ICS 35.240.50
CCS L62

团 体 标 准

T/CPUMT 001—2022

工业信息安全应急处置工具箱

Emergency disposal toolbox for industrial information security

2022-04-21 发布　　2022-04-21 实施

中国和平利用军工技术协会　　发 布

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、贵阳宏图科技有限公司、北京安天网络安全技术有限公司、浙江安腾信息技术有限公司、杭州立思辰安科科技有限公司、北京安盟信息技术股份有限公司、北京珞安科技有限责任公司、北京神州绿盟科技有限公司、华控清交信息科技（北京）有限公司、博智安全科技股份有限公司、北京恒安嘉新安全技术有限公司、安徽长泰科技有限公司、长扬科技（北京）有限公司、北京天融信网络安全技术有限公司、福建中信网安信息科技有限公司、武汉安域信息安全技术有限公司、北京天地和兴科技有限公司、上海工业控制安全创新科技有限公司、西安猎鹰科技有限公司、成都安美勤信息技术股份有限公司、北京万里红科技有限公司、兴唐通信科技有限公司、中能融合智慧科技有限公司、上海伊世智能科技有限公司、北京奇虎科技有限公司、浙江鹏信信息科技股份有限公司、杭州安恒信息技术股份有限公司、广域铭岛数字科技有限公司、北京中超伟业信息安全技术股份有限公司、北京易华录信息技术股份有限公司、工业信息安全（四川）创新中心有限公司、北京声智科技有限公司、中国电子工程设计院有限公司、中国工业互联网研究院、北京北方车辆集团有限公司、哈尔滨工程大学、北京航空航天大学、北京工业大学（信息学部）、江西昌河航空工业有限公司、江西洪都航空工业集团有限责任公司、山东华软金盾软件股份有限公司、青岛宏大纺织机械有限责任公司、北京金山猎豹科技有限公司、三一集团有限公司、中国寰球工程有限公司北京分公司、天津北玻玻璃工业技术有限公司、中移系统集成有限公司、重庆工业大数据创新中心有限公司、广视三信（台州）信息技术有限公司、中海油田服务股份有限公司、山西恒跃锻造有限公司、山东电子学会、亿博智造（北京）科技有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：张晓帆、范灵俊、王盈、杨佳宁、汪礼俊、郝志强、周黎辉、徐翰隆、杨治崇、张俊峰、张大伟、程顺、张兵、郭文科、王晓鹏、梁磐、王云河、傅涛、郑轶、李蓉、王泽政、廉明、冯彬、赵华、汪义舟、安高峰、金华松、李永龙、王鹏、李佐民、蒲戈光、张龙飞、李劲雄、胡特彧、赵闪、胡鹏辉、沙学松、倪华、冀磊、邱辉、于海跃、黄丁智、魏娟、杨宇波、安宇、陈孝良、段萌、叶丽丽、朱浩、李辉、申林山、关振宇、张津丽、杨军华、胡青、段文凯、张殊、林鹏、周祥、江沛、李春超、焦罡、祝守守、张益斌、潘鹏、郑勇、胡聪聪、高国清、付洋、段小莉、张德保、马建红、乔华阳。

本文件为首次发布。

引　言

工业是国民经济的基础，工业信息安全事关经济发展、社会稳定和国家安全。近年来，随着互联网等新一代信息技术与工业生产活动融合的不断深入，工业信息安全面临日益严峻的安全威胁。应急响应作为工业信息安全工作中不容失守的最后一道防线，对于处置漏洞隐患、消减事件损失、保障工业生产等都具有重要意义。

工业信息安全应急处置工具箱适用于工业企业现场发生工业信息安全事件或风险的快速应急处置，作为一种工业级、一体化、专用型的安全产品，凭借丰富的处置功能、高效的分析能力和便捷的可操作性，已成为工业企业、安全企业开展现场应急处置的有效工具。制定本文件，可以为规范工业信息安全应急处置工具箱的技术指标、指导相关产品研发使用、拓宽产品应用渠道与领域，提高我国工业企业信息安全应急保障能力等工作提供支撑。

