国家标准《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》（征求意见稿）编制说明

一、工作简况

1、任务来源

2022 年 4 月 28 日，国家标准化管理委员会发布了《国家标准化管理委员会关于下达 2022 年第一批推荐性国家标准计划及相关标准外文版计划的通知》（国标委发〔2022〕17 号），正式下达了 2022 年第一批推荐性国家标准计划项目，将《信息安全技术 射频识别（RFID）系统安全技术要求及测试评价方法》（计划编号：20220170-T-469）纳入本批标准制修订计划。

2、起草单位情况

该标准由全国信息安全标准化技术委员会（SAC/TC260）归口，公安部第三研究所作为主要承办单位。

中国电子技术标准化研究院、北京中科国技信息系统有限公司、腾讯云计算（北京）有限责任公司、珠海复旦创新研究院、上海化工院检测有限公司、长扬科技（北京）有限公司、西安交大捷普网络科技有限公司、郑州信大捷安信息技术股份有限公司、上海伊世智能科技有限公司、上海临港电力电子研究有限公司、中国汽车工程研究院股份有限公司、中国网络安全审查技术与认证中心、广东技安科技有限公司、浙江工业大学作为标准编制协作单位。

3、主要起草人及其所做的工作

《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》的主要起草人是刘彩霞、顾健、谢芳艺、张艳、刘丹丹、焦志皓、李琳、李哲、戴杰、李建慧、刘海涛、王俊宇、王思怿、赵华、何建锋、刘为华、刘虹、刘宇澄、刘冲、申永波、何红亮、顾国民。

其中，刘彩霞全面负责标准编制工作，包括制定工作计划、确定编制内容提纲、调控整体进度、安排参编人员的任务及各阶段文稿的撰写与修改、意见汇总处理、编制说明的编写；顾健主要负责标准编制过程中的各项技术支持和整体指导；谢芳艺、张艳主要负责标准的前期调研、标准校对、标准试验验证，刘丹丹

主要负责标准各版本的征求意见汇总处理、参与标准各版本的编制、标准编制说明的撰写及标准试验验证；焦志皓主要参与标准各版本的征求意见汇总处理及标准试验验证；王俊宇负责标准中涉及国密算法的标准收集与分析；李琳、李哲、戴杰、李建慧、刘海涛、王思怿、赵华、焦志皓、何建锋、刘为华、刘虹、刘宇澄、刘冲、申永波、何红亮、顾国民等参与标准会议讨论，提供技术要求与测试评价方法意见等。

4、主要工作过程

GB/T 35290-2017《信息安全技术 射频识别（RFID）系统通用安全技术要求》于2017年12月29日正式发布、2018年7月01日实施后，为保障GB/T 35290-2017的实施效果，尽快建立针对读写器、标签、通信链路、后端系统的RFID系统通用性安全评估体系，《信息安全技术 射频识别系统通用安全技术要求》原国家标准编制组立即围绕射频识别（RFID）系统安全功能评价，开展了测试设备调研工作、测试评价方法研究及检验试验方法验证工作，于2018年12月起草完成了《信息安全技术 射频识别（RFID）系统安全测试规范》国家标准草案并向TC260标委会WG5工作组提出了《信息安全技术 射频识别（RFID）系统安全测试规范》国家标准立项申请。专家评审建议该规范与原有安全技术要求标准合并，对GB/T 35290-2017标准进行修订并在修订版中增加测试方法相关内容。

