物联网安全测评
职业技能等级标准

（2021年1.0版）

工业和信息化部电子第五研究所 制定

2021 年 4 月　发布

目　　次

前　　言

本标准按照GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

本标准起草单位：工业和信息化部电子第五研究所、广州市宏升教育科技有限公司。

本标准主要起草人：李倩、罗衡峰、李乐言、李琳、黄宏燨。

1 范围

本标准规定了物联网安全测评职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于物联网安全测评职业技能培训、考核与评价，相关用人单位的聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本适用于本文件。

GB/T 36951-2018 信息安全技术 物联网感知终端应用安全技术要求

GB/T 37024-2018 信息安全技术 物联网感知层网关安全技术要求

GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求

GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求

GB/T 37093-2018 信息安全技术 物联网感知层接入通信网的安全要求

3 术语和定义

物联网安全测评界定的以及下列术语和定义适用于本标准。

3.1 物联网 Internet of Things

物联网，“万物相连的互联网”，是互联网基础上的延伸和扩展的网络，将各种信息传感设备与互联网结合起来而形成的一个巨大网络，实现在任何时间、任何地点，人、机、物的互联互通。

3.2 整体感知 Overall Perception

可以利用射频识别、二维码、智能传感器等感知设备感知获取物体的各类信息。

3.3 可靠传输 Reliable Transmission

通过对互联网、无线网络的融合，将物体的信息实时、准确地传送，以便信息交流、分享。

3.4 智能处理 Intelligent Processing

使用各种智能技术，对感知和传送到的数据、信息进行分析处理，实现监测与控制的智能化。

3.5 射频识别技术 Radio Frequency Identification, RFID

射频识别技术（RFID）是一种简单的无线系统，由一个询问器（或阅读器）和很多应答器（或标签）组成。标签由耦合元件及芯片组成，每个标签具有扩展词条唯一的电子编码，附着在物体上标识目标对象，它通过天线将射频信息传递给阅读器，阅读器就是读取信息的设备。

3.6 微机电系统 Micro-Electro-Mechanical Systems

MEMS 是微机电系统，它是由微传感器、微执行器、信号处理和控制电路、通讯接口和电源等部件组成的一体化的微型器件系统。其目标是把信息的获取、处理和执行集成在一起，组成具有多功能的微型系统，集成于大尺寸系统中，从而大幅度地提高系统的自动化、智能化和可靠性水平。

3.7 机器终端智能交互 Machine-to-Machine/Man, M2M

机器终端智能交互（M2M）它是一种以机器终端智能交互为核心的、网络化的应用与服务。它将使对象实现智能化的控制。M2M 技术涉及 5 个重要的技术部分：机器、M2M 硬件、通信网络、中间件、应用。

4 适用院校专业

中等职业学校：计算机网络技术、络安防系统安装与维护、计算机与数码产

品维修、电子技术应用、通信系统工程安装与维护、物联网技术应用、网络信息安全等专业。

高等职业学校：工业网络技术、电子信息工程技术、应用电子技术、智能产品开发、智能终端技术与应用、电子产品质量测评、移动互联应用技术、物联网应用技术、软件技术、信息安全与管理、移动应用开发、人工智能技术服务

应用型本科学校：计算机科学与技术、软件工程、网络工程、信息安全、物联网工程

5 面向职业岗位（群）

【物联网安全测评】（初级）主要面向企事业单位、政府部门等的物联网系统安全测评等职业岗位，主要完成物联网单元安全测评、物联网整体安全测评、物联网系统风险分析等工作。

【物联网安全测评】（中级）要面向企事业单位、政府部门等的物联网系统安全测试等职业岗位，主要完成白盒渗透测试、黑盒渗透测试、灰盒渗透测试等工作。

【物联网安全测评】（高级）主要面向企事业单位、政府部门等的物联网产品安全测评等职业岗位，主要完成物联网产品标签安全测评、物联网通信链路安全测评、物联网产品传统芯片安全测评等工作。

6 职业技能要求

6.1 职业技能等级划分

物联网安全测评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。

【物联网安全测评】（初级）：主要面向企事业单位、政府部门等的物联网部门，从事物联网系统安全测评，主要包括物联网单元安全测评、物联网整体安全测评、物联网系统风险分析等。

