

工业和信息化人才培养工程培训课程标准

5G应用安全技术

(试行版)

工业和信息化部教育与考试中心

工业和信息化部教育与考试中心

二〇二二年十二月

说 明

为贯彻落实《关于加强和改进工业和信息化人才队伍建设的实施意见》（工信部人〔2022〕138号），立足新发展阶段、贯彻新发展理念、构建新发展格局，工业和信息化部教育与考试中心依据数字技术、智能制造等行业发展人才实际需要，积极整合行业教育资源优势，组织行业专家、教育专家持续研发《工业和信息化人才培养工程培训课程标准》（以下简称“标准”），用于指导工业和信息化人才培养工程相关培训课程建设，高质量推动工业和信息化人才培养工程发展。

《标准》以客观反映现阶段行业技术发展水平和从业人员能力要求为目标，在充分考虑经济发展、科技进步和产业结构变化的基础上，对课程的等级、模块划分进行定义，对培训内容要求、专业能力要求、知识要求和考核权重进行了详细说明。

《标准》组编遵循了有关技术规程的要求，既保证体例规范，又体现以专业活动为导向、以专业技术技能为核心的特点，模块化的结构使其具有根据技术发展进行调整的灵活性和实用性，符合培训工作的需要。

本《标准》编制工作由工业和信息化部教育与考试中心具体组织实施，参与标准编制单位有广东通信行业职业技能鉴定中心、广州传知信息科技有限公司。参与编制人有杨帆、刘志文、郑镇礼、曾雪琴、闫细民、王振世、郭雪雯倩。

本《标准》经工业和信息化部教育与考试中心批准，自颁布之日起施行。

工业和信息化人才培养工程

培训课程标准

1 课程概况

1.1 课程名称

5G 应用安全技术

1.2 课程定义

5G 新应用场景、新网络架构、新空口技术和用户隐私安全等方面引发的安全需求，给 5G 应用安全技术研究提出了新的挑战。本课程了解 5G 网络关键技术及面临的风险，并提升应对 5G 应用安全的实操能力。

1.3 课程技能等级

本课程共设三个等级，分别为：初级、中级、高级。

1.4 课程环境条件

室内、常温。

1.5 课程能力要求

具有较强的学习能力、研究能力；具有一定的理解、判断和表达能力；具有一定的分析解决问题的能力 and 沟通能力。

1.6 普通受教育程度

具有大专及以上学历。

1.7 课程培训要求

1.7.1 培训期限

初级课程不少于线上或线下 80 标准学时；中级课程不少于线上或线下 120 标准学时；高级课程不少于线上或线下 180 标准学时，每学时为 45 至 60 分钟。

1.7.2 培训教师

培训初级、中级理论知识或专业能力培训任务人员，应具有相关课程培训经验 1-3 年。

承担高级理论知识或专业能力培训任务人员，应具有相关课程培训经验 5 年以上，或具有相关职业高级专业技术等级、相关专业高级职称二者之一。

1.7.3 培训场所设备

理论知识培训在标准教室或线上平台进行；专业能力培训在具有相应软、硬件条件的培训场所进行。

操作技能培训需提供所需的材料、工具、设备、软件等。

2 基本要求

2.1 专业道德

2.1.1 专业道德基本知识

2.1.2 专业守则

- (1) 遵纪守法，爱岗敬业
- (2) 精益求精，勇于创新
- (3) 诚实守信，恪守职责
- (4) 遵守规程，安全操作
- (5) 认真严谨，忠于职守

2.2 基础知识

2.2.1 基础理论知识

- (1) 5G 网络的场景和指标
- (2) 5G 应用的端管云架构
- (3) 5G 应用安全需求
- (4) 5G 应用安全威胁
- (5) 5G 应用安全分级
- (6) 5G 应用安全关键技术
- (7) 5G 应用安全方案

2.2.2 实操能力知识

- (1) 5G 应用架构设计
- (2) 5G 应用安全知识库使用
- (3) 基于切片的 5G 应用安全方案设计（使用 5G 仿真环境）
- (4) 基于边缘计算的 5G 应用安全方案设计（使用 5G 仿真环境）

