工业互联网安全管理师

职业能力等级评价标准

（试行稿）

1 项目概况

1.1 项目名称

工业互联网安全管理师

1.2 项目定义

从事工业互联网安全监管与管理，保障相关设备、网络、数据平台合规，能进行风险评估、安全措施设计与实施、威胁监控响应及管理策略更新优化的工作人员。

1.3 能力等级

本项目共设三个等级，分别为：初级、中级、高级。

1.4 能力特征

熟悉工业互联网及网络安全等专业知识，掌握常用安全工具和软件等技术能力，具备出色的问题诊断与解决、良好的沟通协调能力，以及因信息安全领域发展需不断学习适应新技术、新标准的持续学习能力。

1.5 职业能力等级评价要求

1.5.1 申报条件

具备以下条件之一者，可申报初级：

（1）累计从事相关职业工作 1 年（含）以上；

（2）相关专业在校学生。

具备以下条件之一者，可申报中级：

（1）取得本项目或相关职业初级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作 2 年（含）以上。

（2）累计从事相关职业工作 4 年（含）以上。

（3）取得相关专业毕业证书。

具备以下条件之一者，可申报高级：

（1）取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作 3 年（含）以上。

（2）累计从事相关职业工作 6 年（含）以上。

（3）具有高等职业学校、高级技工学校、技师学院相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）。

（4）具有大专及以上相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作 1 年（含）以上。

1.5.2 申报条件注释

（1）满足本项目高级别申报条件可申报本项目低级别。

（2）相关职业：网络安全分析师、信息安全管理员、数据安全专员、网络安全架构师、安全运维工程师、信息安全审计员、云安全工程师、移动安全工程师等工业互联网、网络与信息安全类职业。

（3）相关专业：网络空间安全专业、 信息安全专业、计算机科学与技术专业、通信工程专业等电子信息类、计算机类和通信类专业。

1.5.3 评价方式

职业能力等级评价考试包括理论知识、技能操作两个科目，较高等级必要时可增加综合评审。

理论知识考试以笔试为主，条件成熟时试点开展网络考试，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求。技能操作考核主要采用现场操作、模拟操作、面试答辩等方式进行，主要考核从业人员从事本职业应具备的技能水平。综合评审通常采取审阅申报材料、技术答辩等方式进行全面评议和审查。理论知识考试和技能操作考核均采用百分制，成绩达到 60 分以上者为合格。

