负责处理好工业生产过程中的重要数据及人员信息，保证数据信息在共享、交易等环节中的数据信息传输安全。在此过程中，受利益等因素的驱使，部分企业雇用专业的网络黑客团队，进行网络攻击。或是企业内部人员在利益的驱使下，进行数据泄漏。

目前，我国钢铁企业的数据安全技术还有很大的进步空间，相应的数据访问、加密等技术还应该进一步完善，保证工业生产安全。

（三）工业数据运行周期各环节存在问题

首先，从数据采集角度来看，目前我国钢铁企业的数据采集过程极易受到黑客攻击，严重影响数据信息的真实有效性。并且，不同的钢铁企业其数据类型及通信协议等不尽相同[3]。因此，难以进行统一的工业数据安全风险防护。

其次，从数据传输角度来看，钢铁企业在进行工业数据传输时，对于工业数据的时效性要求较高，传统的工业数据安全风险防护技术并不能满足工业数据传输的需求，使得工业数据在传输过程中存在着被窃听等风险。

再次，从数据储存角度来看，钢铁企业的工业数据分类及分级过程中的访问机制存在问题，在数据储存过程中存在被盗用的风险。

最后，从数据使用角度来看，钢铁企业的工业数据的结构呈现多元化、碎片化特点。传统的工业数据安全风险防护技术在数据包解析过程中，不能将数据包中的数据内容价值完全发挥出来。

（四）工业数据在开放性的互联网环境下的风险面扩大

随着互联网技术的不断发展，钢铁企业打破了传统的封闭式生产环境，数据库、工业主机等端口开放，因此极易受到病毒和木马的攻击，引发一系列的安全问题。并且，随着钢铁企业产品市场的国际化发展，钢铁企业的工业跨境数据逐渐增多，在跨境数据收集及储存的过程中，导致钢铁企业产品设计、生产等敏感数据信息等易出现数据泄漏。对于钢铁企业的生产及发展产生不利影响，影响钢铁企业的转型升级。

三、工业数据安全风险防护在数字化转型背景的影响下的发展策略

（一）出台安全风险防护标准，建立健全工业数据安全风险保障体系

一方面，在钢铁企业的工业数据安全风险防护的发展过程中，相关政府部门应该重视工业数据安全管理工作，结合行业内部的工业数据安全事故，以及相应的案例，制定相应的工业数据安全风险防护标准。工业数据安全是保证我国钢铁企业生产及发展的重要基础，相应的政府部门应该持续研制相应的工业数据安全风险防护标准，结合钢铁市场实际情况，对于工业数据安全风险防护标准进行动态调整。

另一方面，钢铁企业应该结合工业生产过程中的生产环节、数据、场景等的复杂化、多样化的特点，对于工业生产过程中的数据安全风险进行系统化评估。保证钢铁企业工业数据的细致性以及清晰性。对于钢铁企业工业生产中的环境数据及条件数据，进行数据风险分析。建立了风险数据模型，利用大数据的匹配分析，制定相应的风险应急处理策略。同时，钢铁企业必须建立相应的工业数据访问控制机制，对于任何工业数据访问人员进行人员信息登记。当工业数据访问人员的信息准确无误时，方可允许其进行工业数据访问。并且，利用算法优化设置相应的数据访问标准，一旦访问人员行为不符合访问标准时，立刻强制其退出。此外，为了保证工业数据信息的完整性、连续性、保密性，需要对于工业数据信息进行备份，一旦出现数据丢失情况，立即启用备份数据，保证工业生产的正常运行。

（二）注重安全风险防护技术创新，实现工业数据安全风险动态防护

在进行钢铁企业工业数据安全风险防护技术创新时，相应的工作人员应该在零信任架构的基础上，融合工业数据的应用场景，对于访问人员、数据使用的动态细粒度授权等进行控制，保证工业数据的应用、服务、数据库储存等实现精准防护。同时，对于工业数据的使用信息进行实时记录，敏感数据、隐私数据进行去标识处理。重点对于工业数据库的访问、检索、使用情况进行安全防护，做好差异化安全等级水平的工业数据阻截和交换管理工作，实现工业数据安全风险动态防护，促进工业生产的平稳运行。

第一，工业数据加密技术创新。利用密钥和加密函数进行工业数据的密文转换。工业数据的接收方，根据

相应的解密函数进行工业数据还原。如图2所示。其中明文是加密前的工业数据文本，密文是加密后的工业数据文本。加密转换和解密转换则是明文和密文二者之间的转化。密钥则是工业数据加密及解密过程中的算法标准。在这一技术中，可以融合过程数据检测技术，一旦数据加密过程中出现异常情况，立刻进行数据封锁，相应解锁操作，只能由相关企业的工业数据中心管理部门人员进行，最大程度上保证工业数据安全。