3 课程内容要求

本标准对初级、中级、高级各级别的课程要求依次递进，高级别涵盖低级别的要求。

3.1 初级

课程模块	培训内容	专业能力要求	相关知识要求
1. 5G 应用技术基础	1.1 移动制式演进技术	1.1.1 能了解移动制式技术的底层逻辑 1.1.2 能理解从1G到5G的技术演进 1.1.3 能理解从1G到5G的3GPP协议演进脉络	1.1.1 光束公式和香农公式在移动通信中的作用 1.1.2 从模拟移动，到数字移动；从电路域到分组域的演进 1.1.3 3GPP协议关键技术的演进
	1.2 5G 应用场景和指标	1.2.1 能掌握5G三大场景及其应用 1.2.2 能掌握并理解5G八大指标及应用要求	1.2.1 5G大带宽、大连接、低时延场景，以及各自应用特点 1.2.2 5G的速率指标、流量和连接密度指标、效率指标，以及各种应用的指标要求
2. 5G 应用安全需求和挑战	2.1 5G 应用安全需求	2.1.1 了解5G应用安全现状 2.1.2 理解5G应用安全需求 2.1.3 理解5G应用安全目标	2.1.1 5G应用安全含义及现状 2.1.2 5G应用多种接入类型，开放架构等对安全的需求 2.1.3 5G应用安全的特点及目标
	2.2 5G 应用安全挑战	2.2.1 了解5G应用对安全挑战 2.2.2 理解5G演进对应用安全的驱动 2.2.3 理解垂直行业应用发展、工业互联网安全挑战，行业标准挑战	2.2.1 5G应用面临的安全风险及挑战 2.2.2 5G演进方向，对应用安全的驱动 2.2.3 垂直行业应用对5G网络安全的挑战，工业互联网的挑战，统一行业安全标准的挑战
3. 5G 应用安全基础	3.1 5G 应用端管云架构	3.1.1 理解5G应用类型 3.1.2 掌握5G端管云应用架构 3.1.3 掌握5G应用方案设计要点及	3.1.1 5G应用类型 3.1.2 5G端管云架构 3.1.3 5G应用方案设计要点
	3.2 5G 应用安全威胁及措施	3.2.1 理解5G相比4G应用的安全能力增强 3.2.2 清楚5G应用面临的安全威胁及应对措施 3.2.3 掌握5G网络安全总体视图及功能特性 3.2.4 掌握5G应用安全知识库基础和查阅	3.2.1 5G相比4G应用的安全能力增强 3.2.2 5G应用面临的安全威胁及应对措施 3.2.3 5G网络安全总体视图及功能特性 3.2.4 5G应用安全知识库基础

3.2 中级

课程模块	培训内容	专业能力要求	相关知识要求
1. 5G 应用安全分级	1.1 5G 行业应用安全分级	1.1.1 能理解应用安全需求分级 1.1.2 能理解 5G 应用安全分级目标 1.1.3 能理解 5G 应用安全能力分级映射	1.1.1 应用的基础安全需求和高级安全需求 1.1.2 等保 2.0 和行业应用安全分级 1.1.3 安全能力分级映射，安全分级策略
	1.2 5G 行业应用安全分级分级能力映射	1.2.1 能理解 5G 应用安全模型 1.2.2 能理解 5G 应用安全域安全 1.2.3 能理解 5G 应用安全域能力集 1.2.4 掌握根据 5G 应用安全分级使用 5G 应用安全知识库	1.2.1 5G 应用安全模型，生命周期安全 1.2.2 5G 应用安全域终端安全、网络安全、平台（DC）安全 1.2.3 5G 应用安全域能力集，行业安全需求和 5G 安全能力的映射 1.2.4 5G 应用安全分级和 5G 应用安全知识库的对应。
2. 5G 应用安全场景	2.1 eMBB 场景安全	2.1.1 能了解 eMBB 场景安全威胁概述 2.1.2 能进行典型 eMBB 场景安全风险分析 2.1.3 能对 eMBB 场景安全风险进行应对	2.1.1 eMBB 场景安全威胁概述 2.1.2 典型 eMBB 场景安全风险分析 2.1.3 eMBB 场景安全风险应对
	2.2 uRLLC 场景安全	2.2.1 能理解 uRLLC 场景安全威胁概述 2.2.2 能进行典型 uRLLC 场景应用安全风险分析 2.2.3 能对 uRLLC 场景安全风险进行应对	2.2.1 uRLLC 场景安全威胁概述 2.2.2 典型 uRLLC 场景应用安全风险分析 2.2.3 uRLLC 场景安全风险应对
	2.3 mMTC 场景安全	2.3.1 能了解 mMTC 场景安全威胁概述 2.3.2 能对典型 mMTC 场景应用安全风险分析 2.3.3 能对 mMTC 场景安全风险进行应对	2.3.1 mMTC 场景安全威胁概述 2.3.2 典型 mMTC 场景应用安全风险分析 2.3.3 mMTC 场景安全风险应对
3. 5G 应用安全的关键技术	3.1 应用安全增强技术	3.1.1 能理解服务化安全增强技术 3.1.2 能理解智能化安全增强技术 3.1.3 能理解应用专网安全增强技术 3.1.4 能理解可信计算技术 3.1.5 能理解量子安全技术	3.1.1 服务化安全增强技术关键点 3.1.2 智能化安全增强技术关键点 3.1.3 应用专网安全增强技术关键点 3.1.4 可信计算技术关键点 3.1.5 量子安全技术关键点
	3.2 应用可信接入技术	3.2.1 能理解应用数据安全和隐私保护技术 3.2.2 能理解零信任访问控制技术 3.2.3 能理解基于区块链的身份管理技术	3.2.1 应用数据安全和隐私保护技术关键点 3.2.2 零信任访问控制技术关键点 3.2.3 基于区块链的身份管理技术关键点