【物联网安全测评】（中级）：主要面向企事业单位、政府部门等的物联网部门，从事物联网系统安全渗透测试，主要包括白盒测试、黑盒测试、灰盒测试等。

【物联网安全测评】（高级）：主要面向企事业单位、政府部门等的物联网

部门，从事物联网产品安全测评工作，主要包括物联网产品标签安全测评、物联网通信链路安全测评、物联网产品传统芯片安全测评等。

6.2 职业技能等级要求描述

表 1　物联网安全测评职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1 物联网系统单元安全测评	1.1 物理安全测评	1.1.1 检查主机房，测评主机房所在的位置是否具有防震、防风和防雨等多方面的安全防护能力。 1.1.2. 检查主机房出入口、机房分区情况，测评物理访问控制方面的安全防护能实施的能力。 1.1.3 检查主机房的主要设备、介质和防盗设施，测评物联网信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 1.1.4 检查主机房的设计/验收文档，测评物联网信息系统是否采取相应的措施预防雷击。 1.1.5 检查主机房的防水除潮设施，测评物联网信息系统是否采取必要的措施防水和防潮湿。 1.1.6 检查主机房的设计/验收文档，测评物联网通过访谈物理安全负责人，检查主机房的设计/验收文档，测评物联网信息系统是否采取必要的温湿度控制措施。信息系统是否采取必要的措施防止静电。 1.1.7 检查主机房的设计/验收文档，测评物联网信息系统是否采取必要的温湿度控制措施。 1.1.8 检查主机房供电线路、设备，测评物联网信息系统是否具备提供一定的电力供应的能力。 1.1.9 检查平米机房，测评物联网信息系统是否具备一定的电磁防护能力。
	1.2 网络安全测评	1.2.1 检查网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络带宽分配情况等，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 1.2.2 检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等，测评分析物联网信息系统对网络区域边界相关的网络隔离与访问控制能力。 1.2.3 检查核心交换机和接入交换机等网络互联设备的安全审计情况等，测评分析物联网信息系统审计配置和审计记录保护情况。 1.2.4 检查边界完整性检查设备，接入边界完整性检查设备进行测试等，测评分析系统私自连到外部网络的行为。 1.2.5 检查网络边界处的 IDS 等，测评分析物联网信息系统对攻击行为的识别和处理情况。

工作领域	工作任务	职业技能要求
		1.2.6 检查网络防恶意代码产品等，测评分析物联网信息系统网络边界和核心网段对病毒等恶意代码的防护情况。 1.2.7 检查核心交换机、接入交换机和接入路由器等网络互联设备，IDS 和防火墙等网络安全设备，查看其安全配置情况，包括身份鉴别、权限分离、登录失败处理、限制非法登录和登录连接超时等，考察网络设备自身的安全防范情况。
	1.3 主机安全测评	1.3.1 检查服务器、终端计算机的操作系统、数据库系统的身份标识与鉴别机制等，测评主机系统的身份鉴别机制的合理性。 1.3.2 检查操作系统和数据库系统的安全策略、不同的帐户及其权限分配情况等，测评分析主机系统的访问控制能力。 1.3.3 能通过访谈审计员，检查操作系统、数据库系统的安全审计情况等，测评分析主机系统审计配置和审计记录保护情况。 1.3.4 检查操作系统的缓存设置等，测评分析系统的剩余信息保护的能力。 1.3.5 检查主机系统的入侵防范设置等，测评分析主机系统入侵防范能力。 1.3.6 检查主机防恶意代码产品等，测评分析主机系统对病毒等恶意代码的防护情况。 1.3.7 检查主机系统的资源监控、接入方式等设置，测评主机系统对资源控制的情况。
	1.4 应用安全测评	1.4.1 检查应用的身份标识与鉴别机制等，测试身份鉴别机制的有效性，测评应用系统的身份鉴别情况。 1.4.2 检查应用系统的访问控制列表等，测试应用系统的访问控制功能，测评分析应用系统的访问控制能力。 1.4.3 检查应用系统的安全审计情况等，测评分析应用系统审计配置和审计记录保护情况。 1.4.4 检查应用系统的设计文档等，测评分析系统的剩余信息保护的能力。 1.4.5 检查应用系统的设计文档、分析应用系统通信数据包等，测评分析应用系统通信完整性保护能力。 1.4.6 检查应用系统的设计文档、分析应用系统通信数据包等，测评分析应用系统通信保密性保护能力。 1.4.7 检查应用系统的设计文档等，测评分析应用系统通信的抗抵赖能力。 1.4.8 检查应用系统的设计文档等，对应用系统进行容错性测试，测评分析应用系统通信的容错能力。 1.4.9 能通过检查应用系统的资源监控设置，测评应用系统对资源控制的情况。