1.5.4 监考人员、考评人员与考生配比

理论知识考试和技能操作考核中的监考人员与考生配比不低于 1：15，且每个考场不少于 2 名监考人员。技能操作考核中考评人员为 3 人以上单数。

1.5.5 评价时间

理论知识考试时间不少于 90 分钟；技能操作考核时间:初级不少于 120 分钟，中级/高级不少于 180 分钟。

1.5.6 评价场所设备

理论知识考试：在具备稳定的网络环境、性能良好的计算机设备以及监控设施的考试场所进行。

技能操作考核：在标准联网多媒体计算机教室进行，具备模拟真实工业互联网环境的相关设备、网络设施及数据平台等硬件条件。

2 基本要求

2.1 职业道德

（1）遵纪守法，爱岗敬业。

（2）认真严谨，忠于职守。

（3）勤奋好学，不耻下问。

（4）钻研业务，勇于创新。

（5）精益生产，工匠精神。

2.2 基础知识

2.2.1 计算机及网络知识

（1）计算机基础操作知识。

（2）计算机常用应用软件的安装及使用方法。

（3）计算机网络基础知识。

（4）网络设备（如路由器、交换机等）应用知识。

2.2.2 信息安全与合规相关知识

（1）信息安全基础知识。

（2）数据相关合规性要求（DSMM）。

（3）安全保密知识。

（4）国家数据安全相关法律法规、国家/地方标准。

2.2.3 操作系统知识

（1）Linux 基础知识与操作。

（2）Windows 基础知识与操作。

（3）Unix 基础知识与操作。

（4）其它操作系统知识与操作。

2.2.4 数据库安全知识

（1）关系型、时间序列数据库的基本概念。

（2）SQL 基础。

（3）Oracle、MySQL、NoSQL 等数据库基础。

（4）其它数据库知识及数据安全技术应用。

2.2.5 云计算、大数据知识

（1）云计算/大数据基本概念。

（2）云产品的操作使用。

（3）典型大数据平台操作使用。

2.2.6 工业互联网基础知识

（1）工业互联网网络体系。

（2）工业互联网标识解析体系。

（3）工业互联网平台架构。

（4）工业互联网安全体系。

（5）工业互联网设备及软硬件基础知识。

2.2.7 安全法律法规知识

（1）《中华人民共和国劳动法》相关知识。

（2）《中华人民共和国安全生产法》相关知识。

（3）《中华人民共和国网络安全法》相关知识。

（4）《中华人民共和国数据安全法》相关知识。

3 工作要求

本标准对初级、中级、高级各级别的技能要求依次递进，高级别涵盖低级别的要求。

3.1 初级

职业功能	工作内容	技能要求	相关知识
1.态势评估	1.1 业务流程梳理	1.1.1 能收集业务对象的安全业务信息，掌握业务状况 1.1.2 能填写系统安全业务信息调查表，记录业务详情	1.1.1 基础安全业务梳理方法 1.1.2 基础办公软件工具使用方法
	1.2 安全态势调研	1.2.1 能利用在线问卷或现场调研表，收集系统安全态势信息 1.2.2 能根据调研结果填写安全态势报告单，汇报态势情况	1.2.1 问卷调研与访谈的基础方法 1.2.2 系统安全框架的基础知识
2.防护运维	2.1 设备防护运维	2.1.1 能监控设备运行状况，保障设备稳定 2.1.2 能检查设备访问及相应安全策略，确保设备安全	2.1.1 设备监控基本内容 2.1.2 设备访问及安全策略
	2.2 工控系统防护运维	2.2.1 能配置工控系统用户组，规范用户分组 2.2.2 能检查用户组访问策略配置情况，核实策略落实	2.2.1 用户密码的通用规则与设定方法 2.2.2 用户权限分配设定方法
	2.3 网络基础设施防护运维	2.3.1 能配置路由器、交换机等网络设备的访问策略，管控网络访问 2.3.2 能根据网络访问策略配置防火墙等安全设备，加强网络防护	2.3.1 基础网络知识与主流路由器、交换机的操作方法 2.3.2 主流防火墙操作方法
	2.4 应用防护运维	2.4.1 能配置工业互联网平台及应用程序访问策略，优化访问控制 2.4.2 能校验工业互联网平台及应用程序数据日志，保障数据准确	2.4.1 主流工业互联网平台管理后台操作方法 2.4.2 数据安全合规知识及数据安全相关技术工具应用知识
	2.5 数据防护运维	2.5.1 能使用 CRC 等校验技术验证数据完整性，保证数据完	2.5.1 常见校验工具使用方法

		好 2.5.2 能备份数据防护运维日志，留存运维记录	2.5.2 常见日志备份工具的使用方法
3.隐患排查	3.1 设备隐患排查	3.1.1 能排查非必要设备接口物理连接等隐患，消除物理风险 3.1.2 能根据软件漏洞发布信息更新补丁，修复软件漏洞	3.1.1 工业设备主流接口基础知识 3.1.2 系统漏洞扫描工具使用方法
	3.2 工控系统隐患排查	3.2.1 能配置工控软件用户组及操作权限，规范用户权限 3.2.2 能识别工控软件服务进程、端口使用异常状态，发起预警，防范软件异常	3.2.1 用户操作权限相关指令使用方法。 3.2.2 系统网络服务相关指令使用方法
	3.3 网络安全设施隐患排查	3.3.1 能监测防火墙、安全隔离网闸等边界防护设备运行状态，掌控防护设备 3.3.2 能识别入侵防御系统异常状态，发起预警，应对入侵威胁	3.3.1 主流防火墙、网闸等设备使用方法 3.3.2 入侵检测、防御系统知识
	3.4 应用隐患排查	3.4.1 能预警工业互联网平台及应用程序非法登录，保障登录安全 3.4.2 能识别非可信来源的工业应用运行，防范不可信应用	3.4.1 应用安全威胁基础知识 3.4.2 应用安全审计知识
	3.5 数据隐患排查	3.5.1 能配置数据库数据访问权限，管控数据访问 3.5.2 能销毁硬盘、光盘等存储介质中的数据，清除存储数据	3.5.1 主流数据库操作的基础知识 3.5.2 数据逻辑销毁、物理销毁相关知识