3.3 高级

课程模块	培训内容	专业能力要求	相关知识要求
1. 5G 应用安全性和策略	1.1 不同视角下的 5G 应用安全特性	1.1.1 理解攻防视角下的 5G 应用安全 1.1.2 理解应用视角下的 5G 架构安全	1.1.1 5G 应用的攻防特点和攻击手段 1.1.2 引入虚拟化、网络切片、边缘计算等新技术对 5G 应用安全影响
	1.2 5G 应用安全策略	1.2.1 理解 5G 应用更好的机密性 1.2.2 理解 5G 应用更好的完整性 1.2.3 理解 5G 应用更好的隐私保护 1.2.4 理解 5G 应用更好的认证类型	1.2.1 5G 应用的机密性 1.2.2 5G 应用的完整性 1.2.3 5G 应用的隐私保护 1.2.4 5G 应用的认证类型
2. 基于切片的 5G 应用安全	2.1 基于切片的第三方应用安全	2.1.1 掌握基于 5G 切片的应用解决方案 2.1.2 掌握基于 5G 切片的应用安全技术	2.1.1 5G 切片架构、切片是 5G 垂直行业应用的主要特征 2.1.2 5G 切片的应用安全技术要求
	2.2 面向应用 5G 切片安全定制	2.2.1 掌握 5G 应用端到端切片隔离方案 2.2.2 理解 5G 应用切片安全定制方案	2.2.1 5G 应用端到端切片隔离方案：不同应用对 RAN 隔离、承载隔离、5GC 隔离的选择 2.2.2 5G 应用切片共享资源方案、安全定制方案
3. 基于边缘计算的应用安全	3.1 边缘计算的应用安全防护	3.1.1 理解边缘计算应用方案架构 3.1.2 掌握边缘计算应用方案的安全防护	3.1.1 边缘计算应用方案架构 3.1.2 边缘计算应用方案的安全防护要点
	3.2 面向应用的安全开放能力	3.2.1 理解边缘计算的安全能力开放模型 3.2.2 理解智能网络防御和可信数字身份	3.2.1 边缘计算的安全能力开放模型 3.2.2 智能网络防御和可信数字身份

4 考核权重表

4.1 理论知识权重表

课程模块		级别		
		初级 (%)	中级 (%)	高级 (%)
基本要求	职业道德	10	10	10
	基础知识	20	20	20
理论知识要求	5G 应用技术基础	20	5	2
	5G 应用安全需求和挑战	25	5	2
	5G 应用安全基础	25	5	2
	5G 应用安全分级	-	20	4
	5G 应用分场景安全	-	15	5
	5G 应用安全的关键技术	-	20	5
	5G 应用安全特性和策略	-	-	15
	基于 5G 切片的应用安全	-	-	15
	基于边缘计算的应用安全	-	-	20
合计		100	100	100

4.2 实操能力权重表

课程模块		级别		
		初级 (%)	中级 (%)	高级 (%)
实操能力要求	5G 应用架构设计	50	50	20
	5G 应用安全知识库使用	50	50	20
	基于切片的 5G 应用安全方案设计	-	-	30
	基于边缘计算的 5G 应用安全方案设计	-	-	30
合计		100	100	100