工业互联网安全测评与应急职业技能等级标准

标准代码：510120

（2021年2.0版）

北京奇虎鸿腾科技有限公司　制定

2021 年 12 月　发布

目　次

前　言

本标准按照 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。

本标准起草单位：北京奇虎鸿腾科技有限公司、北京奇虎科技有限公司、三六零科技集团有限公司、北京奇付通科技有限公司、东北大学、北京华新智教教育技术有限公司、吉林省安来科技有限责任公司、安徽大富鸿学教育科技有限公司、西安电子科技大学、山东科技大学、北京信息职业技术学院、武汉职业技术学院。

本标准主要起草人：冯玉涛、张记卫、张彬哲、王志威、齐飞、杨莹、那东旭、冯文博、吕雯雯、周家豪、何远良。

1 范围

本标准规定了工业互联网安全测评与应急职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于工业互联网安全测评与应急职业技能培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

GB/Z 20985-2007 信息安全技术 信息安全事件管理指南

GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

GB/T 25069-2010 信息安全技术 术语

GB/T 30283-2013 信息安全技术 信息安全服务分类

3 术语和定义

GB/T 25069-2010 界定的以及下列术语和定义适用于本标准。

3.1

信息安全 information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗依赖性、可靠性等性质。

[GB/T 25069-2010，定义 2.1.52]

3.2

信息安全事件 information security incident

由单个或一系列意外或有害的信息安全事态所组成的，极有可能危害业务运行和威胁信息安全。

[GB/T 25069-2010，定义 2.1.53]

3.3

安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。

[GB/T 25069-2010，定义 2.2.1.6]

3.4

安全服务 security service

根据安全策略，为用户提供的某种安全功能及相关的保障。

[GB/T 25069-2010，定义 2.1.47]

3.5

安全分级 security classification

根据业务信息和系统服务的重要性和受损影响，确定实施某种程度的保护，并对该保护程度给以命名。依据访问数据或信息需求，而确定的特定保护程度，同时赋予相应的保护等级。例：“绝密”、“机密”、“秘密”。

[GB/T 25069-2010，定义 2.2.1.2]

3.6

安全审计 security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

[GB/T 25069-2010，定义 2.2.1.8]

3.7

入侵检测 intrusion detection

检测入侵的正式过程。该过程一般特征为采集如下知识：反常的使用模式，被利用的脆弱性及其类型、利用的方式，以及何时发生及如何发生。

[GB/T 25069-2010，定义 2.2.1.100]

3.8

风险评估 risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。

[GB/T 20984-2007，定义 3.7]

3.9

应急响应 emergency response

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

[GB/T 24363-2009，定义 3.4]

4 适用院校专业

4.1 参照原版专业目录

中等职业学校：工业自动化仪表及应用、网络信息安全、计算机网络技术、网站建设与管理、网络安防系统安装与维护、软件与信息服务、移动应用技术与服务。

高等职业学校：信息安全与管理、云计算技术与应用、计算机网络技术、大数据技术与应用、计算机应用技术、计算机信息管理、软件与信息服务、电气自动化技术、智能控制技术、工业网络技术、工业自动化仪表。

高等职业教育本科学校：电气工程及其自动化、智能控制技术、自动化技术与应用、计算机应用工程、网络工程、信息安全与管理、大数据技术与应用、通信工程。

应用型本科学校：信息安全、网络空间安全、网络工程、软件工程、数据科学与大数据技术、电气工程及其自动化。

4.2 参照新版职业教育专业目录

中等职业学校：工业自动化仪表及应用、网络信息安全、计算机网络技术、网站建设与管理、网络安防系统安装与维护、软件与信息服务、移动应用技术与服务。

高等职业学校：信息安全技术应用、云计算技术应用、计算机网络技术、大数据技术、计算机应用技术、软件技术、电气自动化技术、智能控制技术、工业互联网技术、工业自动化仪表技术。

高等职业教育本科学校：电气工程及自动化、智能控制技术、自动化技术与应用、计算机应用工程、网络工程技术、信息安全与管理、大数据工程技术、现代通信工程、工业互联网工程。

