工业信息安全网络规划师

职业能力等级评价标准

（试行稿）

1 项目概况

1.1 项目名称

工业信息安全网络规划师

1.2 项目定义

从事工业环境中网络安全防护、监测及处置等任务的专业人员。

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

具备计算机网络、信息安全、工业网络及工业控制系统理论基础，能够独立完成网络安全的规划、实施与运维的能力；具备网络拓扑规划、网络设备选型、网络部署及设备配置能力；具备运维网络设备及系统的能力；具备从安全整体出发，考虑网络设备与工业系统的协同工作，确保系统性能、功耗、成本等方面的最优平衡的能力；具备与技术团队、项目经理及客户有效沟通，准确理解需求并按时交付的能力。

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，相关专业在校学生或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。

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 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。

1.5.3 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。

1.5.4 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。

1.5.5 评价场所设备

理论知识考试：在标准教室或标准联网多媒体计算机教室进行。

技能操作考核：在标准联网多媒体计算机教室进行，考生计算机需要按照考核要求安装考试系统客户端及相关应用软件，考试结束后能完成环境的还原。

2 基本要求

2.1 职业道德

(1)诚实守信，勤勉尽责，谨情从业。

(2)坚持独立、客观、公正的原则。

(3)遵守国家法律法规。

2.2 职业守则

(1)客观公正，保持独立性，不受各方的控制和影响。

(2)对国家秘密、商业秘密和个人隐私予以保密。

(3)遵守职业道德规范，不从事任何损害职业形象的活动。

2.3 基础知识

2.3.1 计算机基础知识

（1）操作系统的原理

（2）Linux 系统基本命令

（3）Windows命令提示符基础命令

（4）数据库基本概念

2.3.2 计算机网络基础知识

（1）常见网络拓扑结构

（2）网络协议工作原理

（3）交换机工作原理

（4）路由器工作原理

2.3.3 工业网络基础知识

（1）工业网络拓扑结构

（2）工业网络协议工作原理

（3）工业交换机工作原理

（4）工业路由器工作原理

2.3.4 工业控制系统基础知识

（1）工业控制系统概念

（2）工业控制系统类型

2.3.5 网络安全基础知识

（1）网络安全威胁类型

（2）防火墙基本原理

（3）入侵检测系统工作原理

（4）入侵防御系统工作原理

2.3.6 相关法律、法规、标准知识

（1）《中华人民共和国网络安全法》的相关知识。

（2）《中华人民共和国数据安全法》的相关知识。

（3）《中华人民共和国个人信息保护法》的相关知识。

（4）《关键信息基础设施安全保护条例》的相关知识。

（5）《信息安全等级保护管理办法》的相关知识。

（6）其它网络安全相关法律法规、管理规定、标准的相关知识。

3 工作要求

本标准初级、中级、高级的技能要求和相关知识要求依次递进，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	相关知识要求
1.安全防护	1.1 网络部署	1.1.1 能初始化交换机、路由器等网络设备，联通网络设备。 1.1.2 能配置IP地址、VLAN、STP、网关、DNS、路由协议等，联通基础网络。	1.1.1 交换机、路由器的配置方法 1.1.2 网络协议配置方法
	1.2 安全规则实施	1.2.1 能配置桌面操作系统密码规则、账户规则及系统安全规则，防护桌面系统账户安全。 1.2.2 能设置桌面操作系统防火墙的入站规则、出站规则及流量监测等功能，防护桌面系统网络安全。 1.2.3 能安装防病毒软件，设置病毒库更新、木马拦截、病毒查杀及病毒隔离等规则，防护桌面系统安全。	1.2.1 操作系统访问控制策略实施方法 1.2.2 防火墙的配置方法 1.2.3 防病毒软件安装及配置方法
2.安全监测	2.1 网络监测	2.1.1 能监测路由器、交换机等网络设备性能，提交设备监测报告。 2.1.2 能检查网络设备信号指示灯、温度等运行状态，提交日常巡检报告。	2.1.1 网络设备性能监测方法 2.1.2 网络设备巡检方法
	2.2 系统监测	2.2.1 能使用系统监测工具，监测系统设备的CPU、内存、硬盘及网络流量等状态，提交日志监测报告。 2.2.2 能使用系统安全检测工具，检测木马及	2.2.1 操作系统的日志/告警原理 2.2.2 病毒感染、木马植入等终端类攻击

		病毒程序，提交检测报告。	行为的识别方法 2.2.3 操作系统异常进程的判别方法
3.安全处置	3.1 网络安全处置	3.1.1 能使用网络设备配置工具，配置VLAN、封禁IP地址，隔离攻击源。 3.1.2 能分析网络层面影响范围与网络设备审计日志，撰写网络攻击报告。	3.1.1 WAF产品的配置方法 3.1.2 网络安全产品的用户权限管理方法 3.1.3 日志分析方法
	3.2 系统安全处置	3.2.1 能使用杀毒软件及防火墙等系统防护工具，扫描并清除桌面操作系统的木马、病毒等潜在威胁。 3.2.2 能使用系统漏洞扫描工具，扫描桌面操作系统漏洞。 3.2.3 能下载与安装系统补丁，修复系统漏洞。	3.2.1 病毒扫描工具的使用方法 3.2.2 系统补丁安装方法

