ICS 35.240.50
CCS L 62

T

团　　体　　标　　准

T/CPUMT 007—2022

工业控制系统信息安全事件应急演练基本要求

Basic requirements for incident emergency exercises of industrial control system information security

2022-11-08 发布　　2022-11-08 实施

中国和平利用军工技术协会　发布
中　国　标　准　出　版　社　出版

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国和平利用军工技术协会提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、中能融合智慧科技有限公司、飞诺门阵（北京）科技有限公司、中国移动通信集团福建有限公司泉州分公司、浙江木链物联网科技有限公司、北京天融信网络安全技术有限公司、成都安美勤信息技术股份有限公司、浙江中控技术股份有限公司、联通数字科技有限公司、新华三技术有限公司、奇安信科技集团股份有限公司、博智安全科技股份有限公司、北京安盟信息技术股份有限公司、浪潮工业互联网股份有限公司、深圳华龙讯达信息技术股份有限公司、北京国泰网信科技有限公司、北京卫达信息技术有限公司、杭州中电安科现代科技有限公司、盛视科技股份有限公司、河南金盾信安检测评估中心有限公司、北京金钻芯科技公司、宁波和利时信息安全研究院有限公司、成都久信信息技术股份有限公司、北京神州慧安科技有限公司、北京控制与电子技术研究所、河北兰科网络工程集团有限公司、上海工业自动化仪表研究院有限公司、上汽通用五菱汽车股份有限公司、北京北武安信科技有限公司、北京声智科技有限公司、空间视创（重庆）科技股份有限公司、深圳融安网络科技有限公司、上海市网络技术综合应用研究所、参数技术（上海）软件有限公司、苏州国芯科技股份有限公司、中国兵器装备集团有限公司、中国电子信息产业集团有限公司第六研究所、中国电子科技集团公司第十五研究所、公安部第一研究所、公安部第三研究所、中国工业互联网研究院、北京通明湖信息技术应用创新中心、国家信息技术安全研究中心、北京中科北斗技术研究院、中国航空综合技术研究所、浙江海瑞网络科技有限公司、北京邮电大学、上海大学、首钢京唐钢铁联合有限责任公司、北京关键科技股份有限公司、河南天祺信息安全技术有限公司、浙江安远检测技术有限公司、深圳市网安计算机安全检测技术有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：黄海波、周开宇、沈寓实、施正炼、雷濛、寇增杰、阎育斌、余梦达、张婧宇、付志强、王弢、傅涛、张大伟、肖雪、胡丽华、李欣、郭成军、张俊峰、苗应亮、吴海禄、邱亮、黄晓波、李小川、付江、李晓龙、王汝成、王英、唐国强、宋博浩、陈孝良、王晶、陈桂耀、张延国、郎燕、王廷平、安维嵘、王绍杰、刘健、李秋香、邹春明、张玉良、曹军威、方进社、刘卜源、潘焕友、陈晗、崔宝江、袁建军、周华中、张怀珠、于帅玺、胡剑杰、彭泉、云淑林、丰存旭、贾璐璐、李佳、张亚杰、唐宇、杨亚萍、余觉非、曹锋、张德保、段小莉、马建红、乔华阳。

引　言

工业信息安全泛指工业运行过程中的信息安全，涉及工业领域各个环节，包括工业控制系统信息安全、工业互联网安全、工业数据安全、工业云安全、工业物联网安全、工业电子商务信息安全等内容。工业控制系统信息安全事件应急为工业信息安全应急工作的关键一环，也越来越受到国家相关主管部门、地方政府、工业企业的关注。

与其他应急处置工作一样，有效的工业控制系统信息安全应急处置工作对于在工业企业遭受网络安全事件后，减少人员伤亡、挽回经济损失、降低负面社会影响具有关键性作用。在国家、地方相关政策法规、培训宣贯等的推动下，地方行业主管部门、工业企业的应急管理意识不断增强，也出现了很多形式的应急演练，但在演练形式、演练内容上差距较大，演练质量参差不齐，很多演练服务流于形式，演练脚本不符合相关国家应急预案要求，环节设计与实际的处置差距较大等问题，未形成一套规范标准。因此，制定应急演练标准，进一步完善工业信息安全应急标准体系，常态化有效的开展应急演练，做到以演代练、平战结合，对于在工业控制安全事件真正发生时迅速组织协调各方资源、控制并处理事件具有重要作用。

GB/T 38645—2020 主要针对网络安全事件应急演练提出了框架性指南，本文件规定典型行业工业控制系统安全事件应急演练基本要求，旨在为军工、制造、石油化工、钢铁、有色、电力、水务等典型行业的工业控制系统信息安全应急演练提供指导。

工业控制系统信息安全事件应急演练
基本要求

1 范围

本文件规定了军工、制造、石油化工、钢铁、有色、电力、水务等典型行业的工业控制系统信息安全应急演练的目的、原则、形式、规划、准备、实施过程、评估总结和改进的要求。

本文件适用于针对典型行业工业控制系统信息安全事件开展的应急演练活动。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业控制系统 industrial control system;ICS

在工业部门和关键基础设施中应用于各种工业生产的控制系统。

注：工业控制系统包括监控和数据采集系统(SCADA)、集散控制系统(DCS)和其他较小的控制系统，例如可编程序控制器(PLC)。

[来源：GB/T 25069—2022，3.205]

3.2

信息安全事件 information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[来源：GB/T 25069—2022，3.684]

4 应急演练目的

应急演练目的包括下列内容。

a) 检验预案：发现应急预案中存在的问题，完善应急预案内容，提高应急预案的科学性、实用性和可操作性。

b) 完善准备：检查应对工业控制系统信息安全事件所需应急队伍、物资、装备、技术等方面的准备情况，发现不足并及时予以调整补充。

c) 磨合机制：明确行业管理部门、相关单位和人员的职责任务，理顺工作流程，完善各关联方之间的应急联动机制，提升协调配合能力。

d) 锻炼队伍：增强应急演练管理部门、指挥机构、参演机构和人员等对应急预案的熟悉程度，锻炼应急处置需要的技能，加强配合，提高其应急处置能力。

e) 宣传教育：普及应急知识，不断增强信息安全管理的专业化程度，提高全员工业控制系统信息安全风险防范意识。