工作领域	工作任务	职业技能要求
	1.5 数据安全测评	1.5.1 检查鉴别信息、用户数据在传输过程和存储过程的完整性保护措施，检查设计/验收文档，查看是否有相应的功能，通过网络抓包等手段进行验证。 1.5.2 检查鉴别信息、用户数据在传输过程和存储过程的保密性，检查设计/验收文档，查看是否有相应的功能，通过网络抓包等手段进行验证。 1.5.3 检查系统数据备份、恢复功能，检查网络冗余设备及系统备份设备的运行情况。
	1.6 安全管理制度测评	1.6.1 检查安全管理制度、安全总体方针、安全策略等相关文档，测评被测单位安全管理制度的总体情况。 1.6.2 检查安全管理制度的制定、发布流程规定以及相关的记录，测评被测单位安全管理制度的制定、发布情况。 1.6.3 检查安全管理制度的评审、修订流程规定以及相关的记录，测评被测单位安全管理制度的评审、修订情况。
	1.7 安全管理机构测评	1.7.1 检查岗位设置等相关文档，测评被测单位岗位设置的情况。 1.7.2 检查岗位的人员设置情况，测评被测单位人员配备情况。 1.7.3 检查被测单位的审批流程规定以及相关的记录，测评被测单位的授权和审批情况。 1.7.4 检查被测单位与其他单位就信息安全方面的沟通和合作机制以及相关的记录，测评被测单位的沟通和合作情况。 1.7.5 检查被测单位关于信息安全方面的审核和检查机制以及相关的记录，测评被测单位的审核和检查情况。
	1.8 人员安全管理测评	1.8.1 检查人员录用制度和相关的记录文档，测评被测单位人员录用的情况。 1.8.2 检查人员离岗制度和相关的记录文档，测评被测单位人员离岗的情况。 1.8.3 检查人员考核制度和相关的记录文档，测评被测单位人员考核的情况。 1.8.4 检查外部人员访问管理制度和相关的记录文档，测评被测单位人员访问管理的情况。
	1.9 系统统建设管理测评	1.9.1 检查系统定级报告，测评被测单位的系统定级情况。 1.9.2 检查系统的安全设计方案，测评系统在设计阶段是否充分考虑到安全设计。 1.9.3 检查产品采购和使用的制度和相关文档，测评被测单位产品采购和使用的情况。 1.9.4 检查软件开发环境以及相关的制度、设计文档

工作领域	工作任务	职业技能要求
		等，测评被测单位自行软件开发的情况。 1.9.5 检查外包软件开发的相关制度、设计文档等，测评被测单位外包软件开发的情况。 1.9.6 检查工程实施过程的记录文档，测评被测单位工程实施的情况。 1.9.7 检查系统测试报告、验收报告等相关文档，测评被测单位系统验收的情况。 1.9.8 检查系统交付流程规定及相关的记录文档，测评被测单位系统交付的情况。 1.9.9 检查系统备案证明及相关备案材料，测评被测单位系统备案的情况。 1.9.10 检查系统等级测评报告，测评被测单位等级测评实施的情况。 1.9.11 检查被测单位与安全服务商的合同等文件，测评被测单位的安全服务商选择情况。
	1.10 系统运维管理测评	1.10.1 检查机房、办公环境的管理制度以及相关的记录文档，测评被测单位的环境管理情况。 1.10.2 检查物联网信息系统相关资产的管理制度以及相关的记录文档，测评被测单位的资产管理情况。 1.10.3 检查存储介质的管理制度以及相关的记录文档，测评被测单位的介质管理情况。 1.10.4 检查设备的管理制度以及相关的记录文档，测评被测单位的设备情况。 1.10.5 检查对网络运行情况，测评被测单位的设备情况。 1.10.6 检查网络安全管理制度以及制度的实行情况，测评被测单位网络安全管理的情况。 1.10.7 检查系统防范恶意代码的管理制度及其落实情况，测评被测单位恶意代码防范管理的情况。 1.10.8 检查系统密码管理制度及其落实情况，测评被测单位密码管理的情况。 1.10.9 检查系统变更管理制度及其落实情况，测评被测单位变更管理的情况。 1.10.10 检查系统备份与恢复管理制度及其落实情况，测评被测单位备份与恢复管理的情况。 1.10.11 检查安全事件处置流程和相关的记录文档，测评被测单位安全事件处置的情况。 1.10.12 检查应急预案流程和相关的记录文档，测评被测单位应急处理的情况。
2 物联网系统整体测评	2.1 安全控制间安全测评	2.1.1 单元安全测评完成后，测评项中存在不符合或部分符合的，能进行控制间安全测评。 2.1.2 分析统一功能区域同一层面内，能判断是否存在其他测评项对该测评项具有补充作用。

