 DOI: https://doi.org/10.12345/gcjsygl.v7i12.13152

Research on Network Security Risk Assessment and Prevention Strategy of Industrial Control System

Liquan Sun

Qinghai Yellow River upstream Hydropower Development Co., Ltd. Longyangxia Power Generation Branch, Hainan, Qinghai, 813000, China

Abstract

With the development of industrial control system, under the continuous promotion of information technology, the industrial control system gradually presents the development trend of network, information, intelligent and network. However, with the gradual increase of industrial control system network security problems, many countries have issued relevant policies and regulations to regulate and restrain the network security problems of industrial control system. In recent years, China has also issued relevant policies and regulations to regulate and restrain the development of industrial control system. Network security risk assessment of industrial control system is an effective method to find and identify the network security risks of industrial control system, which is a process of continuous accumulation and continuous improvement. This paper analyzes the current situation and existing problems of the network security risk assessment of the industrial control system in China, and puts forward the corresponding countermeasures and suggestions, in order to provide reference for the network security risk assessment and prevention of the industrial control system in China.

Keywords

network security; industrial control system; vulnerability; network attack

工控系统网络安全风险评估及防范策略研究

孙黎全

青海黄河上游水电开发有限责任公司龙羊峡发电分公司，中国·青海 海南 813000

摘　要

随着工业控制系统的发展，在信息化技术的不断推动下，工业控制系统逐渐呈现出网络化、信息化、智能化、网络化的发展趋势。然而，随着工业控制系统网络安全问题的逐渐增多，许多国家都发布了相关的政策法规对工业控制系统网络安全问题进行规范和约束。近年来，中国也出台了相关政策法规以规范和约束工业控制系统的发展。工控系统网络安全风险评估是一种有效地发现和识别工控系统网络安全风险的方法，是一个不断积累、不断改进的过程。论文分析了中国工控系统网络安全风险评估现状及存在的问题，并提出了相应的对策建议，以期对中国工控系统网络安全风险评估和防范工作提供参考。

关键词

网络安全；工控系统；漏洞；网络攻击

1 引言

工控系统是指在工业领域中，由计算机控制的可在特定环境下运行的各种设备，包括生产控制、管理和监控等。工业控制系统网络安全是指控制系统在正常运行过程中受到恶意代码的攻击，导致控制系统发生故障或者数据泄露[1]。随着信息化技术的发展，工业控制系统网络安全问题逐渐增多，特别是近几年发生的一系列信息安全事件，如“震网”病毒、“勒索病毒”等，使得工业控制系统网络安全问题引起了高度重视。从国内外的研究来看，工业控制系统网络安全问题主要体现在以下几个方面：①工控系统自身存在漏洞；②工控系统的通信协议存在漏洞；③工控系统自身被植入病毒或木马；④工控系统被黑客攻击。基于以上分析，论文对中国工控系统网络安全风险评估现状及存在的问题进行了深入分析，并提出了相应的对策建议。

【作者简介】孙黎全（1995–），男，中国青海湟中人，本科，助理工程师，从事电气二次专业和自动化、网络安全、智能化研究。

2 概述

工业控制系统（Industrial Control System，简称 ICS）是指在生产、过程、设备和管理过程中使用信息和通信技术进行信息交换的系统。随着 IT 技术的发展，计算机技术和网络技术广泛应用于工业生产过程，使得工业控制系统与信

息社会融合越来越紧密，工控系统也越来越复杂。目前，工控系统的网络安全形势十分严峻，威胁着整个工业生产过程的安全。近年来，工业控制系统被利用攻击破坏事件时有发生，对国家安全和社会稳定构成了巨大威胁。2012 年 11 月 15 日，美国政府宣布对伊朗石油行业进行制裁；2016 年 10 月 1 日，俄罗斯和乌克兰爆发了针对能源行业的网络攻击事件；2016 年 10 月 17 日，伊朗首都德黑兰遭勒索病毒攻击，造成数千人死亡；2017 年 6 月 28 日，伊朗发生的核设施网络攻击事件等。