2021年5月，《信息安全技术 射频识别（RFID）系统通用安全技术要求及测试评价方法》国家标准修订立项申请通过立项评审。2021年8月25日，全国信息安全标准化技术委员会发布了《全国信息安全标准化技术委员会关于 2021年网络安全标准项目立项的通知》（信安字[2021]14号），将《信息安全技术 射频识别（RFID）系统安全技术要求及测试评价方法》（计划编号：2021-16）纳入本批标准修订预研计划。随后，公安部第三研究所成立了该项国家标准编制组。标准编制组由刘彩霞、顾健、张艳、谢芳艺、刘丹丹、焦志皓等具有RFID系统检测经验、RFID 系统安全检测经验以及标准编制经验的科研人员共同组成。为确保完成后的标准贴近RFID系统安全实际需求及国内现有RFID系统安全研发、生产水平，标准编制组通过本单位微信公众号面向全国广泛征集标准参与起草单位，并通过全国信息安全标准化技术委员会（SAC/TC260）面向会员单位广泛征集标准参与起草单位，吸纳了中国电子技术标准化研究院、北京中科国技信息系

统有限公司、腾讯云计算（北京）有限责任公司、珠海复旦创新研究院、上海化工院检测有限公司、长扬科技（北京）有限公司、西安交大捷普网络科技有限公司、郑州信大捷安信息技术股份有限公司、上海伊世智能科技有限公司、上海临港电力电子研究有限公司、中国汽车工程研究院股份有限公司、中国网络安全审查技术与认证中心、广东技安科技有限公司、浙江工业大学等国内相关技术领域用户单位、研发企事业单位及科研院所的部分研发负责人及主要研发人员参与标准的调研与内容研讨。

之后，标准起草组多次组织召开起草组工作会议、参加全国信息安全标准化技术委员会秘书处 WG5 工作组召开的国家标准起草进展推进评审会议、全国信息安全技术标委会工作组会议周及全国信息安全标准化技术委员会秘书处组织的国家标准研讨会议，结合各起草单位意见、会员单位意见及历次专家评审意见，参照 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中物联网安全扩展要求的不同安全保护能力对射频识别系统进行了安全分级，并反复修改完成了《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》（草案）。

《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》（草案）先后参加了参与全国信息安全标准化技术委员会秘书处 WG5 工作组和秘书处组织的专家评审，与会专家一致认为本标准文稿已比较成熟，对设计、开发、使用、测试和评估具备安全技术要求的射频识别系统整体及构成射频识别系统的各类射频识别电子标签、阅读器/读写器、通信链路及管理单元的安全功能具有指导意义，标准编写规范，基本符合 GB/T 1.1—2020 的规定，同意通过对该项标准的审查，建议编制工作组根据会议意见修改后发起公开征求意见。

2022 年 7 月 25 日，标准起草组按照 2022 年 3 月 01 日秘书处组织的专家审查会的全部专家审查意见及责任专家意见、责任编辑意见，修改完成《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》（征求意见稿）并提交至全国信息安全标准化技术委员会秘书处。

二、标准编制原则和确定主要内容的论据及解决的主要问题

1、标准编制原则

为了使本标准的内容从一开始就与现有国家标准保持一致，符合我国的实际情况，遵从我国有关法律、法规的规定。编制过程中遵循的具体原则与要求如下：

a）实用性

标准必须是可用的，才有实际意义。本标准在编写过程中严格按照流程对产品的现状、技术等相关领域展开系统的、全面的调研工作，注重与相关研发生产单位的交流，广泛了解了市场上主流RFID系统、RFID标签和RFID读写器的功能，进行提炼和扩展，使得标准更贴近产品实际情况，保证操作性。

b）先进性

标准是先进经验的总结，同时也是技术的发展趋势。目前，我国市场上RFID系统种类繁多，要制定出先进的产品标准，必须参考国内外先进技术和标准，吸收其精华，才能制定出具有先进水平的标准。本标准的编写始终遵循这一原则。

c）协调性

标准既要与国际接轨，更要与我国现有的政策、法规、标准、规范等相一致。编制组在对标准起草过程中始终遵循兼容性原则，其内容符合我国已经发布的有关政策、法律和法规。

d）前瞻性

制定标准要求前瞻性思维，要在保证标准适用性、先进性的前提下，引领技术发展方向。编制组在对标准起草过程中坚持前瞻性原则，致力于通过标准的前瞻性技术要求推动产品质量提升与技术进步。本标准在兼顾当前射频识别（RFID）系统安全技术现状的同时，积极关注相关领域科学研究方向、行业发展的技术趋势和实战需求，提出了多项前瞻性技术条款，积极引导射频识别（RFID）系统安全技术发展及相关行业发展。