应用型本科学校：信息安全、网络空间安全、网络工程、软件工程、数据科学与大数据技术、电气工程及其自动化。

5 面向职业岗位（群）

【工业互联网安全测评与应急】（初级）：主要面向工业互联网领域的企事业单位、政府等的网络通信部门、信息安全部门或安服部门，在安全测评、网络运维、安全服务、产品研发及攻防对抗等岗位，从事网络安全信息收集、渗透测试、风险评估、安全事件恢复等工作。

【工业互联网安全测评与应急】（中级）：主要面向工业互联网领域的企事业单位、政府等的网络通信部门、信息安全部门或安服部门，在安全测评、网络运维、安全服务、产品研发、攻防对抗及应急管理等岗位，从事网络安全信息收集、安全实施、渗透测试、风险评估、安全事件分析及恢复等工作。

【工业互联网安全测评与应急】（高级）：主要面向工业互联网领域的企事业单位、政府等的网络通信部门、信息安全部门或安服部门，在安全测评、网络运维、安全服务、产品研发、攻防对抗、安全管理及应急管理等岗位，从事网络安全信息收集、安全实施、渗透测试、风险评估、安全事件分析及恢复、安全架构设计、安全组织管理等工作。

6 职业技能要求

6.1 职业技能等级划分

工业互联网安全测评与应急职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【工业互联网安全测评与应急】（初级）：熟知网络安全法律法规，掌握工业互联网安全测评与应急基础知识和技能，能够完成对系统主机、控制系统、网

络系统、通信协议等安全信息收集工作，并根据项目安全要求实现安全设备调试与配置，并掌握安全事件复现能力。

【工业互联网安全测评与应急】（中级）：熟知网络安全法律法规，掌握工业互联网安全测评与应急基础知识和技能，能够完成对系统主机、控制系统、网络系统、通信协议等测试评估工作，并根据项目需求编制并实施解决方案，并掌握安全事件分析能力。

【工业互联网安全测评与应急】（高级）：熟知网络安全法律法规，掌握工业互联网安全测评与应急知识和技能，能够完成对系统主机、控制系统、网络系统、网络协议、事件处置、安全取证等测试评估工作，并根据项目安全需求，进行安全架构设计并组织实施解决方案，并掌握组织和实施安全事件应急响应能力。

6.2 职业技能等级要求描述

表 1 工业互联网安全测评与应急职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.工业互联网云平台信息识别与收集	1.1 网络架构识别	1.1.1 能识别主流工业互联网平台网络组成。 1.1.2 能识别主流工业互联网网关设备。 1.1.3 能识别主流工业互联网安全设备。 1.1.4 能使用网络流量工具针对特定网络目标进行流量捕获。
	1.2 系统信息收集	1.2.1 能识别主流操作系统，并根据获取操作系统版本信息。 1.2.2 能使用操作系统工具，创建、修改、删除用户信息。 1.2.3 能使用操作系统工具，获取系统进程、服务、网络、日志等信息。

	1.3 网络服务信息收集	1.3.1 能识别不同网络服务的编程语言。 1.3.2 能使用网络服务工具，创建、修改环境配置。 1.3.3 能使用网络服务工具，获取基本的服务信息。
2.工业互联网控制设备信息识别与收集	2.1 工控设备识别	2.1.1 能识别工业控制系统中不同的设备。 2.1.2 能使用 PLC 相关工具，获取 PLC 基本信息。 2.1.3 能根据项目内容，区分不同行业的工业控制系统网络架构。
	2.2 工控网络信息查找	2.2.1 能使用局域网工具枚举局域网设备的 IP 地址。 2.2.2 能使用网络流量抓包工具，完成网络数据的捕获。 2.2.3 能识别网络流量中的基本信息，如 TCP、UDP 流量。
	2.3 工控协议分析	2.3.1 能配置边缘计算网关设备与云平台之间的通信。 2.3.2 能识别 Modbus TCP、MQTT、OPC 等工控通信协议。