工作领域	工作任务	职业技能要求
		2.1.3 能分析是否存在其他安全措施或技术与该要求具有相似的安全功能。 2.1.4 经过综合分析，单元安全测评中的不符合或部分符合项不造成系统整体安全保护能力的缺失，能判断该测评项结论为符合。
	2.2 层面间安全测评	2.2.1 单元安全测评完成后，测评项中存在不符合或部分符合的，能进行层面间安全测评。 2.2.2 能分析其他层面上功能相同或相似的测评项是都对该测评项存在补充作用。 2.2.3 能分析技术与管理上各层面的关联关系。 2.2.4 经过综合分析，单元安全测评中的不符合或部分符合项不造成系统整体安全保护能力的缺失，能判断该测评项结论为符合。
	2.3 区域间安全测评	2.3.1 单元安全测评完成后，测评项中存在不符合或部分符合的，能进行区域间安全测评。 2.3.2 能分析系统中访问控制路径（如不同功能区域间的数据流流向和控制方式）是否存在区域间安全功能的相互补充。 2.3.3 经过综合分析，单元安全测评中的不符合或部分符合项不造成系统整体安全保护能力的缺失，能判断该测评项结论为符合。
	2.4 系统结构安全测评	2.4.1 通过物理安全测评 ，能分析物联网系统的物理布局安全。 2.4.2 通过网络安全测评 ，能分析物联网系统的网络结构安全。 2.4.3 通过应用安全测评 ，能分析物联网系统的业务逻辑安全。
3 物联网系统风险分析	3.1 物联网系统安全保护能力分析	3.1.1 能对单元安全测评每个测评项进行打分。 3.1.2 能根据计算公式和单元安全测评情况，对安全层面进行打分。 3.1.3 能判断安全层面得分是否符合安全需求。
	3.2 物联网系统业务安全和系统服务安全造成的影响程度分析	3.2.1 能对整体测评之后单元安全测评结果中的不符合或部分项进行风险分析和等级确定。 3.2.2 能分析不符合项或部分符合项所产生的安全问题被威胁利用的可能性。 3.2.3 能分析不符合项或部分符合项的威胁对系统业务安全和系统服务安全造成的影响程度。
	3.3 物联网系统面临风险汇总和等级确定	3.3.1 能对整体测评之后单元安全测评结果中的不符合或部分项进行风险分析和等级确定。 3.3.2 能分析不符合项或部分符合项所产生的安全问题被威胁利用的可能性。 3.3.3 能汇总和统计所有风险的情况。

工作领域	工作任务	职业技能要求
	3.4 物联网系统风险结果分析	3.4.1 能对整体测评之后单元安全测评结果中的不符合或部分项进行风险分析和等级确定。 3.4.2 能分析不符合项或部分符合项所受到的关联威胁。 3.4.3 能分析不符合项或部分符合项的危害结果。