工业信息安全应急处置工具箱

1 范围

本文件规定了工业信息安全应急处置工具箱（简称“工具箱”）的组成与型号、技术要求、试验方法，检验规则及标牌、包装、运输和贮存等。

本文件适用于工业信息安全应急处置工具箱的设计、研发、生产、检验检测和验收，可应用于军工、市政、冶金、电力、医药、化工、石油石化、交通运输和机械装备制造等各类工业行业的信息安全应急处置。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 191 包装储运图示标志
GB/T 4208 外壳防护等级（IP代码）
GB/T 9969 工业产品使用说明书 总则
GB/T 13306 标牌
GB 16796 安全防范报警设备 安全要求和试验方法
GB/T 20275 信息安全技术 网络入侵检测系统技术要求和测试评价方法
GB/T 20280 信息安全技术 网络脆弱性扫描产品测试评价方法
GB/T 20945 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
GB/T 24363 信息安全技术 信息安全应急响应计划规范
GB/T 26268 网络入侵检测系统测试方法
GB/T 28451 信息安全技术 网络型入侵防御产品技术要求和测试评价方法
GB/T 29766 信息安全技术 网站数据恢复产品技术要求与测试评价方法
GB/T 34990 信息安全技术 信息系统安全管理平台技术要求和测试评价方法
GB/T 37079 设备可靠性 可靠性评估方法
GB/T 37954 信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法
GB/T 39786 信息安全技术 信息系统密码应用基本要求
GA/T 911 信息安全技术 日志分析产品安全技术要求
GA/T 1536 信息安全技术 计算机主机安全检测产品测评准则
QB/T 4399 手提式工具箱
QB/T 5536 工具箱柜通用技术条件

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业信息安全应急处置工具箱 emergency disposal toolbox for industrial information security

集成工业信息安全应急处置全流程所需的软硬件工具，对接国家级工控安全远程应急支援服务平台（3.3）的一体化、工业级的专用型安全产品。

3.2

现场应急处置技术平台 on-site emergency technology platform

将集成应急处置所需的各类软件工具和关键数据资源内置于工具箱应急处置终端中的流程化技术平台。

3.3

工控安全远程应急支援服务平台 remote service platform of emergency support for ICS security

集成工业信息安全远程应急支援所需的威胁情报、分析引擎、数据资源、安全专家等功能资源，为工具箱提供远程技术支撑，为现场应急人员提供远程支援的服务平台。

3.4

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 20985.1—2017，3.4]

3.5

工业控制系统 industrial control system

多种工业生产中使用的控制系统。

注：包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等，现已广泛应用在工业部门和关键基础设施中。

[来源：GB/T 37962—2019，3.1]

3.6

应急处置 emergency disposal

对突发险情、事故、事件等采取紧急应对的措施或行动。

3.7

工业协议指纹 industrial protocol fingerprint

用来远程识别工业控制系统（3.5）的设备硬件、操作系统、运行软件和网络协议类型等信息的特征参数。

4 组成与型号

4.1 组成

工具箱由箱体、应急处置终端、辅助工具三部分组成。每部分具体组成如下：

a) 箱体为容纳应急处置终端和辅助工具的外壳；

b) 应急处置终端为移动式计算机，包括现场应急处置技术平台和各类通讯接口，提供应急处置全流程功能模块及关键数据资源；

c) 辅助工具由安全 U 盘（内置各类应急处置软件工具）、加密硬盘、移动电源、网线、串口线、上网卡、加密光盘及刻录设备和微型扫描仪等软硬件工具组成，提供数据取证、备份恢复、入侵排查、日志分析和应急通讯等功能。

4.2 型号

工具箱型号采用字母数字表示。它们分别由工具箱代号、分类代号、分级代号、厂商代码以及系列号五部分组成。

a) 工具箱代号指的是工具箱名称，按照QB/T 4399中的规定，采用“TBS”表示。

注1：参见QB/T 4399的相关规定，本文件规定的工具箱的型式为简易型（H型）。

b) 分类代号指的是工具箱适用的行业类别，采用行业中文名称的两位大写首字母表示。行业类别可参考GB/T 4754中的相关规定。

c) 分级代号指的是工具箱的应急处置能力级别，采用各级别的英文名称表示。根据工具箱面向不同规模和级别的应急处置对象时的配置水平，工具箱级别可分为轻量级（Light）、标准级（Standard）和增强级（Enhanced）：