e）兼容性

本标准既要与国际接轨，更要与我国现有的政策、法规、标准、规范等相一致。编制组在对标准起草过程中始终遵循此原则，其内容符合我国已经发布的有关政策、法律和法规。

2、标准编制思路

本标准按照以下编制思路开展编制工作：

a） 格式上依据 GB/T1.1-2020 进行编制；

b） 广泛征集射频识别产品研发生产企事业单位、检验检测机构及用户单位意见。

3、编制背景及目的意义

近年来，RFID技术作为物联网关键技术，已在车联网、爆炸危险化学品标识管理、机动车标识管理、公共安全管理、交通物流管理、图书馆管理、服装、零售、仓储管理、人员定位等领域大规模应用。实际应用中，RFID 安全问题一直是学术界和工业界关注的焦点之一。就RFID的典型应用结构体系而言，安全问题会出现在标签、阅读器/读写器、通信链路（空中接口）、通信链路（网络传输）、管理单元等各个环节。为此，公安部第三研究所牵头起草了适用于具有安全技术要求的RFID系统及其各类组件的设计、开发和使用的GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》推荐性国家标准。该标准已于2017年12月29日正式发布，2018年7月01日实施。

为保障GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》有效实施，有必要尽快建立针对标签、阅读器/读写器、通信链路、管理单元的RFID系统通用性安全评估体系，围绕射频识别（RFID）系统安全功能评价，明确测试设备，统一测试方法。否则，缺乏统一的测试方法进行检验检测判定射频识别系统的GB/T 35290-2017标准符合性，严重影响其实施效果。如不能尽快补足短板、加快相关测试评价方法制定，将会严重影响具备安全功能要求的RFID系统的技术进步、安全使用及规模化应用。因此，急需对GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》进行修订，增补与相关要求对应的测试评价方法。围绕射频识别系统安全问题，在保留原有安全功能要求的基础上，明确测试设备，统一测试评价方法，完善建立射频识别（RFID）系统安全评价体系。

修订GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》，形成GB/T 35290-202X《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》，规范射频识别系统的安全性技术要求及其测试方法，对客观评价射频识别系统的安全功能，从信息安全的角度加强该类射频识别系统的使用与管理十分必要。同时，本标准的制定，将为相关行业提供射频识别系统安全应用的技术依据，推动具备安全要求的射频识别系统在各类涉及国计民生的重要领域实

际应用，对提高车联网、爆炸危险化学品标识管理等多领域的射频识别系统安全性，切实保障涉及国计民生的重要信息数据安全具有重要意义。

4、标准主要修订内容及依据

1）增加测试环境要求

经过标准编制组研究决定，以 RFID 系统的信息安全技术为理论基础，以 GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》为基础研究，增加测试环境要求及测试评价方法要求，完成了《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》标准草案的编制工作。

测试环境要求中分别增加了一般要求（见 8.1）、测试环境（见 8.2）、测试条件（见 8.3）、通用测试设备（见 8.4），明确了以下检验测试的一般原则要求：

a） 测试过程中涉及 13.56MHz 频段射频识别系统的，空中接口协议默认按照 GB/T 22351-2015 的要求；

b） 测试过程中涉及 800/900MHz 频段射频识别系统的，空中接口协议默认按照 GB/T 29768-2013 的要求；

c） 测试过程中涉及 2.45GHz 频段射频识别系统的，空中接口协议默认按照 GB/T 28925-2012 的要求；

d） 测试前先确认进行安全符合性测试所需的指令和通信参数；

e） 符合国家密码相关规定的密码算法包括但不限于符合 GB/T 37033.1-2018、GB/T 37033.2-2018、GB/T 37033.3-2018 的射频识别系统密码；

f） 电子标签安全要求测试优先选择基准阅读器/读写器作为测试设备；

g） 阅读器/读写器安全要求测试优先选择基准电子标签作为测试设备；

h） 当 f）、g)项条件不具备时，采用射频信号发生器向被测电子标签或被测阅读器/读写器发射模拟基准阅读器/读写器或模拟基准电子标签射频信号，采用射频分析仪或频谱分析仪接收被测电子标签或被测阅读器/读写器发射的射频信号方式进行测试。