3.2 中级

职业功能	工作内容	技能要求	相关知识要求
1.安全防护	1.1 网络部署	1.1.1 能初始化工业网络设备及安全设备，联通工业网络设备。 1.1.2 能配置工业网络设备MAC地址绑定、NAT等，联通工业网络设备。 1.1.3 能安装、部署与配置无线接入点，联通无线终端与有线网络设备。 1.1.4 能安装、部署工业入侵检测系统、工业防火墙、隔离网闸等工业网络安全设备，搭建工业网络安全防护环境。	1.1.1 工业网络安全设备基础配置方法 1.1.2 入侵检测设备技术原理及配置方法 1.1.3 安全隔离网闸设备的配置方法 1.1.4 工业防火墙设备的配置方法 1.1.5 无线网络配置方法
	1.2 安全规则实施	1.2.1 能配置工业入侵检测系统、工业防火墙、隔离网闸等工业网络安全设备的规则，防护工业网络安全环境。 1.2.2 能配置服务器操作系统用户规则、密码规则、访问控制规则、权限控制等系统安全规	1.2.1 工业网络安全设备安全规则配置方法 1.2.2 操作系统安全防护技术 1.2.3 防火墙隔离区区

		则，防护服务器操作系统的系统安全。 1.2.3 能配置防火墙隔离区区域划分与规则，联通系统服务内外部网络。	域划分方法
2.安全监测	2.1 网络监测	2.1.1 能使用Wireshark、SolarWinds 等网络监测工具，监测工业网络流量，识别网络异常，提交异常报告文档。 2.1.2 能核对监测报告的数据、术语等信息，修正监测报告。	2.1.1 工业网络流量监测方法 2.1.2 工业网络流量异常识别方法 2.1.3 工业网络设备性能指标
	2.2 系统监测	2.2.1 能使用系统监测工具，监测PLC（可编程逻辑控制器）、DCS（分散控制系统）等工业控制系统，识别关键进程与服务状态异常，提交异常报告文档。 2.2.2 能导出工业系统中的作业生产、设备状态等数据，备份关键数据。	2.2.1 工业系统异常识别方法 2.2.2 工业系统数据备份与恢复技术
3.安全处置	3.1 网络安全处置	3.1.1 能利用网络设备配置工具，封禁攻击源IP地址等操作，遏制网络攻击。 3.1.2 能分析网络运行数据及网络安全日志，溯源安全事件，提交安全报告文档。	3.1.1 工业网络设备应急处置技术 3.1.2 数据报文抓取和分析方法 3.1.3 网络安全产品日志数据分析方法
	3.2 系统安全处置	3.2.1 能更新系统补丁与病毒库，优化防护软件配置。 3.2.2 能使用漏洞扫描工具，扫描工业系统漏洞。 3.2.3 能下载、安装工业系统补丁，验证与修复工业系统漏洞。	3.2.1 工业系统病毒查杀与防护工具使用方法 3.2.2 安全漏洞扫描方法 3.2.3 工业系统补丁安装方法

3.3 高级

职业功能	工作内容	技能要求	相关知识要求

1.安全防护	1.1 网络部署	1.1.1 能设置三层交换机、工业路由器等工业网络设备的VLAN、路由策略、QoS等功能，优化带宽利用率、网络吞吐量等网络性能指标。 1.1.2 能设置无线网络用户漫游、用户隔离、加密认证等功能，搭建无线网络安全环境。	1.1.1 工业网络设备的配置与优化技巧 1.1.2 网络性能指标体系 1.1.3 无线网络安全技术
	1.2 安全规则实施	1.2.1 能制定访问控制、数据加密、安全审计等安全策略，构建网络安全策略框架。 1.2.2 能分析安全潜在威胁和业务需求，调整和优化安全策略。 1.2.3 能分析业务流程、等保要求，设计工业信息网络拓扑结构。	1.2.1 企业级网络安全策略体系框架构建方法 1.2.2 安全策略的动态管理与适应性调整
2.安全监测	2.1 网络安全监测	2.1.1 能梳理网络安全监测指标，构建网络监测指标体系。 2.1.2 能制定网络监测计划，分配网络监测任务。	2.1.1 网络安全监测指标体系设计方法 2.1.2 团队管理与任务分配策略
	2.2 系统安全监测	2.2.1 能分析梳理系统安全监测需求，设计系统监测方案。 2.2.2 能建立应急响应机制，制定应急处置预案。	2.2.1 系统监测方案设计方法 2.2.2 应急响应预案与流程设计方法
3.安全处置	3.1 网络安全处置	3.1.1 能实施应急处置预案，开展紧急救援与网络恢复工作。 3.1.2 能调查与取证安全事件、评估损失，提交取证报告。	3.1.1 网络安全事件应急响应体系与流程 3.1.2 网络安全调查与取证技术
	3.2 系统安全处置	3.2.1 能识别系统中存在的未经授权的访问、数据篡改、网络攻击等潜在安全漏洞和风险点，评估和优化系统安全策略。 3.2.2 能制定和执行整改计划，监督整改过程。	3.2.1 工业控制系统安全策略评估方法 3.2.2 项目管理方法

4 权重表

4.1 理论知识权重表

	技能等级		
	初级	中级	高级

项目		（%）	（%）	（%）
基本要求	职业道德	5	5	5
	基础知识	15	10	5
相关知识	安全防护	30	25	25
	安全监测	25	30	25
	安全处置	25	30	40
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	安全防护	40	30	25
	安全监测	30	35	30
	安全处置	30	35	45
合计		100	100	100