文献标识码：B 文章编号：1003-0492（2021）11-062-05 中图分类号：TN915.08

电厂网络安全应急处置研究

Research on Network Security Emergency Disposal of Power Plant

★谢增孝，张信情，冯丰业，朱继峰，徐昊（浙江浙能中煤舟山煤电有限责任公司，浙江 舟山 316100）
★孙科达（浙江省能源集团有限公司，浙江 杭州 310063）

摘要：当前，新的攻击手段和攻击方式不断出现，要求防护体系不断加强以应对新形势。电力系统是最早关注网络信息安全问题的行业，历经10余年电力工控系统安全防护建设，已经初步建成了安全分区、专网专用、横向隔离、纵向认证的电力监控系统安防体系。然而，电力监控系统信息安全危机应急处置的水平及能力还存在较大不足，具体体现在应急机制不完善、应急保障缺失、应急演练不到位、事故处置经验不足等方面。电力监控系统信息安全应急管理体系的标准化研究有助于在各个发电厂进一步推广应用，有助于应急处置经验的分享，有助于进一步提高电力工控领域的应急管理水平。

关键词：电力系统；工控系统；应急处置

Abstract: In the new period , new cyber attack methods continue to appear, which inevitably requires the protection system to constantly updated and strengthened. Electric power system is the first to follow network information security. After more than 10 years of security protection construction of power control system, a security system of power supervisory system with security zoning, private network, horizontal isolation and vertical certification has been preliminarily established. However, with the gradual improvement of the information security protection system of the power supervisory system, there are still great deficiencies in ability of the information security crisis emergency response of the power supervisory system, which are embodied in the imperfect emergency mechanism, the lack of emergency support, the lack of emergency drill, the lack of experience in accident disposal and so on. The research on the standardization of information security emergency management system of power supervisory system will help to further promote the application in various power plants, share the experience of emergency disposal, and further improve the level of emergency management in the field of electric industrial control system.

Key words: Power system; Industrial control system; Emergency response

1 引言

2016年11月，全国人大常委会表决通过了《中华人民共和国网络安全法》，其中第三章“网络运行安全”部分，首次明确定义了“关键信息基础设施”的概念，并将工控系统纳入其中；第五章“监测预警与应急处置”部分，对建立健全网络安全风险评估和应急工作机制、制定网络安全事件应急预案、定期组织应急演练等做出了相应规定，从立法高度明确了网络安全应急工作机制。

然而，在新时期下，新的攻击手段和攻击方式不断出现，也必然要求防护体系不断加强以应对新形势。发电厂电力监控系统较之其他行业的工控系统有较大区别，电力系统是最早关注网络信息安全问题的行业，并且历经10余年电力工控系统安全防护建设，已经初步建成了安全分区、专网专用、横向隔离、纵向认证的电力监控系统安防体系。然而，在电力监控系统信息安全防护体系逐步完善的同时，电力监控系统信息安全危机应急处置的水平及能力还存在较大不足，具体体现在应急机制不完善、应急保障缺失、应急演练不到位、事故处置经验不足等方面。

为建立健全电厂网络安全事件应急工作机制，提高应对网络安全事件的处置能力，最大限度地预防和减少网络安全事件及其造成的损失和危害，保护公众利益，保障信息和财产安全，保障信息系统及业务安全稳定运行，对电厂网络及相关系统可能发生的安全事件类型、常规网络安全事件的处置方法与对电力行

业工业控制系统的行业特点进行总结研究，分析其成因并寻求有效的应急处置方法，发现可以从以下几个方面入手。

2 确认电厂网络安全应急处置资源

电厂网络的安全应急处置工作，可不必受限于本单位资源，扩展思路与方法。保障人民群众的生命财产安全与生产，是首要要务。

2.1 可用人力资源

在应对网络安全事件时，可利用的人力资源应急力量如下：

（1）上级单位本部及合作高校企业（含竞争性企业）从事网络通信、信息安全、信息运行、业务系统应用的专家和技术人员。

（2）兄弟单位及其他相关单位的信息安全、业务系统专家。

（3）网络安全应急机构、网络安全服务商的信息安全技术人员，包括与本单位业务来往的网络与信息系统供应商、集成商及技术服务人员。

2.2 可用物资和装备资源

网络安全应急物资和装备资源主要包括：

（1）备品备件、计算机设备、网络设备、网络安全设备与软件、通信装备、交通工具、维修工具，以及事件处置案例、解决方案等。

（2）相关厂商可以协调提供的网络安全应急物资和装备。

3 明确电厂网络安全应急处置程序

（1）电厂网络与信息安全管理工作应坚持“积极防御、综合防范”的方针，遵循“统一领导、分级负责、统筹规划、突出重点、强化管理、注重技术”和“谁主管、谁负责，谁运营、谁负责”的原则。在网络与信息安全领导小组统一领导下，建立健全电厂网络安全事件应急处置工作责任制，明确责任，并将责任落实到人。同时，加强与各部门间的协调与配合，形成合力，共同履行应急处置工作。