3.工业互联网网络安全评估	3.1 网络安全评估准备	3.1.1 理解资产、威胁、保障能力以及脆弱性概念； 3.1.2 掌握风险评估准备阶段工作内容。 3.1.3 能够识别工业互联网系统规划设计方案； 3.1.4 能够识别网络拓扑图； 3.1.5 能够识别系统安全防护规划； 3.1.6 掌握无损扫描、有损扫描等常见网络资产分析技术。 3.1.7 掌握内网目标主机信息收集技术，如 ICMP、TCP、UDP 等技术方式。 3.1.8 能使用信息搜索工具（如：Shodan、ZoomEye 网络空间搜索引擎）进行基本的资产信息收集。 3.1.9 能使用信息搜索工具，对网络安全信息进行分组、分类。
	3.2 安全测试与验证	3.2.1 能使用常见的安全测试工具，进行基本的网络五元组信息收集。 3.2.2 能使用常见的安全测试工具，识别不同的设备类型。 3.2.3 能使用常见的安全测试工具，识别不同的通信协议。 3.2.4 能使用常见的安全测试工具，对设备进行已知漏洞验证。
	3.3 网络安全评估检查	3.3.1 能根据项目要求，确定网络安全评估范围。 3.3.2 能根据项目要求，分析服务器安全配置。 3.3.3 能根据项目要求，分析工控设备安全配置。 3.3.4 能根据项目要求，从网络流量中分析漏洞信息。 3.3.5 能根据项目要求，分析资产信息中的漏洞信息。

	3.4 网络安全评估报告编制	3.4.1 能根据报告编写要求，梳理安全测试信息。 3.4.2 能根据报告编写要求，梳理网络资产信息。 3.4.3 能根据报告编写要求，梳理网络威胁信息。
4.工业互联网网络安全应急处置	4.1 安全事件信息收集	4.1.1 能识别网络安全事件及相关信息。 4.1.2 能根据不同事件类型，对网络安全事件进行分类。
	4.2 安全事件分析	4.2.1 能根据业务影响分析模型，分析网络安全事件与业务风险的关系。 4.2.2 能根据有害程序、网络攻击、信息破坏、信息内容安全、设备设施故障、灾害性事件等特征进行分类。 4.2.3 能使用常见的安全工具，对有害程序、网络攻击、信息破坏、信息内容安全进行初步分析。 4.2.4 能使用虚拟机等模拟软件，搭建有害程序、网络攻击、信息破坏、信息内容安全分析环境。
	4.3 安全事件应急处置	4.3.1 能根据安全事件的特征，进行行为分析。 4.3.2 能根据安全事件的攻击路径，进行网络安全防护。 4.3.3 能根据安全事件的恶意行为，修复系统响应漏洞。

	4.4 安全应急报告编写	4.4.1 能根据项目要求，收集应急响应监测数据。 4.4.2 能根据项目要求，分析、总结安全事件发生的原因。 4.4.3 能根据项目要求，分析、总结安全事件处置过程。

表 2 工业互联网安全测评与应急职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1.工业互联网网络安全实施	1.1 网络安全架构设计	1.1.1 能根据项目要求，设计、规划工业互联网网络安全架构。 1.1.2 能根据项目要求，规划、配置网络安全设备。 1.1.3 能独立完成网络安全设备的网络连接、部署和配置。
	1.2 操作系统安全配置	1.2.1 能根据项目要求，独立配置系统账户安全权限。 1.2.2 能根据项目要求，独立配置 UGO/ACL 权限。 1.2.3 能根据项目要求，独立配置文件、程序安全权限。
	1.3 网络服务安全配置	1.3.1 能根据项目要求，独立配置交换机、路由器安全权限。 1.3.2 能根据项目要求，独立配置网络服务安全权限。 1.3.3 能分析网络服务中常见的网络安全故障。

2. 工业互联网控制设备安全实施	2.1 工控设备安全配置	2.1.1 能根据项目要求，配置工控设备与网络连接。 2.1.2 能根据项目要求，独立配置工控设备访问权限。 2.1.3 能根据项目要求，独立配置工控设备数据安全权限。
	2.2 工控网络安全配置	2.2.1 能独立完成工控网络设备的网络连接、部署和配置。 2.2.2 能根据项目要求，独立完成对工控网络数据的安全审计权限配置。 2.2.3 能根据项目要求，独立完成对工控网络防护设备安全规则配置。
	2.3 工控协议安全配置	2.3.1 能使用网络数据分析工具，识别网络中使用的通信协议。 2.3.2 能根据项目要求，独立配置工控协议安全规则。
3. 工业互联网网络安全评估	3.1 网络安全评估方案设计	3.1.1 能根据项目需求，设计网络安全评估方案。 3.1.2 能根据项目要求，设计测试路径及测试方法。 3.1.3 能根据项目要求，组织网络安全评估小组，准备评估相关资料工具。
	3.2 渗透测试与验证	3.2.1 能根据项目要求，进行源地址欺骗、报文泛洪、网络探测、畸形报文等网络安全测试。 3.2.2 能根据项目要求，进行内网横向渗透测试。 3.2.3 能根据项目要求，对工业控制系统进行已知漏洞验证。