3.2 中级

职业功能	工作内容	技能要求	相关知识
1.态势评估	1.1 评估表单设计	1.1.1 能设计安全业务信息收集清单，定位风险源头 1.1.2 能设计安全业务信息调查表，分析潜在风险	1.1.1 待评估的业务对象基本业务知识 1.1.2 调查表、调查问卷的一般设计方法
	1.2 态势评估实施	1.2.1 能评估安全技术、措施和运营，并出具报告 1.2.2 能根据态势评估报告改进安全建议，提高系统稳定性	1.2.1 系统安全评估基本原理与方法 1.2.2 工业系统安全防护体系知识
2.防护运维	2.1 设备防护运维	2.1.1 能配置设备远程访问策略，管控用户权限 2.1.2 能配置设备访问及相应安全策略，限制非法操作	2.1.1 系统远程登录工具的使用方法 2.1.2 设备安全审计的基本内容
	2.2 工控系统防护运维	2.2.1 能设计用户组访问策略，监测访问行为 2.2.2 能填写工控软件安全审计记录表，审查安全合规	2.2.1 常见工控系统基本配置方法 2.2.2 基础办公软件工具使用方法
	2.3 网络基础设施防护运维	2.3.1 能设计路由器、交换机等网络设备的访问策略 2.3.2 能根据网络访问策略设计防火墙等安全设备防护方案	2.3.1 基础网络知识与主流路由器、交换机的配置方法 2.3.2 常见网络攻击的形式和基本应对方法
	2.4 应用防护运维	2.4.1 能预警工业互联网平台及应用程序非法登录，并启动处置预案 2.4.2 能禁止非可信来源的工业应用运行	2.4.1 工业互联网平台与应用程序运行日志相关内容相关知识 2.4.2 工业应用安全审计的基本内容
	2.5 数据防护运维	2.5.1 能设计数据完整性校验方案，保障数据完整 2.5.2 能识别数据防护运维日志异常记录，洞察日志异常	2.5.1 常见数据校验方法与校验工具使用方法 2.5.2 常见数据库运行日志格式知识
3.隐患排查	3.1 设备隐患排查	3.1.1 能使用 Sniffer 等工具对设备进行安全渗透测试，检测设备安全	3.1.1 渗透测试类型和工具应用知识 3.1.2 系统脚本语言的编写知

		3.1.2 能根据安全渗透测试结果排查安全隐患，消除设备隐患	识
	3.2 工控系统隐患排查	3.2.1 能制定工控软件用户组及操作权限方案，规划用户权限 3.2.2 能识别异常访问行为，并启动处置预案	3.2.1 常见工控系统用户组及操作权限配置方法 3.2.2 常见故障修复工具使用方法
	3.3 网络基础设施隐患排查	3.3.1 能制定防火墙、安全隔离网闸等边界防护方案，构建边界防护 3.3.2 能根据入侵防御系统预警，执行处置预案，处理入侵预警	3.3.1 网络安全基础知识 3.3.2 网络攻防手段与相应工具使用方法
	3.4 应用隐患排查	3.4.1 能监测系统运行环境，识别异常运行状况，掌控系统状况 3.4.2 能配置应用程序的启动、更新策略及访问权限，规范程序运行	3.4.1 常见的系统运维工具及基本使用方法 3.4.2 程序运行资源配置相关指令操作方法
	3.5 数据隐患排查	3.5.1 能制定数据敏感字段识别方案，明确数据重点 3.5.2 能根据数据敏感度识别方案对数据包进行脱敏处理，保障数据安全	3.5.1 国家信息保护相关法律知识 3.5.2 数据替换、仿真、加密等常见数据脱敏知识
4.问题处置	4.1 设备安全问题处置	4.1.1 能识别身份鉴别信息盗用并停用账户，保护用户安全 4.1.2 能设计终端接入限制策略，规范终端接入 4.1.3 能设计非法用户登录等应急响应预案，应对突发状况	4.1.1 网路窃听的一般形式和手段 4.1.2 系统脚本语言的编写知识 4.1.3 系统入侵处置流程知识
	4.2 工控系统安全问题处置	4.2.1 能根据安全漏洞发布信息，更新恶意代码库，提升系统防护	4.2.1 常见安全工具更新方法 4.2.2 系统入侵处置流程知识

		4.2.2 能执行系统入侵应急处置预案，保障系统稳定	
	4.3 网络基础设施安全问题处置	4.3.1 能识别网络节点入侵行为，记录并阻断接入，防范网络攻击 4.3.2 能执行网络入侵处置预案，优化网络安全	4.3.1 常用网络安全软件的功能与基本用法 4.3.2 常见网络攻击手段的特征和屏蔽方法