表 2　物联网安全测评职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1 物联网系统安全渗透白盒测试	1.1 测试准备	1.1.1 能根据任务要求对测试内容进行调研。 1.1.2 能根据任务要求确定测试人员的分配。 1.1.3 能根据任务要求确定测试周期。 1.1.4 能根据任务要求编写测试方案。
	1.2 测试实施	1.2.1 能根据任务要求和方案完成白盒测试。 1.2.2 能根据任务要求和方案保存测试记录。 1.2.3 能根据任务要求和方案保证测试完整。
	1.3 结果分析	1.3.1 能使用单元测试的测试方法对测试结果进行分析。 1.3.2 能使用技术评审的测试方法对测试结果进行分析。 1.3.3 能编写测试报告。
2 物联网系统安全渗透黑盒测试	2.1 测试准备	2.1.1 能根据任务要求对测试内容进行调研。 2.1.2 能根据任务要求确定测试人员的分配。 2.1.3 能根据任务要求确定测试周期。 2.1.4 能根据任务要求编写测试方案。
	2.2 测试实施	2.2.1 能根据任务要求和方案完成黑盒测试。 2.2.2 能根据任务要求和方案保存测试记录。 2.2.3 能根据任务要求和方案保证测试完整。
	2.3 结果分析	2.3.1 能使用因果图法对测试结果进行分析。 2.3.2 能使用场景法对测试结果进行分析。 2.3.3 能编写测试报告。
3 物联网系统安全渗透灰盒测试	3.1 测试准备	3.1.1 能根据任务要求对测试内容进行调研。 3.1.2 能根据任务要求确定测试人员的分配。 3.1.3 能根据任务要求确定测试周期。 3.1.4 能根据任务要求编写测试方案。
	3.2 测试实施	3.2.1 能根据任务要求和方案完成灰盒测试。 3.2.2 能根据任务要求和方案保存测试记录。 3.2.3 能根据任务要求和方案保证测试完整。

工作领域	工作任务	职业技能要求
	3.3 结果分析	3.3.1 能使用单元测试的测试方法对测试结果进行分析。3.3.2 能使用技术评审的测试方法对测试结果进行分析。 3.3.3 能使用因果图法对测试结果进行分析。 3.3.4 能使用场景法对测试结果进行分析。 3.3.5 能编写测试报告。

表 3　物联网安全测评职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.物联网产品标签安全测评	1.1 标签容量测评	1.1.1 测出标签 reserved 区的容量。 1.1.2 测出标签 epc 区的容量。 1.1.3 测出标签 tid 区的容量。 1.1.4 测出标签 user 区的容量。
	1.2 标签性测试	1.2.1 测试标签激活电场强度。 1.2.2 测试标签激活灵敏度。 1.2.3 测试标签反向散射功率。 1.2.4 测试标签中心频率。
	1.3 标签读写功测评	1.3.1 测试标签静态识别距离。 1.3.2 测试标签前向识读距离。 1.3.3 测试标签写入距离。
2.物联网通信链路安全测评	2.1 标签射频一致性测试	2.1.1 测试标签解调。 2.1.2 测试标签工作频率。 2.1.3 测试标签数据编码。 2.1.4 测试标签前导码。 2.1.5 测试标签频率允差。 2.1.6 测试标签链接时序 T1。 2.1.7 测试标签链接时序 T2。 2.1.8 测试标签状态机。 2.1.9 进行标签命令测试。 2.1.10 测试标签防碰撞。
	2.2 标签协议一致性测试	2.2.1 测试标签发射频谱密度模板。 2.2.2 测试标签信道占用带宽。 2.2.3 测试标签发收转换时间。 2.2.4 测试标签调制准确度。 2.2.5 测试标签扩频序列。 2.2.6 测试标签码片速率。 2.2.7 测试标签位速率。 2.2.8 测试标签前导码、同步码和校验码。 2.2.9 测试标签帧选项。 2.2.10 测试标签位传输顺序。