	3.3 网络安全评估检查	3.3.1 能根据项目要求，对系统中服务器进行安全配置核查。 3.3.2 能根据项目要求，对工业控制系统设备进行安全配置核查。 3.3.3 能根据项目要求，对工业互联网网络架构进行脆弱性分析。 3.3.4 能根据项目要求，对工业互联网安全漏洞进行分级分类。
	3.4 网络安全报告编制	3.4.1 能根据项目报告编写要求，完成渗透测试报告的设计与编写。 3.4.2 能根据项目报告编写要求，完成资产分析报告的设计与编写。 3.4.3 能根据项目报告编写要求，完成网络安全评估报告的设计与编写。
4.工业互联网网络安全应急处置	4.1 安全事件信息管理	4.1.1 能进行信息安全事件制度规划、设计。 4.1.2 能根据项目要求，规划、设计网络安全应急演练和响应方案。 4.1.3 能根据项目要求，从系统重要程度、系统损失和社会影响对信息安全事件分级。
	4.2 安全事件分析	4.2.1 能根据项目要求，分析有害程序、网络攻击、信息破坏、信息内容安全的文件、资源结构。 4.2.2 能根据项目要求，分析有害程序、网络攻击、信息破坏、信息内容安全的行为及特征。 4.2.3 能根据项目要求，分析有害程序、网络攻击、信息破坏、信息内容安全的攻击路径。 4.2.4 能根据项目要求，分析有害程序、网络攻击、信息破坏、信息内容安全的技术实现及检测特征。

	4.3 安全事件应急处置	4.3.1 能对网络安全应急响应规划组织架构。 4.3.2 能根据项目要求，梳理网络安全应急响应的准备、检测、取证、恢复和报告各个环节内容。 4.3.3 能根据项目要求，完成网络安全应急响应报告的规划及编写。 4.3.4 能根据安全事件的特征，进行行为分析。 4.3.5 能根据安全事件的攻击路径，进行网络安全防护。 4.3.6 能根据安全事件的恶意行为，修复系统响应漏洞。
	4.4 安全应急报告编写	4.4.1 能根据项目要求，分析应急响应需求。 4.4.2 能根据项目要求，完成具体角色和责任分工文档设计与编写。 4.4.3 能根据项目要求，完成安全事件技术对应表文档设计与编写。

表 3 工业互联网安全测评与应急职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.工业互联网网络安全规划	1.1 网络安全架构规划	1.1.1 能根据项目要求，独立规划、设计工业互联网网络安全架构。 1.1.2 能根据项目要求，独立规划、设计网络安全设备。 1.1.3 能根据项目要求，独立规划、设计网络安全测试方案。 1.1.4 能根据项目要求，独立规划、设计网络安全防护方案。

	1.2 操作系统安全设计	1.2.1 能根据项目要求，独立规划、设计 windows 域安全环境搭建及配置。 1.2.2 能根据项目要求，独立规划、设计 windows 安全防护策略。 1.2.3 能根据项目要求，独立规划、设计 linux 系统安全防护策略。
	1.3 网络服务安全设计	1.3.1 能根据项目要求，分析网络协议弱点并设置防护策略。 1.3.2 能根据项目要求，独立配置网络服务安全权限。 1.3.3 能分析网络服务中的常见安全故障。
2. 工业互联网控制设备安全规划	2.1 工控设备安全设计	2.1.1 能独立配置工控设备与网络连接。 2.1.2 能根据项目要求，独立配置工控设备访问权限。 2.1.3 能根据项目要求，独立配置工控设备数据安全权限。
	2.2 工控网络安全设计	2.2.1 能独立完成工控网络设备与网络连接。 2.2.2 能根据项目要求，独立完成对工控网络数据的安全审计权限配置。 2.2.3 能根据项目要求，独立完成对工控网络防护设备安全规则配置。
	2.3 工控协议安全设计	2.3.1 能根据项目要求，独立规划、设计工业控制系统设备安全架构。 2.3.2 能根据项目要求，规划、设计工业控制系统网络安全架构。 2.3.3 能根据项目要求，规划、设计工业控制系统设备安全策略。