1) 轻量级工具箱可支持单一网域的产线级工业信息安全应急处置任务；

2) 标准级工具箱可支持多网域的集团级工业信息安全应急处置任务；

3) 增强级工具箱可支持涉及多企业的供应链级工业信息安全应急处置任务。

注2：关于工具箱面向不同规模和级别的应急处置对象时的配置水平要求将在后续系列标准中进行规定。

d) 厂商代码指的是工具箱生产厂商的名称，采用厂商中文名称的四位大写首字母表示。

e) 系列号指的是由生产厂商自定义的代码，由一个或多个数字或英文字母表示。

工具箱型号编码规则见图1所示。

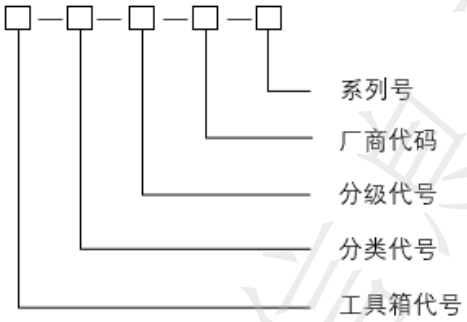

图1 工具箱型号编码规则

示例1：

适用于军工的增强级工具箱型号为：TBS-JG-Enhanced-ABCD-001

示例2：

适用于电力的轻量级工具箱型号为：TBS-DL-Light-EFGH-28

5 技术要求

5.1 基本要求

5.1.1 箱体应采用抗干扰能力强、防震防抖材料，如 ABS 工程塑料或不低于同等性能的其他材料。

5.1.2 箱体表面应无磕碰伤痕、变形等缺陷；表面涂层完整，无脱漆、起泡、裂纹等现象；内外表面应平整光滑，无凹凸毛刺等现象。

5.1.3 箱体各紧固件应牢固不松动，各装配部件应设计合理，便于安装和维修拆卸。

5.1.4 箱体焊缝应均匀牢固，无气孔、夹渣、烧穿等缺陷。

5.1.5 箱体外壳防护等级(IP)应不小于 IP54，符合露天、装置区和生产厂房等运输或储藏环境的要求。

5.1.6 应急处置终端和辅助工具应具备支持以太网口（千兆以上）、光纤接口、USB2.0，以及 RS232、RS422 和 RS485 串行接口等常见通讯接口，具备带刻录功能的高密度数字视频光盘（DVD）光驱等。

5.2 功能

5.2.1 处置功能

应急处置终端中的现场应急处置技术平台及辅助工具应采用“准备、检测、抑制、根除、恢复、跟踪”应急响应模型，集成全流程功能模块及关键数据资源，具备工业信息安全应急处置各阶段所需的功能模块。各个功能模块包含内容如下：

a) 准备阶段：包含应急资源库更新升级等；

b) 检测阶段：包含漏洞检测、工业协议解析等；

c) 抑制阶段：包含镜像备份、证据固定等；

d) 根除阶段：包含流量分析、日志分析、进程分析、恶意代码检测、病毒查杀和融合分析等；

e) 恢复阶段：包含数据恢复、预置应急处置模板等；

f) 跟踪阶段：包含预置应急处置技术分析报告模板等。

注：参考NIST SP800-61，应急响应模型（Prepare-Detection-Containment-Eradication-Recovery-Follow-Up，

PDCERF）将应急响应流程分成准备、检测、抑制、根除、恢复、跟踪阶段。根据应急响应总体策略为每个阶段定义适当的目的，明确响应顺序和过程。

5.2.2 适配功能

应急处置终端应支持主流工业主机、工业软件、工业控制器、物联网设备、工业网络设备、安全设备和工业互联网平台等软硬件系统的识别检测和应急处置功能。

5.2.3 应急资源储备

现场应急处置技术平台应具备应急资源库，并支持在线、离线更新功能。应急资源库包括但不限于：

a) 工业信息安全漏洞库；
b) 协议指纹库；
c) 恶意代码库；
d) 应急处置模板库；
e) 知识库。

5.2.4 分析功能

现场应急处置技术平台应具备数据融合分析能力，支持对处置过程中采集数据的关联分析和统计对比功能，预置多种应急处置技术分析报告模板。

5.2.5 后端平台对接

现场应急处置技术平台应具备与国家级工控安全远程应急支援服务平台的对接功能，协同平台的专家资源、威胁情报和分析引擎等，提供现场处置与远程支援相结合的一体化技术支撑。

5.2.6 特殊功能要求

对于爆炸危险环境、高温高压、电磁辐射等特殊领域工业环境，应根据工具箱的不同类别和级别增加相应功能要求。

5.3 性能

5.3.1 可靠性与敏捷性

现场应急处置技术平台的正常启动可靠性应大于99.99%。现场应急处置技术平台的硬件启动时间应小于3 min。应急处置终端应满足24 h连续性工作，不发生故障。

5.3.2 续航与供电

应急处置终端在额定工况下，续航时间应不小于6 h；在借助辅助工具中移动电源的情况下，续航时间应不小于12 h。

5.3.3 应急资源库容量

现场应急处置技术平台内置的应急资源库，应预置工业协议指纹不少于50种，包含工业控制器、工业组态软件等多种工业资产漏洞不少于10^5个、工控漏洞不少于800个、恶意代码特征不少于2×10^6个；应内置工业勒索、挖矿等典型工业信息安全事件应急处置模板不少于5种等。

