核电厂DCS系统网络安全现状分析

Analysis of
Cyber Security Status of
DCS System in
Nuclear Power Plant

生态环境部核与辐射安全中心　著

中国环境出版集团

核电厂DCS系统网络安全现状分析

Analysis of Cyber Security Status of DCS System in Nuclear Power Plant

生态环境部核与辐射安全中心 著

中国环境出版集团 · 北京

图书在版编目（CIP）数据

核电厂DCS系统网络安全现状分析/生态环境部核与辐射安全中心著. —北京：中国环境出版集团，2018.12
ISBN 978-7-5111-3888-0

Ⅰ. ①核… Ⅱ. ①生… Ⅲ. ①核电厂—计算机网络—信息安全—研究 Ⅳ. ①TM623-39

中国版本图书馆CIP数据核字（2018）第300570号

出 版 人 武德凯
责任编辑 董蓓蓓
责任校对 任 丽
封面设计 宋 瑞

出版发行 中国环境出版集团
（100062 北京市东城区广渠门内大街16号）
网 址：http://www.cesp.com.cn
电子邮箱：bjgl@cesp.com.cn
联系电话：010-67112765（编辑管理部）
010-67113412（第二分社）
发行热线：010-67125803，010-67113405（传真）
印 刷 北京建宏印刷有限公司
经 销 各地新华书店
版 次 2018年12月第1版
印 次 2018年12月第1次印刷
开 本 880×1230 1/32
印 张 3.5
字 数 80千字
定 价 20.00元

本书编写人员

主 编　刘景宾　杨安义

编 者　刘景宾　杨安义　张云波　卞玉芳

　　周　林　乔　宁　曾　瑞

校 核　王忠秋　王晓峰　初起宝

前　言

自 2010 年伊朗“震网”病毒爆发以来，网络安全逐渐成为国内外关注的热点。之后，英国、韩国等国核电厂先后发生了信息泄露等事件，更是引发了公众的广泛关注。当前，我国大部分核电厂都采用了数字化仪表和控制系统（以下简称“数字仪控系统”）。数字仪控系统在提高核电厂安全性和经济性的同时，也给核安全带来了新的威胁与挑战，网络安全是其中之一。有意或无意的网络攻击，可使核电厂相关系统和设备的可控性和可用性以及信息和数据的保密性和完整性受到损害，威胁生命和环境安全，甚至是国家安全。因此，加强核电网络安全对于确保核安全具有重要的现实意义。

根据核安全审评要求，国内多个核电厂已开展了网络安全评估，从技术和管理两方面对数字仪控系统的网络安全可能面临的风险进行了分析，并对评估中发现的问题和薄弱环节进行了初步的整改和加强。同时，部分核电厂还制订了针对网络攻击的应急预案。从相关审评情况和经验反馈来看，虽然核电领域的核电厂、设计院、供应商等单位已经就核电

网络安全开展了一些工作，取得了一些成绩，但当前仍存在一些问题，主要有国外产品网络安全资料有限、国内法规标准尚不完善、组织机构不健全且专业人员匮乏、分等级保护原则未严格实施等。

为进一步加强核电厂网络安全建设，应将网络安全纳入核电安全管理体系，同时必须开展相应的先进监管技术研究。根据中国核能行业协会核电厂同行评估及经验交流委员会发布的《关于2016—2017年核电厂同行评估及经验交流软课题研究项目立项的通知》（核协评估〔2016〕30号），“核电厂DCS系统信息安全研究与标准研制”软课题研究项目于2016年11月正式通过审核并立项。环境保护部核与辐射安全中心作为合作单位之一负责核电厂DCS信息安全现状的调研和法规标准分析等工作。本书是课题“核电厂DCS系统信息安全研究与标准研制”的研究成果之一。

环境保护部核与辐射安全中心审评人员在综合调研国内多个机组的网络安全现状、结合国内外的相关法规标准和审评经验后编写了本书，以供读者在核安全从业过程中参考使用。

全书由刘景宾、杨安义主编。

其中第1章由卞玉芳编写；第2章、第5章由杨安义编写；第3章由周林编写；第4章由乔宁编写；第6章、第7章由刘景宾编写；第8章由张云波编写；第9章由曾瑞编写。

全书由王忠秋、王晓峰、初起宝校核。

在本书编写过程中，虽然经过反复斟酌和修改，但由于时间紧迫，难免存在不足之处，诚望广大读者提出宝贵意见，以便再版时修改完善。

作者

2018 年 8 月

目 录

第1章

概 述

随着计算机和网络通信技术的发展，特别是信息化与工业化深度融合，信息系统、网络系统成为了核电站重要的基础设施和战略资产，分布式控制系统（Distributed Control System，DCS）已经全面进入核电站的实际应用。核电站DCS系统采用计算机和网络技术及相关设备，实现了信息的集中和控制系统的智能化，有效提高了核电厂运行的效率、安全性和可靠性。与此同时，核电站DCS系统的广泛应用，也给核安全带来了新的威胁与挑战，网络安全威胁是其中之一。