3.3 高级

职业功能	工作内容	技能要求	相关知识
1.态势评估	1.1 方案设计	1.1.1 能编制系统安全评估方案，规划评估流程 1.1.2 能根据评估结果优化系统安全方案，提升安全水平	1.1.1 工业互联网系统各层安全内容相关知识 1.1.2 安全业务知识和安全风险的评估方法
	1.2 流程设计	1.2.1 能根据系统安全方案制定实施计划，推动方案落地 1.2.2 能设计系统安全策略、管理制度、流程规范，完善安全体系	1.2.1 系统安全体系框架及原理 1.2.2 工业互联网安全系统安全防护框架知识
2.隐患排查	2.1 设备隐患排查	2.1.1 能编制设备安全渗透测试方案，规划测试流程 2.1.2 能根据安全渗透测试结果优化设备安全配置方案	2.1.1 渗透测试类型、方法、技巧等相关知识 2.1.2 系统安全脚本的编写知识
	2.2 工控系统隐患排查	2.2.1 能优化工控系统用户组及操作权限方案，规范用户操作 2.2.2 能设计异常访问行为处理预案，应对异常情况	2.2.1 PLC、DCS、FCS 等系统相关软件基础与操作知识 2.2.2 工控系统常见故障与处理操作手册
	2.3 网络基础设施隐患排查	2.3.1 能优化防火墙、安全隔离网闸等边界防护方案，加固边界防御 2.3.2 能编制防御系统入侵行为处理预案，抵御入侵威胁	2.3.1 网络安全与安全设备基础知识 2.3.2 网络攻防手段与相应工具使用方法
	2.4 应用隐患排查	2.4.1 能使用脚本批量配置应用程序的启动、更新策略及访问权限，并对配置进行记录 2.4.2 能使用脚本配置工业程序可信更新源，保障程序更新安全	2.4.1 常见的系统运维工具及基本使用方法 2.4.2 常见工业应用来源列表
	2.5 数据隐患排查	2.5.1 能制定数据库备份策略，确保数据可恢复 2.5.2 能制定敏感数据判定与	2.5.1 常见数据备份工具的使用方法 2.5.2 个人信息保护相关法律

		处理预案，保护敏感数据安全	
3.问题处置	3.1 设备安全问题处置	3.1.1 能优化设备终端接入限制策略，加强终端管控 3.1.2 能优化非法用户登录等应急响应预案，提高应急效率	3.1.1 系统脚本语言的编写知识 3.1.2 系统入侵处置流程知识
	3.2 控制系统安全问题处置	3.2.1 能利用安全工具扫描系统漏洞，更新恶意代码库，增强系统防护 3.2.2 能设计系统入侵应急处置预案，完善应急机制	3.2.1 系统漏洞扫描工具的使用知识 3.2.2 系统入侵处置流程知识
	3.3 网络基础设施安全问题处置	3.3.1 能配置脚本阻断网络节点攻击行为，防御网络攻击 3.3.2 能设计网络入侵处置预案，提升处置能力	3.3.1 网络节点攻击的一般防御方法，如安全组、强化密码等 3.3.2 常见网络攻击手段的特征和屏蔽方法
	3.4 应用安全问题处置	3.4.1 能优化系统运行环境，停止异常程序运行，保障系统稳定 3.4.2 能配置应用程序更新源，阻止非法来源程序下载、执行	3.4.1 常见的系统运维工具基本使用方法 3.4.2 应用程序资源分配相关指令操作方法
	3.5 数据安全问题处置	3.5.1 能制定策略，阻断对数据的非法访问、下载、传输等操作 3.5.2 能制定数据违规操作应急处置预案，应对数据危机	3.5.1 主流数据库操作的基础知识 3.5.2 数据逻辑、物理销毁工具使用方法
4.培训指导	4.1 安全知识培训	4.1.1 能够制定初级、中级技术人员培训大纲，规划培训框架 4.1.2 能够编写初级、中级技术人员培训讲义，丰富培训内容 4.1.3 能够完成初级、中级技术人员课程培训讲授，传授专	4.1.1 本职业技能与理论基础知识和培训工作计划的制订要求 4.1.2 培训方案编制和实施的要求和方法 4.1.3 培训教材、讲义、课件的编写知识

		业知识	
	4.2 安全工作指导	4.2.1 能够指导初级、中级技术人员开展安全态势评估，提升评估能力 4.2.2 能够指导初级、中级技术人员开展安全系统运维，保障系统运行 4.2.3 能够指导初级、中级技术人员开展安全隐患排查，消除安全隐患 4.2.4 能够指导中级技术人员进行安全系统问题处置，解决系统问题	4.2.1 指导技能操作的知识 4.2.2 技术革新的方法 4.2.3 操作经验和技能总结方法 4.2.4 技能和理论基础知识水平考核的要求和方法

4 权重表

4.1 理论知识权重表

项目		技能等级		
		初级	中级	高级
		（%）	（%）	（%）
基础要求	职业道德	5	5	5
	基础知识	15	10	5
相关知识	工业互联网系统安全态势评估	30	20	10
	工业互联网系统安全防护运维	30	25	–
	工业互联网安全隐患排查	20	20	30
	工业互联网安全问题处置	–	20	30
	工业互联网安全培训指导	–	–	20
合计		100	100	100

4.2 技能要求权重表

项目		技能等级		
		初级	中级	高级
		（%）	（%）	（%）
技能要求	工业互联网系统安全态势评估	40	30	10
	工业互联网系统安全防护运维	30	30	–
	工业互联网安全隐患排查	30	20	30
	工业互联网安全问题处置	–	20	40
	工业互联网安全培训指导	–	–	20
合计		100	100	100