（2）区分系统、明确边界。电厂工控系统是一体化的整体系统，往往“牵一发而动全身”，通常一处的异常将带动其他区域系统的联动异常。在此前提下，需要对事发系统与其余系统的关联性进行整理与划分，明确事件处置边界。

（3）精细处置，按步执行。在发生安全事件时，对其事发系统及相关网络、硬件应实行精细化操作。在事发之前，就应该明确其可能发生的安全事件类型，列举其存在的问题及事件表现形式。同时给出具体的应急处置流程与精细化的操作方法与步骤。

（4）科学落实，常练常知。建立科学的应急处置流程预案，实现电厂网络安全应急处置的程序化。同时定期开展应急处置演练活动，将应急处置流程深入进每一个相关人员意识当中。尤其抓住停机检修机遇，在条件允许情况下进行实践演练。在实际发生安全事件时，保障应急处置工作能够得到有序开展。

4 通过信息化手段贯通处置环节

由于电厂中的设备操作通常遵循着严格的操作管理制度，每位操作员都存在着固定的操作规程。发生网络安全事件后，为提高应急处置操作的及时性与有效性，避免二次事故，本文提出一种电厂应急处置指挥系统。在电厂网络安全应急处置总体原则的指导下，通过建立电厂应急处置指挥系统可以有效实现电厂应急处置相关人、财、物等资源的统一管理与调度，以信息化流程的方式规范应急处置操作人员的操作内容。系统内以应急处置流程进行串联各方角色，并预置电厂中可能出现的安全事件应急处置预案，通过流程在线流转的方式指导应急处置的实际操作，以保障在事件发生的第一时间采取正确恰当的处置措施及时止损，将事件造成的不良影响降到最低。

电厂应急处置指挥系统是电厂应急处置体系的重要组成部分。从业务上形成处置任务的下发及处置过程的监督、处置结果数据汇总的功能。该系统部署于管理信息大区，在应急处置过程中起到协调应急处置流程确

认、资源协调、应急处置数据汇总等功能。

安全事件应急处置工作以电厂应急处置指挥系统中的应急处置工单的形式进行流程流转、进度跟进。应急处置管理人员可在电厂应急处置指挥系统终端对安全风险、安全事件信息进行筛选、标记，形成处置工单，通过平台系统将工单下发至对应的应急处置人员，并在应急处置实施过程中对该工单应急处置的实施进度实时进行跟踪。应急处置单位在接到工单后，安排人员实施应急处置并反馈应急处置过程、汇总结果数据到系统。电厂应急处置指挥系统业务流程如图1所示。

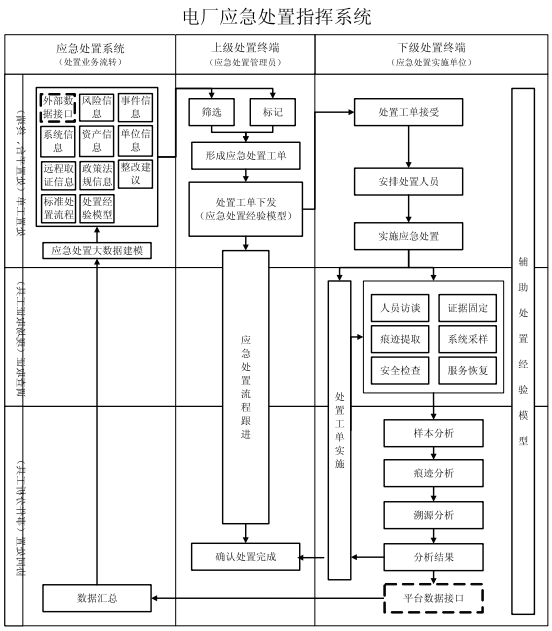

图1 电厂应急处置指挥系统业务流程设计图

· 应急处置系统：为应急处置业务开展承载系统，其功能包括处理应急处置流程流转、数据建模、信息管理等。

· 上级处置终端：为应急处置上级终端设备，包括终端电脑以及平板电脑实现与平台数据联动下发处置流程并跟踪。

· 下级处置终端：为应急处置下级终端设备，包括终端电脑以及平板电脑实现对收到的应急处置任务安排人员进行应急处置实施，并同步事件信息至对应现场处置工具。

· 现场取证工具：现场处置工具之一，为应急处置实施单位现场调查取证用工具，具有收集信息包括人员访谈、证据固定、痕迹提取、系统采样、安全检查等功能。

· 事件分析工具：现场处置工具之一，为对现场取证工具提取到的信息进行整理分析的专用工具，功能包括样本分析、痕迹分析、溯源分析。并将分析结果反馈处置终端与处置平台。