工作领域	工作任务	职业技能要求
		2.2.11 测试标签发起方。 2.2.12 测试标签寻址方式。 2.2.13 测试标签 TID。 2.2.14 测试标签存储区结构。 2.2.15 测试标签状态转移。 2.2.16 测试标签防碰撞。 2.2.17 测试标签安全协议。
	2.3 读写器射频一致性测试	2.3.1 测试读写器调制方式和工作频率。 2.3.2 测试读写器打开和关闭载波时的射频信号包络。 2.3.3 测试读写器到标签的射频信号包络。 2.3.4 测试读写器数据编码。 2.3.5 测试读写器前导码。 2.3.6 测试读写器解调。 2.3.7 测试读写器链接时序 T2。 2.3.8 测试读写器链接时序 T3。 2.3.9 测试读写器链接时序 T4。 2.3.10 测试读写器命令。 2.3.11 测试读写器多标签防碰撞处理。
	2.4 读写器协议一致性测试	2.4.1 测试读写器发射频谱密度模板。 2.4.2 测试读写器信道占用带宽。 2.4.3 测试读写器发收转换时间。 2.4.4 测试读写-调制准确度。 2.4.5 测试读写器扩频序列。 2.4.6 测试读写器码片速率。 2.4.7 测试读写器位速率。 2.4.8 测试读写器前导码、同步码和检验码。 2.4.9 测试读写器帧选项。 2.4.10 测试读写器位传输顺序。 2.4.11 测试读写器命令。 2.4.12 测试读写器防碰撞算法。 2.4.13 测试读写器安全协议。
3. 物联网产品传统芯片安全测评	3.1 电学测评	3.1.1 判断电路是否存在安全隐患。 3.1.2 判断电路哪部分存在安全隐患。 3.1.3 判断其电流输运和信号传递路径的方法。
	3.2 软硬件协同测评	3.2.1 对电路的各个功能模块进行测试。 3.2.2 分析其中的控制数据流向、信号传递的模块。 3.2.3 分辨电路控制指令的功能，确定各个阶段电路的工作状态。
	3.3 物理测评	3.3.1 能检测提取相应的电路结构。 3.3.2 能分析判断其中超过功能要求的部分。

工作领域	工作任务	职业技能要求
		3.3.3 确定是否存在后门电路和冗余电路等安全隐患。
4. 物联网整体安全设计与测评	4.1 测评设计	能对一个物联网系统的整体安全设计出测评指标，提出测试方法，提出整体测评方案。
	4.2 安全方案设计	能对一个物联网系统的安全提出整体的安全解决方案，提供设计方案并实施。

参考文献

[1] GB/T1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则

[2] GB/T 33474-2016 《物联网参考体系结构》

[3] GB/T 36468-2018 《物联网系统评价指标体系编制通则》

[4] GB/T 36478《物联网信息交换和共享》

[5] 刘云浩，物联网导论[M].北京：科学出版社，2010

[6] 朱方洲，基于 BS7799 的信息系统安全风险评估研究[D].合肥工业大学

[7] 翟根红、王异轩、谢关友等，对我国建立 RFID 标准体系的几点思考[J].[4]物流技术，2008

[8] （德）Klaus Finkenzell 著，陈大才编译，射频识别(RFID)技术——无线[4]电感应的应答器和非接触 IC 卡的原理（第 2 版）[M].北京：电子工业出版社，2001

[9] 石蕾、陈敏雅，RFID 系统中阅读器的设计与实现[J].电脑开发与应用，2008，（07）

[10] 王爱玲、盛小宝、司军，讨论我军 RFID 标准体系的构建[J] .物流科技，2007

[11] 纪亚萍，基于 Wi-FiSoC 的物联网平台设计[D].兰州大学，2015

[12] 王怡、鄂旭，基于物联网无线传感的智能家居研究[J].计算机技术与发展，2015，25（02）：234-237.（2014-12-27）[2017-08-31]

[13] 武传坤，物联网安全关键技术与挑战[J].密码学报，2015，2（01）：40-53.[2017-08-31].DOI:10.13868/j.cnki.jcr.000059

[14] 沈苏彬、杨震，物联网体系结构及其标准化[J].南京邮电大学学报

[15] 赵巧，基于物联网的农作物试验基地监控管理系统设计[J].农机化研究，2019，41（1）：222-225

[16] 张曼君、马铮、高枫、张小梅，物联网安全技术架构及应用研究[J].信息技术与网络安全，2019，38（02）：4-7

[17] 桑圣洁，物联网安全架构浅析[J].信息系统工程，2018，（01）：73

[18] 高冲，物联网安全架构与技术路线[J].信息与电脑（理论版），2017，（15）：149-151

[19] 中商产业研究院，2019 年中国工业物联网市场前景研究报告[J].电器工业，2019（10）：42-44

[20] 中等职业院校专业目录

[21] 普通高等学校高等职业教育（专科）专业目录

[22] 普通高等学校本科专业目录