智慧化工生产过程中工控网络安全风险评估与防范

马润泽
国能新疆化工有限公司　新疆　乌鲁木齐　830019

摘　要：随着智慧化工时代的到来，工控网络已经成为了化工生产中重要的信息技术基础设施，但同时也带来了网络安全隐患。本文通过分析工控网络的结构和特点，对工控网络安全风险进行评估，并提出相应的防范措施，以保障化工生产安全。

关键词：智慧化工；工控网络；安全风险评估；防范措施

引言：当今世界，工业互联网已成为与电力、煤炭、化工、新能源等领域深度融合的新兴网络生态。工控网络已经成为了化工生产中重要的信息技术基础设施，它与化工设备和工程技术紧密结合，实现了数据的采集、处理和控制，为化工生产的数字化、自动化和智能化提供了有力的支撑。然而，工控网络也带来了安全隐患，黑客攻击、病毒入侵、数据泄露等网络安全事件层出不穷，给工控网络的稳定运行和数据安全带来了不小的威胁。因此，对工控网络安全风险进行评估和防范显得尤为重要。

1 国内工控安全发展现状

工控安全是工业生产运行过程中的信息安全、功能安全与物理安全的统称，涉及工业生产各个环节，其核心任务就是要通过监测预警、应急响应、检测评估、功能测试等手段确保工业业务稳定可靠运行。当前，随着全球网络安全形势深刻变化以及工业互联网深度融合形态快速发展，工控安全形势更加复杂严峻，总体来看，工控安全有四个特征。一是涵盖主体多，包含设备安全、控制安全、网络安全、应用安全以及数据安全。二是影响范围广，工控网络联通了工业现场与办公网，使网络攻击可直达生产一线。三是造成损失大，网络安全和生产安全交织，安全事件危害更严重。工控一旦遭受攻击，不仅影响工业生产运行，甚至会引发安全生产事故，给人民生命财产造成严重损失，甚至还将危害国家总体安全。四是防护复杂多样，工控安全防护思路需在分域隔离基础上，同步加强动态、协同、体系化安全防护。

2 智慧化工生产过程中工控网络的结构和特点

2.1 工控网络的结构和功能特点

工控网络是指用于控制生产过程、监测生产状态和管理生产资源的网络系统。它是化工生产中的重要信息技术基础设施，主要由控制器、传感器、执行器、计算机、服务器、交换机等组成。

2.2 工控网络的主要特点有以下几点：

高度集成化：工控网络的设备和系统集成程度非常高，包括传感器、控制器、执行器等多种设备，它们之间相互依存、相互支持、相互控制。这种集成化的特点使得工控系统更为复杂和灵活。

实时性和可靠性：工控网络的主要特点是对实时性和可靠性要求极高，需要能够在快速变化的生产环境中及时响应，维护生产的连续性和稳定性。

可编程性：工控网络可以通过编程来完成控制和管理任务，根据生产需求进行设置和调整。工控网络具有可编程性的特点，可以实现生产自动化和智能化。

多样化：由于工业自动化的发展，工控网络系统越来越多地采用多种通讯标准，网络拓扑结构也日趋复杂。对于这种多样化的特点，网络安全防护措施需要随之不断升级和改进。

分层结构：工控网络分为控制层、数据层和通信层三个层次。控制层是指控制器和控制器之间的网络；数据层是指数据采集和处理的网络；通信层是指与外部通信的网络。

专用协议：工控网络通常采用专用的通讯协议，如MODBUS、PROFIBUS、CAN等，与普通网络通讯协议不同。

硬件设备：工控网络的硬件设备具有较高的实时性和可靠性要求，如基于硬件的装置控制器（PLC）、接口卡等。

安全性要求：工控网络的安全性要求较高，因为它涉及到工业控制和生产安全等重要领域。此外，工控网络中往往涉及到大量机密信息和成本高昂的专利技术，信息泄露和数据盗取可能会给企业带来严重的损失。

2.3 工控网络的系统漏洞

在工控网络中，由于其特殊的设计和应用环境，其系统漏洞主要表现在以下两个方面：

设计和实现漏洞：工控网络系统设计和实现中存在

一定的安全漏洞，如系统配置不安全、缺乏加密和认证方式、接口系统存在缺陷等。

系统管理漏洞：工控网络管理存在一定的漏洞，主要表现在安全管理不够严格、系统更新不及时、人为疏忽等方面。

工控网络的系统漏洞会给化工生产带来严重的危害，主要表现在以下方面：

（1）生产事故：攻击者可以利用工控网络中的漏洞，通过远程控制系统来实施破坏行为，达到刻意破坏、损坏设备的目的。这样就会导致生产事故的发生，给化工生产带来巨大的经济和社会损失。