近年来，世界各国石油石化、金属冶炼、核电等高风险行业的危险事故频发，互联网信息安全问题也不断被爆出。统计数据表明，目前工业系统是遭受攻击最多、最严重的系统，出于各种目的，一些黑客开始向工业领域渗透，把关键基础设施（如供水供电、核电、交通、炼油等）的工业控制系统作为攻击目标，关键领域的系统和网络每天遭受恶意试探式攻击达数万次，如此高频率的网络攻击，使得网络安全的局势尤为严峻。2010年6月，“震网”（Stuxnet）病毒造成伊朗铀浓缩设备严重损坏，同时也使其在建核电站推迟发电，对伊朗核工业造成大面积影响。英国、美国、德国、乌克兰、韩国等国电站或核电站也相继出现网络安全事件。

核电站作为国家重要基础设施，核电DCS系统的可用性和性能对核电站来说有着至关重要的经济利益。黑客、木马、病毒、蠕虫等对核电DCS系统的攻击会导致系统遭到破坏，信息和数据被非法访问、更改、泄露，系统控制的装置和设备失灵，甚至核设施和核电厂被强制关闭。信息系统的非正常停运和瘫痪，会严重影响整个生产的正常运行，甚至可能导致恶性安全事故，最终对人员、设备和环境造成严重后果。

本书首先调研了全球核电站网络安全现状，梳理了近年来全球核电站网络安全事件，总结归纳了国际原子能机构（IAEA）、美国核管理委员会（NRC）、国际电工委员会（IEC）和英国皇家国际事务研究所等近年来针对核电站 DCS 系统网络安全的行动、具体措施以及法规标准。其次通过多地实地调研，总结了我国核电厂 DCS 系统网络安全现状及威胁。最后针对加强我国核电厂网络安全工作提出了意见和建议。

第2章

工业控制网络特征介绍

工业控制计算机，是一种采用总线结构，对生产过程及其机电设备、工艺装备进行检测与控制的工具的总称。它具有重要的计算机属性和特征，如具有计算机 CPU、硬盘、内存、外设及接口，并有实时的操作系统、控制网络和协议、计算能力，友好的人机界面等。

计算机网络从广义上可划分为通用的IT信息系统网络和各类专用的工业控制系统网络（以下简称“工业控制系统”或“工控系统”，ICS）两大类。工业控制系统往往又被称为“系统中的系统”，一般由工业以太网和现场总线控制系统组成，包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）、过程控制系统（PCS）、可编程控制器（PLC）等。这些系统广泛应用于核设施、钢铁、有色、化工、石油、电力、天然气、交通、先进制造等国家关键基础设施。典型的 ICS 网络如图 2-1 所示，分别由控制器层、操作站层和数据采集层构成。核电厂的生产控制网络属于工业控制系统网络。

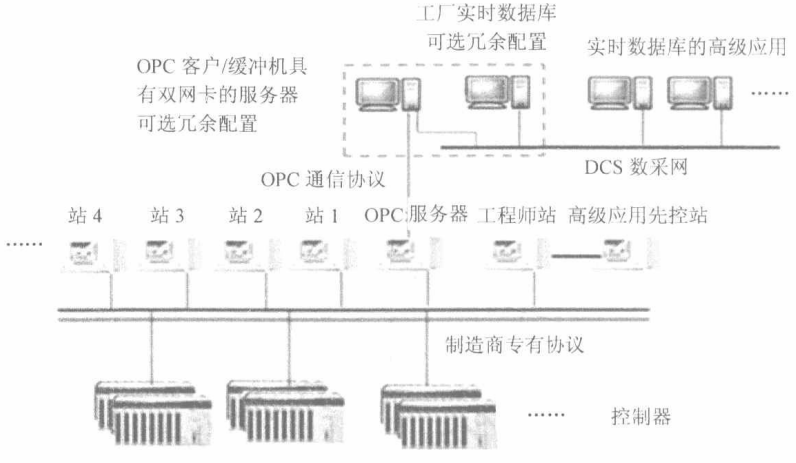

图 2-1　典型工业控制网络系统

目前所用的大部分 ICS 网络，其开发年代远远早于现今普遍使用的基于互联网的 IT 信息系统网络。设计之初，ICS 网络与其他网络是分离的，基于专用的硬件、软件和通信协议进行开发设计。数据传输量相对较少，重点考虑满足工业生产控制的可靠性、可维护性和可用性等需求。对网络安全的考虑相对简单，主要是对网络和控制平台在物理方面的限制，如设备有物理上独立的房间、控制人员进入和操作等。

随着工业化和信息化“两化融合”的发展，以及“工业 4.0”、“互联网+”、物联网等一系列新技术、新理念的推动，越来越多的工业控制网络系统和 IT 信息网络连接在一起，在推动技术进步、增加市场竞争力的同时，也使得工业控制网络系统自身的安全漏洞在网络互联的大时代背景下不断突显、放大，直接影响到工业生产的稳定与安全。

工业以太网和现场总线标准均为公开标准，工业控制网络核心使用的工控 PC 机，大多数同样基于 Windows-Intel 平台，工业以太网与民用以太网在技术上并无本质差异。熟悉工控系统的程序员开发针对性的恶意攻击代码并不存在很高的技术门槛，同时，传统工控网络主要凭借内网隔离来防范安全风险，缺乏综合防控措施。因此，工业控制网络系统安全面临的形势较为严峻。随着电力信息网和通信数据网两网融合的不断发展和深入，对工业控制网络的安全薄弱点进行安全防护考虑是十分必要的。