3 工控系统风险

3.1 工控系统风险评估

工控系统网络安全风险评估是指通过对工控系统的信息技术应用和网络安全风险进行辨识、分析和评价，找出工控系统中存在的威胁、脆弱性以及由此产生的影响，从而对工控系统所面临的网络安全风险进行评估，并提出相应的防护措施。

由于工控系统是工业企业重要的基础设施，一旦受到攻击，会造成严重后果。因此，国家对工控系统网络安全风险评估高度重视，制定了《工业控制系统信息安全行动计划》《工业控制系统信息安全指南》等相关政策法规，规范了网络安全风险评估工作 [2]。

从中国工控系统网络安全风险评估工作情况来看，目前中国对工控系统网络安全风险评估工作尚处于起步阶段，还存在一些不足。

3.2 风险等级划分

为了便于评估，根据工业控制系统的特点，论文将风险划分为 4 个等级。其中，工业控制系统信息安全风险等级最高，这是因为工业控制系统的安全性和可靠性要求更高，因此其网络安全风险也就更高；工业控制系统网络安全风险等级最低，这是因为工业控制系统的主要功能是控制生产过程和设备的正常运行，不需要太多的信息交互，因此其网络安全风险也就较低。综上所述，根据工控系统网络安全风险的评估结果可知：工控系统网络安全风险等级为 2 级的比例最大，达到了 72.09%。

由于工业控制系统与社会基础设施（如水、电、气等）和关键基础设施（如交通、金融、电力等）之间联系紧密，且容易受到攻击和破坏，因此一旦发生安全事故可能会对社会稳定造成较大影响。因此，对工控系统进行网络安全风险评估及等级划分时应注意其对社会稳定的影响。

4 工业控制系统网络安全标准规范

标准是促进产品研发、生产和使用的基础，是产品质量的保证。国家工业控制系统信息安全标准化技术委员会（简称“信安标委”）是工业控制系统网络安全标准化技术委员会的秘书处单位，负责制定与实施国家工业控制系统信息安全标准化相关的技术标准。

信安标委现有工作组 8 个，分别负责制定与实施网络安全、信息安全相关的国家标准和行业标准，并在国家网络与信息安全标准化技术委员会内承担部分工作，同时负责组织、协调与工业控制系统相关的国家标准和行业标准的制修订工作。

信安标委成立以来，在国家工业控制系统信息安全标准化技术委员会指导下，完成了网络安全国家标准体系构建、国家网络安全标准制定、重点行业领域标准制修订等工作，有效促进了中国工业控制系统网络安全标准化工作的开展，并取得了显著成绩。

5 国内外工业控制系统安全风险评估工作现状

随着信息化技术的不断发展，网络安全事件越来越频繁，网络安全风险越来越严重。因此，许多国家都相继出台了相关政策法规来规范和约束工控系统网络安全问题。近年来，中国也不断加大对工控系统网络安全的重视程度，积极开展相关工作。2014 年 3 月，工业和信息化部出台了《工业控制系统信息安全管理办法》；2015 年 12 月，工业和信息化部制定了《工业控制系统信息安全防护指南》；2016 年 2 月，中国互联网信息办公室发布了《互联网信息服务风险预警通报（第二期）》；2017 年 3 月，工业和信息化部印发了《关于加快推进网络安全产业发展的指导意见》；2017 年 6 月，工业和信息化部发布了《工业控制系统信息安全防护指南》。这些政策法规和规范性文件的发布，为中国工控系统网络安全风险评估工作的开展提供了政策和法规依据。国外对于工控系统网络安全风险评估的研究和发展也有一定的成果。例如，美国的联邦贸易委员会（FTC）、欧洲联盟（EU）、日本产业省厅等机构均已颁布了有关工控系统网络安全的风险评估规定。