（2）生产安全问题：攻击者可以攻击控制设备和传感器，窃取、篡改和破坏数据等，从而影响化工生产安全和产品质量，给企业带来重大的财产和声誉损失，甚至威胁到国家安全。

（3）信息泄露：攻击者可以借助工控网络中的漏洞，获取企业重要信息或敏感数据，如生产计划、产品研发成果、企业隐私等，在产业链中借助信息泄露，获得利益。

（4）可靠性受损：攻击者可以利用工控网络中的漏洞，对关键设备进行破坏或者操作，从而导致系统出现工作异常，引起生产运行延迟和生产设施损坏。这将对生产系统的可靠性和稳定性产生极大的负面影响。

因此，对于工控网络的漏洞和安全问题，化工企业需要高度重视，采取有效的安全策略和防范措施，确保生产安全和信息安全。

综上所述，工控网络的漏洞主要受到设计和实现阶段以及系统管理阶段两方面因素的影响，因此安全防护措施需要针对性地优化。

3 智慧化工生产过程中工控网络安全风险评估

工控网络的安全风险评估主要包括以下方面：

3.1 网络拓扑结构评估：评估工控网络的拓扑结构是否合理，是否存在单点故障和冗余连接等问题。

网络拓扑结构评估是对工控网络拓扑结构进行评估，以判断网络结构是否合理，是否存在单点故障、冗余连接等问题。主要的评估方法包括以下几个方面：

（1）网络结构拓扑评估：对网络的物理结构和逻辑结构进行评估，确定网络设备的位置和连接方式，是否符合安全基本原则和技术规范。

（2）网络可用性评估：评估网络的可靠性和可用性，包括网络的冗余性设计、备份和恢复等方面，确保网络的稳定性和高可用性，减少因单点故障引起的停机时间。

（3）网络性能评估：评估网络的带宽、延迟、吞吐量等性能指标，以保证网络的高效运行和及时响应请求。

（4）网络安全评估：评估网络的安全性能，包括防火墙、入侵检测、反病毒等安全措施，以保障网络数据的安全和保密性。

（5）网络管理评估：评估网络的管理和维护管理水平，包括硬件设备的更新、软件升级、备份和灾难恢复等管理流程，以确保网络能够长期稳定运行。

3.2 网络通信评估：网络通信评估是对工控网络通讯协议和安全机制进行评估，以判断通信方式是否安全可靠，是否容易被攻击或破解等问题。主要的评估方法包括以下几个方面：

（1）通讯协议评估：评估工控网络所使用的通讯协议是否符合安全规范，是否容易被破解或攻击。需要关注协议的数据加密、身份验证、鉴权等安全机制。

（2）网络通讯安全评估：评估工控网络通信安全的机制和措施是否到位，比如加密方式、数据完整性验证、攻击检测等方面。

（3）通讯网络架构评估：评估工控网络的通讯网络结构和拓扑，要确保通信链路的可靠性、安全性和实时性。

（4）无线通讯评估：评估无线通讯网络与有线网络通讯的安全和可靠性，尤其需要关注无线网络的身份验证、数据加密等安全机制。

（5）通讯组件评估：评估工控网络的通讯组件，如网卡、路由器、交换机等设备的配置是否安全可靠，是否容易受到攻击或破坏。

3.3 网络访问控制评估：评估工控网络对外部的访问控制措施是否有效，是否容易受到黑客攻击或内部攻击等问题。网络访问控制评估是对工控网络对外部访问的控制措施进行评估，以判断是否有效，是否容易受到内部和外部的攻击等问题。主要的评估方法包括以下几个方面：