5.3.4 特殊性能要求

对于爆炸危险环境、高温高压、电磁辐射等特殊领域工业环境，应根据工具箱的不同类别和级别增加相应性能要求。

5.4 安全

5.4.1 网络安全

应急处置终端应支持身份鉴别、访问控制、日志审计、通信安全防护、漏洞检测和恶意程序防范等安全防护功能，以保障自身网络安全。

5.4.2 数据安全

应急处置终端应采用符合 GB/T 39786 要求的密码学技术，保障数据处理、传输和存储过程中的数据安全和敏感信息保护。

5.4.3 供应链安全

工具箱应确保软硬件的预装及更新安全，宜采用国产操作系统、软件组件或开源组件进行部署集成。

5.4.4 物理和电气安全

工具箱物理特性安全和电气安全应符合 GB/T 34990 中的相关规定，保护工具箱的物理特性在使用中不被损坏，电气性能不发生偏离，保障工具箱及相关组成设备的自身安全。

6 试验方法

6.1 试验条件

6.1.1 试验环境温度应不低于-20 ℃，不高于 60 ℃；对于应用于特殊工业环境的工具箱，其试验环境应符合该特殊工业环境的相关要求。

6.1.2 应搭建适用的试验台，试验台应通电、联网，具备试验空间。

6.2 试验工具

6.2.1 应采用主流品牌工业控制器、工业软件、工业主机和工业机器人等试验所需的硬件设备。

6.2.2 应采用主流工业协议、恶意代码样本、流量包和日志样本等试验所需的数据库及样本文件。

6.2.3 应采用安全性测试工具、可靠性测试工具等其他试验工具。

6.3 基本要求试验

6.3.1 工具箱箱体材料通过供货商提供的具有 CNAS 资质的第三方机构出具的报告进行检验。

6.3.2 箱体外观采用目视检验，焊缝质量等通过专业仪器进行检测，如探缝仪器。

6.3.3 箱体外壳防护等级按 GB/T 4208 的相关规定进行检验。

6.3.4 工具箱应急处置终端和辅助工具接口情况通过搭建适用的试验台进行检验，内容包括但不限于业务功能覆盖是否完整、业务规则覆盖是否完整、参数验证是否达到要求。

6.4 功能试验

6.4.1 现场应急处置技术平台及辅助工具的处置流程按 GB/T 24363 的相关规定进行检验。其中：

a) 镜像备份、证据固定、数据恢复功能按 GB/T 29766 的相关规定进行检验；
b) 漏洞检测功能按 GB/T 20280、GB/T 37954 的相关规定进行检验；
c) 工业协议解析、流量分析、恶意代码检测功能按 GB/T 20275、GB/T 26268、GB/T 28451 的相关规定进行检验；
d) 日志分析功能按 GB/T 20945、GA/T 911 的相关规定进行检验；
e) 进程分析、病毒查杀功能按 GA/T 1536 的相关规定进行检验；
f) 融合分析、预置应急处置模板、应急处置技术分析报告模板等功能按照人工核查的方式进行检验。

6.4.2 现场应急处置技术平台的后端平台对接功能通过搭建适用的试验台进行检测，检测内容包括但不限于：

a) 检测是否支持现场处置和远程支援两种工作模式，可与工控安全远程应急支援服务平台联动通讯；

b) 检测是否支持通过接口向平台上传现场待分析的文件、流量、日志和安全事件的样本数据，实现支援平台的联动处置；
c) 检测是否支持用户通过无线、移动互联网远程与专家或专业服务团队开展协同处置，具备应急处置报告输出、报告模板获取和配置等功能。

6.4.3 对于应用到爆炸危险环境、高温高压、电磁辐射等特殊领域工业环境中的工具箱，应按照相关行业的功能检验要求。

6.5 性能试验

6.5.1 应急处置终端的可靠性按 GB/T 37079 的相关规定进行检验。
6.5.2 应急处置终端的续航与供电通过人工试验的方式进行检测。
6.5.3 通过对相关数据库数量进行技术核查的方式，检验现场应急处置技术平台包含的工业协议指纹、安全漏洞、工控漏洞、恶意代码特征和工业信息安全事件应急处置模板的数量。
6.5.4 对于应用到爆炸危险环境、高温高压、电磁辐射等特殊领域工业环境的工具箱，应按照相关行业的性能检验要求。