应急处置指挥系统成为服务不同科室、不同部门、上下级单位间事件处置的协作平台。通过本系统的建设，网络安全事件的处置可以联动不同部门、上下级单位相互配合；通过配套线下应急处置工具的使用，可以将信息采集的数据通过平台同步到分析部门；分析的结果支持同步到报告查看、输出的部门。将网络安全事件应急处置流程中涉及的部门、单位、人员通过平台功能进行协同、联动，提高应急处置的效率与信息同步效率。

5 DCS系统异常处置预案举例

5.1 明确应急处置人员职责

应实行“因岗定人”的原则，预先建立应急处置小组，明确各岗位在电厂安全事件应急处置过程中的工作职责，如表1所示。

表1 各岗位应急处置人员职责

现场应急处理小组		职责
组长	维护部分管仪控主任	准确执行指挥部下达的行政命令； 组织准确分析在DCS控制系统信息安全事件过程中机组发生的故障，组织进行消除。
副组长	运行部	准确执行指挥部下达的行政命令； 与电网调度中心保持联系，通报生产和电网信息；根据故障情况制定并执行机组运行变更方案，保障机组正常运行； 收集、整理有关事故处理信息，向指挥部提出指挥方案和策略。
联络员	仪控主管	根据收集到的各种信息，对故障情况进行初步分析，与应急组成员制定初步处理方案。
组员	仪控点检	根据收集到的各种信息，对故障情况进行初步分析，与应急组成员制定初步处理方案。
	信息工控网络安全专职	根据收集到的各种信息，对故障情况进行病毒感染和恶意代码攻击影响程度评估，确定病毒查杀和安全防护加固方案。
	仪控班班长	根据收集到的各种信息，对故障情况进行初步分析，与应急组成员制定初步处理方案。
	运行部	准确执行当值值长下达的操作命令； 负责紧急情况下的设备检查巡检及操作。

5.2 明确现场应急处置程序

在DCS系统故障发生时应能够快速地组织、协调应急救援力量开展故障处理工作。

（1）当DCS系统网络发生故障时，值长立即报省调、公司领导，运行人员及时通知相关专业技术人员到现场检查、处理，同时加强现场设备巡检工作。

（2）DCS系统发生网络瘫痪时，应在保证机组设备安全的前提下，要求运行人员维持机组负荷稳定，减少操作。提示运行人员通过后备手段监视各参数，并按《舟山煤电运行规程》做好事故停机预想。

（3）当发生病毒感染或黑客攻击导致系统网络故障造成DCS系统瘫痪后，先切断系统与外界的联系，防止继续受到黑客的攻击和病毒感染。同时切断与公用系统的网络连接，防止事故扩大到其他机组。

（4）如果是单台操作员站瘫痪，则先停止单台操作员站运行并断开其光纤和以太网的连接。如果所有操作员站瘫痪，运行人员无法从操作员站上监视机组参数和下发操作指令，只能通过其他可视仪表及光字报警系统来判断机组的运行状态。

（5）所有检查工作必须开具工作票，期间涉及信号强制操作必须走申请、审批流程。

5.3 明确应急处置操作步骤

DCS系统是电厂生产工控系统的核心系统。DCS系统发生安全事件将直接影响企业生产。本节以DPU控制器组态逻辑破坏举例，明确应急处置操作步骤的方法与意义。

DCS系统DPU控制器组态逻辑破坏运行岗位处置卡如表2所示。

表2 DPU控制器组态逻辑破坏运行岗位处置卡

类型	操作内容
故障现象	运行检查显示： （1）“模件故障”光字牌报警； （2）该控制器所辖所有信号测点均呈紫色且数据不刷新； （3）该控制器控制的设备均呈紫色，无法操作； （4）DPU所属的控制系统失控，现场控制设备状态全部回到初始值。
联系维护	联系仪控值班人员处理。
运行处理	（1）所属控制设备切就地运行； （2）若条件允许，隔离故障系统，并采取短期的就地手操控制； （3）减少重大操作，维持机组稳定运行； （4）做好事故停机预想； （5）在故障处理过程中，如发生主要参数变化大，危及机组安全，则应立即停机。