第二，工业数据安全防火墙技术创新。建立多层防火墙架构，从工业数据网络、应用、储存三方面入手。全方位抵御外部网络的技术攻击，保证工业数据的安全性。同时，对于工业数据防火墙技术的软、硬件设备进行优化升级，将防火墙技术的功能充分发挥出来。

第三，工业数据访问控制技术创新。在进行钢铁企业工业数据访问控制技术创新过程中，要对于访问控制策略及访问权限进行预先定义。在访问权限使用的全过程中进行数据检测，保证钢铁企业工业数据信息资源不会被技术入侵。一方面，要对于访问者的身份进行认证，访问者将身份信息上传到云端后，系统会进行自动分析与比对，确认信息无误后，启动人脸识别及指纹识别系统，最大程度上保证访问人员信息准确无误。另一方面，对于钢铁工业数据信息进行分级处理，不同等级的数据信息要进行不同的标记，访问者只能访问他这一等级的工业数据信息。

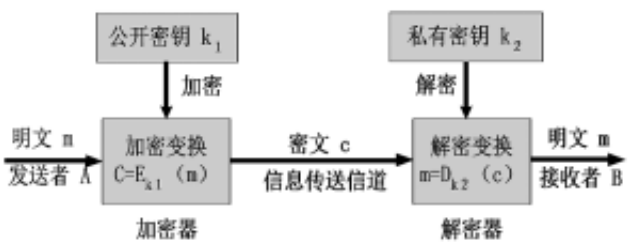

图2 工业数据加密流程图

（三）创新工业数据安全供给渠道，延长工业数据安全产业链

多方联动，共同促进工业数据安全风险防护体系的高质量发展。政府、相应的工业企业、专业院校、社会机构等合作，联合建立工业数据安全风险防护技术创新研究中心，设置相应的激励机制，充分调动各方参与热情，促进技术成果转化。对于研发成果进行工业数据安全防护技术测评，安全防护效果较好的工业安全风险防护技术可以进行物质奖励或政策奖励，激发各方的技术研究热情，延长工业数据安全产业链[4]。

同时，重视人才培养，加大对于工业数据安全风险防护人才的培养，完善人才选拔及考核机制，定期组织工业数据安全风险防护比赛，“赛证”结合，为后期企业人才选拔提供一定的参考标准。提高工业数据安全风险防护人才数量与工业企业需求之间的协调性，为我国相关工业企业的转型升级奠定人才基础。

（四）重视工业业务全流程，形成科学合理的工业数据安全建设思路

充分结合钢铁企业的差异化、碎片化、专业化、技术化等行业特点，对于钢铁企业的业务场景、法律标准等进行系统化考量，对于钢铁行业的上下游关键业务领域进行分析及业务划分，完善各业务领域的工业数据安全系统体系。

构建常态化、内生化、智能化、制度化的工业数据安全防护机制。首先，建立常态化的工业数据治理体系，对于钢铁企业的工业数据资产进行日常风险分析，保证钢铁企业工业数据安全风险防护与企业常态化业务管理相融合。其次，建立内生化的工业数据技术管理机制，通过建立工业数据安全风险防护技术体系，将钢铁企业的数据安全防护技术与企业业务建设相融合，实现钢铁企业建设全过程的工业数据安全风险防护。再次，建立智能化的工业数据安全运营系统，设置钢铁企业工业运营风险告警机制，对工业运营全过程实现闭环管理，提高钢铁企业工业数据安全运行效率。最后，建立制度化的工业数据管理模式，将相应的企业管理方法与工业数据安全风险防护的各应用场景相融合，成立专门的工业数据安全管理部门，优化相应的工业数据安全管理流程，实现工业数据管理模式的制度化发展。

结语

综上所述，通过对于钢铁企业的工业数据安全风险防护策略的探讨，我国其他的工业企业可以结合钢铁企业数字化转型经验，进行本行业的工业数据安全防护技术创新。工业数据的智能化发展是时代发展的必然趋势，相关企业应该顺应时代潮流，在数字化转型的过程中，重视工业数据安全防护工作，促进我国经济发展。

参考文献

[1]韩佳琳，曹诗南，章蕾，等.数字化转型背景下工业数据安全风险与应对分析[J].通信世界，2022（14）：30-31.

[2]朱雅麟.企业数字化转型中的风险识别与预警机制研究[J].中文科技期刊数据库（全文版）经济管理，2023（7）：0001-0004.

[3]龚志杰.试论工业互联网信息安全问题及防护技术[J].中国信息化，2022（9）：67-68.

[4]闫寒，李端.工业互联网安全风险分析及对策研究[J].网络空间安全，2020，11（2）：81-87.