6 工控系统网络安全风险存在的问题与对策

6.1 存在的问题

工控系统网络安全风险评估在中国已经有了一定的发展，但在实施过程中仍然存在一些问题，主要表现在：一是对工控系统网络安全风险评估认识不足，仍然存在着“重建设轻运维”的思想，只对新建、改建项目进行网络安全风险评估，对已建项目开展定期或不定期的安全风险评估。二是缺少统一的工控系统网络安全风险评估规范和标准，尚未形成一套完整的工控系统网络安全风险评估体系。三是对工控系统网络安全风险评估工作重视不够，缺少相关技术人员和专门的管理人员，导致在风险评估过程中缺少相应的技术支撑。四是缺乏工控系统网络安全风险评估支撑平台，工业控制系统网络安全风险评估缺乏有力的技术支持和管理保障，难以实现全面有效的网络安全风险评估工作。

6.2 对策建议

工控系统网络安全风险评估是一个长期的过程，需要从顶层设计着手，建立起一套完整的体系和标准，并逐步完

善相关技术方法和工具。首先，需要加快工控系统网络安全风险评估相关国家标准、行业标准等标准的制定工作，建立起一套完善的标准体系，为工控系统网络安全风险评估工作提供统一的指导依据。其次，需要在现有技术方法和工具的基础上，不断积累经验、改进方法、创新工具，在实践中逐步完善相关技术方法和工具。再次，需要加强工控系统网络安全风险评估标准、技术方法和工具的推广应用。最后，需要建立起一支高水平、专业化的网络安全风险评估人才队伍，为工控系统网络安全风险评估工作提供强有力的人才支撑。

6.3 风险防范策略

针对以上工业控制系统网络安全风险，论文提出了以下防范策略：

①增强人员安全意识，加强对工控系统的管理，加强人员培训。工控系统的管理员必须具备网络安全意识，通过定期培训增强相关人员的安全意识和防护能力。

②完善工业控制系统的管理制度。在现有基础上，建立工控系统管理制度和管理流程，加强对生产数据的监控和管理，以及时发现工业控制系统中存在的漏洞和隐患。

③加强工控系统设备的管理与维护。通过定期检查，及时发现设备故障，并采取措施对设备进行维护。

④完善相关法律法规。针对工控系统中存在的漏洞和隐患，尽快制定相关法律法规对工控系统进行监管，确保工业控制系统的安全稳定运行。

7 典型应用

中国的工业控制系统主要由两部分组成，分别是以现场总线为基础的集散控制系统和以太网为基础的工业以太网。工控系统通常是在 IT 和 CT 技术的基础上发展而来的，通过无线或有线方式与终端设备连接，并通过以太网进行通信。中国工控系统中存在大量的通信协议不规范、通信协议漏洞等问题，导致信息无法共享，容易受到攻击。随着近年来网络与信息技术的迅速发展，工控系统也在不断升级和优化。工业控制系统的发展趋势是向智能化和数字化方向发展。其中，由于工业控制系统本身的特点，其安全问题与普通计算机相比更加复杂、严重和突出，因此有必要采取相应的对策以保障工业控制系统安全稳定运行。

8 结语

论文主要研究了中国工控系统网络安全风险评估现状及存在的问题，并从评估工作机制、评估标准体系建设、人才队伍建设等方面提出了相关建议。目前，中国工控系统网络安全风险评估工作机制还不够完善，评估标准体系也不够健全，且缺乏相应的人才队伍建设。在未来的工控系统网络安全风险评估工作中，需要进一步完善相关工作机制，并加强对风险评估人才的培养。只有建立健全相关工作机制和人才队伍建设，才能切实保障中国工控系统网络安全。

参考文献

[1] 王小山,杨安,石志强,等.工业控制系统信息安全新趋势[J].信息网络安全,2015(1):6.

[2] 温晓明,贾斌.工业控制系统网络安全存在的问题及改进措施[J].设备管理与维修,2019(15):3.