6.6 安全试验

6.6.1 工具箱的网络安全、数据安全、供应链安全按 GB/T 34990 的相关规定进行检验。
6.6.2 物理和电气安全按 GB 16796 的相关规定进行检验。

7 检验规则

7.1 检验项目

工具箱检验项目分为出厂检验和型式检验。检验项目应符合表2的要求。

表2 检验项目

检验项目	序号	检验内容	出厂检验	型式检验	技术要求	试验方法
基本要求	1	箱体材料	--	Δ	5.1.1	6.3.1
	2	箱体表面及装配	Δ	Δ	5.1.2、5.1.3	6.3.2
	3	箱体焊缝	Δ	Δ	5.1.4	6.3.2
	4	箱体外壳	Δ	Δ	5.1.5	6.3.3
	5	应急处置终端和辅助工具接口	Δ	Δ	5.1.6	6.3.4
功能	1	处置功能、适配功能、应急资源储备、分析功能	--	Δ	5.2.1、5.2.2、5.2.3、5.2.4	6.4.1
	2	后端平台对接	--	Δ	5.2.5	6.4.2
	3	特殊功能要求	--	Δ	5.2.6	6.4.3
性能	1	可靠性与敏捷性	Δ	Δ	5.3.1	6.5.1
	2	续航与供电	Δ	Δ	5.3.2	6.5.2
	3	应急资源库容量	Δ	Δ	5.3.3	6.5.3
	4	特殊性能要求	Δ	Δ	5.3.4	6.5.4
安全	1	网络安全、数据安全、供应链安全	--	Δ	5.4.1、5.4.2、5.4.3	6.6.1
	2	物理和电气安全	Δ	Δ	5.4.4	6.6.2
注：“Δ”为必检验项目，“--”为非检验项目。						

7.2 出厂检验

7.2.1 工具箱出厂前，应逐台进行出厂检验，并保证所有零部件、配套件与整机质量符合要求，检验合格并填写合格证书后方可出厂。
7.2.2 出厂检验项目中若有一项不合格，即为不合格。

7.3 型式检验

7.3.1 工具箱有下列情况之一时，应进行型式检验：

a) 正式生产后，如结构、材料、工艺有较大改变，可能影响工具箱性能时；
b) 工具箱停产 1 年后，恢复生产时；
c) 出厂检验结果与上次型式检验结果有较大的差异时；
d) 工业信息安全产品相关质量监督机构提出要求或合同规定等。

7.3.2 型式检验的项目全部合格为型式检验合格，如有不合格项，应加倍抽样。对不合格项进行复检，复检仍不合格的则判定该工具箱继续型式检验不合格，其中安全性能不允许复检。

8 标牌、包装、运输和贮存

8.1 标牌

应在工具箱箱体和应急处置终端的明显位置处装设标牌。标牌应符合GB/T 13306的相关规定，其内容包括但不限于：

a) 制造单位名称和地址；
b) 工具箱名称、型号规格；
c) 工具箱商标；
d) 工具箱编号；
e) 出厂日期；
f) 工具箱净重量和运行重量；
g) 外型尺寸 L×W×H(mm)；
h) 电源、电压、功率。

8.2 包装

工具箱包装应满足以下要求：

a) 采用箱装，应符合 QB/T 5536 的相关要求；
b) 包装箱内应有下列文件，并封存在不透水的口袋内：
    1) 质量证明文件；
    2) 出厂合格证；
    3) 功能说明书；
    4) 使用说明书；
    5) 装箱单。
c) 说明书内容应符合 GB/T 9969 的相关规定。

8.3 运输

运输过程中应固定牢靠，避免撞击碰伤；装卸时应轻装轻卸，防止撞击，防止倒置，运输、包装以及收发货标志应遵守GB/T 191的相关规定。

8.4 贮存

工具箱宜放在室内干燥、通风良好且无腐蚀性介质环境中，避免阳光直射，如露天停放应有防雨、防晒及防潮等措施。

参 考 文 献

[1] GB/T 4754　国民经济行业分类
[2] GB/T 20985.1—2017　信息技术　安全技术　信息安全事件管理　第1部分：事件管理原理
[3] GB/T 37962—2019　信息安全技术　工业控制系统产品信息安全通用评估准则
[4] NIST SP800-61 Rev.2,Computer Security Incident Handling Guide,2012.08.06
[5] 中华人民共和国网络安全法
[6] 中华人民共和国数据安全法