（1）访问控制策略评估：评估网络的访问控制策略是否实施合理，能否有效防止恶意访问。要考虑授权策略、用户审批权限等方面。

（2）用户身份验证评估：评估网络的用户身份验证机制是否安全可靠，比如密码复杂度设置、登录次数限制、自动注销等安全措施。

（3）内部访问控制评估：评估内部员工和设备的访问控制机制，比如权限控制、授权管理等方面，以防止内部人员利用其权限进行不当操作或窃取数据等。

（4）外部访问控制评估：评估外部人员和设备的访问控制机制，通过防火墙、VPN等安全手段，限制外部人员的访问权限，从而防止黑客攻击，恶意破坏等事件。

（5）事件监控评估：评估事件监控机制，及时发现、报告任何异常事件，如登录失败、攻击行为等，以及响应事件的方式。

3.4 物理安全评估：物理安全评估是对工控网络物理

安全措施进行评估，以判断设备的物理安全措施是否完善，是否容易被人为破坏或损坏等问题。主要的评估方法包括以下几个方面：

（1）安全设施评估：评估工控设备的安全设施，如摄像头、门禁、警报器等，以确保设备的安全运行。

（2）工控设备布置评估：评估工控设备的布置是否符合安全要求，是否容易被人为破坏或损坏，考虑到设备的位置、布线和安装方向等因素。

（3）机房环境评估：评估工控设备所在机房环境的安全性和可靠性，包括供电、空调、防火等方面，以确保设备可以长期稳定运行。

（4）外部设备接入评估：评估外部设备的接入，采用防毒软件等安全措施防范来自外部的攻击事件。

（5）数据备份评估：评估工控数据备份的安全性和实用性，根据业务需要和安全策略进行数据备份，减少因数据丢失或损坏而产生的风险。

4 智慧化工生产过程中工控网络安全防范措施

随着工业4.0和智能化生产的快速发展，工控网络安全已经成为企业信息安全的一个重要方面。在智慧化化工生产过程中，工控网络被广泛应用于生产控制和数据采集等环节，如若工控网络的安全防范措施不到位，极有可能造成企业财产损失、生产事故等严重后果，甚至危及企业整体安全。

因此，智慧化化工企业需要实施强有力的工控网络安全防范措施，防范和应对各种安全威胁和攻击，从而保护企业业务信息和生产过程的安全和稳定。一方面，这将有助于提高企业的工控网络管理水平，显著提高企业的安全保障能力，构建自身体系强大的安全保护垫；另一方面，这也将有助于企业的生产自动化和智能化、数字化，提高产品质量和服务水平，更为重要的是，是企业在市场竞争中占有更有竞争力。

综上所述，智慧化工生产过程中强化工控网络安全的防范措施具有重要的现实意义和深远的发展意义。企业应加强安全意识和管理水平，制定全面的安全规范和措施，并及时更新和升级安全防范技术，提升工控网络的安全性和可靠性，以更好地保证企业信息安全和发展。

4.1 安全防范政策和规范

（1）制定完善的网络安全策略：建立和完善公司网络安全管理制度和操作规程，规范安全管理流程和控制要求，提高安全意识和管理水平。

（2）加强教育和培训：加强对员工的安全教育和培训，提高安全意识和技能，加强安全保护意识。

（3）安全管理职责：建立明确的安全责任体系，制定安全责任分工方案，明确各岗位的安全职责和权限。

（4）安全规范引进：借鉴国内外先进的网络安全制度和标准，将其引入到公司网络安全管理中，规范公司网络安全管理。

4.2 访问控制与认证

强化密码安全：设置复杂密码必训练员工恰当的密码保护和管理方法，密码长度，有效期，容错次数等方面进行规范管理。

（1）认证技术应用：加强对访问用户身份的认证，采用双因素认证和身份验证等技术手段，确保网络用户的身份合法性。

（2）访问授权管理：对内部员工和外来人员的访问控制进行审批和授权，配置严格的访问权限，限制外来人员的访问权限。

4.3 网络安全监控

（1）安全监控技术：选择符合公司业务需求的安全监控设备和技术，并进行合理的网络安全监控方案设计。

（2）安全事件监控：建立安全事件监测系统，能够及时发现、报告任何异常事件，如登录失败、恶意攻击、入侵等。

（3）安全漏洞监测：对网络安全漏洞进行评估和漏洞扫描，及时查找和修补系统漏洞，提高网络的安全性和稳定性。

4.4 数据备份和恢复

（1）建立定期备份制度：对产业信号、工控管家的数据库，加强数据备份策略，建立有效的数据备份和恢复机制，保障数据流畅及数据库的故障恢复。

（2）数据恢复准备：制定完善的数据库恢复计划，明确数据恢复的步骤和方法，保障数据的高效恢复和业务的快速恢复。

以上是智慧化工生产过程中工控网络安全防范措施的主要内容，建议按照实际情况制定完善的安全防范政策和规范，并建立完善的安全管理体系，加强对网络安全的监控、管理和维护，提高网络安全保护能力，提高企业的智慧化和信息化管理水平。

结语：在智慧化工的背景下，工控网络的安全风险日益成为化工生产中的重大安全隐患。本文通过对工控网络结构和特点的分析，进行了安全风险评估和防范措施的提出，对保障工控网络安全和化工生产安全具有重要的参考价值。

参考文献

[1]王冬梅. 工控系统网络安全评估方法研究[J].现代电子技术,2018(4):71-74.

[2]章靖. 工业控制系统中的网络安全综述[J].光电技术应用,2018,33(5):43-45.