3.工业互联网网络安全评估	3.1 网络安全评估方案规划	3.1.1 能根据项目要求，独立规划、设计网络安全评估方案、流程。 3.1.2 能根据项目要求，独立规划、设计渗透测试路径。 3.1.3 能根据项目要求，设计、选择、实现网络安全评估工具。
	3.2 渗透测试与验证	3.2.1 使用黑盒测试方法，对工业互联网网络进行安全漏洞测试。 3.2.2 能利用中间人工具，对工业控制系统网络数据进行安全测试。 3.2.3 能根据项目要求，利用固件分析工具，对工业控制系统固件进行安全分析。
	3.3 网络安全评估检查	3.3.1 能根据项目要求，独立分析工业控制系统各生命周期风险。 3.3.2 能根据项目要求，规划、设计风险评估范围，组建风险评估团队。 3.3.3 能根据项目要求，规划、设计风险评估相关制度。 3.3.4 能根据项目要求，对工业互联网环境进行安全配置核查。 3.3.5 能根据项目要求，对工业互联网环境进行脆弱性分析。
	3.4 网络安全报告编制	3.4.1 能根据项目报告编写要求，设计与编写渗透测试报告。 3.4.2 能根据项目报告编写要求，设计与编写资产分析报告。 3.4.3 能根据项目报告编写要求，设计与编写网络安全评估报告。

4.工业互联网网络安全应急处置	4.1 安全事件信息管理	4.1.1 能根据项目要求，规划、设计信息安全事件制度。 4.1.2 能根据项目要求，规划、设计网络安全应急演练和响应方案。 4.1.3 能根据项目要求，从系统重要程度、系统损失和社会影响对信息安全事件分级。
	4.2 安全事件分析	4.2.1 能使用常见的加密算法，分析有害程序、网络攻击、信息破坏、信息内容安全逻辑。 4.2.2 能使用常见的反调试技术，分析有害程序、网络攻击、信息破坏、信息内容安全的行为。 4.2.3 能使用 DUMP 工具，调试有害程序、网络攻击、信息破坏、信息内容安全的内容。 4.2.4 能使用脱壳技术，分析有害程序、网络攻击、信息破坏、信息内容安全的组成。
	4.3 安全事件应急处置	4.3.1 能根据项目要求，规划、设计网络安全应急响应制度。 4.3.2 能根据项目要求，规划、设计网络安全应急响应流程。 4.3.3 能根据项目要求，规划、设计网络安全预防与预警机制。 4.3.4 能根据项目要求，规划、设计网络安全应急响应小组。 4.3.5 能根据安全事件的特征，进行行为分析。 4.3.6 能根据安全事件的攻击路径，进行网络安全防护。 4.3.7 能根据安全事件的恶意行为，修复系统响应漏洞。
	4.4 安全应急报告编写	4.4.1 能根据项目要求，规划、设计网络安全应急报告文档。 4.4.2 能根据项目要求，规划、设计应急响应协调方案。

参考文献

[1] 教育部关于印发《职业教育专业目录（2021年）》的通知（教职成〔2021〕2号）

[2] 《教育部关于公布2019年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2020〕2号）

[3] 《教育部关于公布2020年度普通高等学校本科专业备案和审批结果的通知》（教高函〔2021〕1号）

[4] 《国家职业技能标准编制技术规程》（2018年版）

[5] 《普通高等学校本科专业类教学质量国家标准》

[6] 《工业互联网人才白皮书》（2020）

[7] 《工业互联网体系架构》（版本2.0）

[8] 《工业互联网平台白皮书》（2019）

[9] 《工业互联网标准体系》（版本2.0）

[10] 《工业互联网安全框架》（2018）