DCS系统DPU控制器组态逻辑破坏维护岗位处置卡如表3所示。

表3 DPU控制器组态逻辑破坏维护岗位处置卡

类型	操作内容
故障现象	（1）接到运行告知检查显示： ·“模件故障”光字牌报警； ·该控制器所辖所有信号测点均呈紫色且数据不刷新； ·该控制器控制的设备均呈紫色，无法操作。 （2）仪控检查：DPU控制机柜内控制器状态灯异常。
故障原因	（1）PCU的两路电源同时失电或故障； （2）控制器感染病毒，逻辑遭到破坏； （3）通讯故障； （4）控制器模件本身硬件故障； （5）运行模件故障后切换至冗余模件不成功。
故障后果	所属各测量和设备反馈信号无法监视，所控制的设备无法操作。
联系运行	如在短时间内无法恢复网络，又无备用仪表可以监视时，联系运行，按打闸机组处理。
处理办法	（1）检查并记录模件故障情况与故障代码，根据相关代码查阅模件使用手册，有针对性地进行消缺处理； （2）通常情况下，可以先对模件进行插拔上电复位，尽快恢复系统运行。如果复位不成功，则进行模件初始化，重新下装组态； （3）将工程师站主机恢复为最近的一次备份状态。恢复后打开相应DPU的逻辑程序，准备对故障DPU进行逻辑程序重装； （4）将故障的一对DPU的控制器的备用电池拔下，将光纤插头与主控DPU连接插头拔下，将该控制器从槽位中拔出。等待十分钟，放电消除记忆程序后插回，恢复所有连接插头； （5）对该DPU执行全面的程序下装工作，具体方法见DCS逻辑下载方法进行； （6）程序下装结束后，观察并确认控制器状态是否正常。在工程师站打开逻辑图并进入在线状态，检查逻辑组态和模块参数是否正确； （7）一对DPU全部恢复正常后，进行主备冗余切换试验并确认状态正常； （8）其他故障DPU可按照以上步骤进行恢复； （9）发现模件硬件已损坏时，则更换模件，重新下装组态； （10）如果发现模件已失电，则应检查电源情况，如有损坏，进行更换。

6 结语

最大限度地预防和减少信息安全事件及其造成的损失和危害，保护公众利益，保障公司信息和财产安全，保障公司信息系统及业务安全稳定运行，是电厂网络安全应急处置工作的最终目的。为确保电力监控系统在运行过程中发生网络与信息安全事件时，运行和维护人员能够迅速、准确地组织故障处理，最大限度地降低故障

造成的影响，需要建立健全信息安全应急工作机制，提高应对信息安全事件的处置能力。在制定相应的工作方法时，只有明确流程、分工、职责，将应急处置步骤落实到岗位，才具备操作与指导意义。信息化手段的建设可以有效打通各向关节，连通信息孤岛，实现电力监控系统网络安全事件应急处置的有序、有效开展。AP

作者简介：

谢增孝（1971-），男，浙江天台人，高级工程师，学士，现就职于浙江浙能中煤舟山煤电有限责任公司，主要从事火力发电厂设备管理工作。

张信情（1973-），女，浙江宁波人，工程师，现就职于浙江浙能中煤舟山煤电有限责任公司，研究方向是信息管理及网络安全。

冯丰业（1995-），男，浙江宁波人，助理工程师，学士，现就职于浙江浙能中煤舟山煤电有限责任公司，研究方向是网络安全。

朱继峰（1976-），男，浙江宁波人，高级工程师，硕士，现就职于浙江浙能中煤舟山煤电有限责任公司，研究方向是自动化。

徐　昊（1975-），男，浙江宁波人，工程师，学士，浙江浙能中煤舟山煤电有限责任公司，研究方向是能源工程及安全生产管理。

孙科达（1980-），男，浙江宁波人，高级工程师，硕士，现就职于浙江省能源集团有限公司，研究方向是智能电厂建设及网络安全。

参考文献：

[1] 国家能源局．电力监控系统安全防护专项监管报告发布[R]．http://www.nea.gov.cn/2017-05/03/c_136253418.htm.

[2] 陈瑾. JN供电公司应急供电服务能力评估体系构建研究[D]. 济南: 山东财经大学, 2019.

[3] 吴善庆, 石成忠, 李艳, 等. 风电场电力监控系统网络安全管理与技术研究[J]. 电力系统装备, 2021, (9). 143 - 145.

[4] 冯杰, 张鉴燮, 于振, 等. 基于任务特征的电网企业应急预案体系重构[J]. 中国安全生产科学技术, 2020, (10). 146 - 151.