2）增加测试评价方法

本次修订主要在 GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》的基础上，增加测试环境要求及测试评价方法要求。

其中，测试评价方法要求分为电子标签安全测试评价、阅读器/读写器安全测试评价、通信链路（空中接口）安全测试评价、通信链路（网络传输）安全测试评价及管理单元测试评价五个部分，每个部分又分为基本级要求和增强级要求，测试方法分别对应每一项具体安全功能，分别描述了每项安全功能要求的测试方法、预期结果和结果判定。

3）修改射频识别系统描述

在GB/T 35290-2017《信息安全技术 射频识别系统通用安全技术要求》中，射频识别（RFID）系统由标签、读写器、后端系统、标签和读写器之间的空中接口通信链路、读写器和后端系统之间的网络传输通信链路等五个部分组成。因射频识别产业应用中仅具备读取功能的阅读器使用量越来越大，其相对同时具备写入功能的读写器而言，安全要求可以适当降低，因此，本次修订将“读写器”扩展为“阅读器/读写器”，并对阅读器和读写器提出了差异性安全功能要求。同时，鉴于有征求反馈意见提出，射频识别系统构成中的“后端系统”，导致同时出现了总分两个系统名称，可能引发歧义，建议修订。经反复调研查阅相关文献资料及在行业内开展调研，目前该部分定义多样，存在“应用系统”、“后端系统”、“应用高层”、“高层应用”、“管理系统”等多种名称，标准起草组最终选择按其功能用途，命名为“管理单元”。因此，在《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》征求意见稿第四稿中，修订为“射频识别系统是由电子标签、阅读器/读写器、通信链路及管理单元等四个部分组成的自动识别系统。”，并按照相关评审专家意见把射频识别系统描述从附录A调整入正文概述部分。

4）修改了射频识别、射频识别系统、电子标签、被动标签、半主动标签、阅读器、读写器等多个术语和定义的描述

考虑 GB/T 29261.3-2012 发布时间较久，尚未与近年来的行业发展和技术进步情况同步修订，相关术语定义与本标准关注的射频识别系统存在一定偏差，且其中多项术语定义与实际行业界定的概念认知存在一定出入。为使本标准使用者更好地理解应用本标准相关技术条款，标准起草组在研究GB/T 29261.3-2012并充分开展调研的基础上，对部分术语定义进行了修改并在本次修订中进行了增补和调整。

5）修改射频识别系统安全等级要求与网络安全等级保护要求的对应问题

在 GB/T 35290-2017《信息安全技术 射频识别（RFID）系统通用安全技术要求》中，提出基本级安全功能要求应具备 GB/T 22239-2019 中第二级安全保护能力，并应同时涵盖第一级安全保护能力；增强级安全功能要求应具备 GB/T 22239-2019 中第四级安全保护能力，并应同时涵盖第三级安全保护能力。鉴于射频识别（RFID）系统的当前安全技术实际状况和应用最为广泛的被动标签普遍存在存储空间有限、算力不足等现实问题，短时期达到 GB/T 22239-2019 中第二级安全保护能力或第四级安全保护能力比较困难，如提出过高安全功能要求，可能导致系统标签、阅读器/读写器等成本大幅增加，反而不利于产业发展，标准起草组经反复讨论，本着既兼顾我国 RFID 系统产品的技术现状，又具有一定的前瞻性和先进性，能够引领技术及产品发展的原则，按照 RFID 系统组成的结构特征，将 RFID 系统通用安全技术要求按标签安全、阅读器/读写器安全、通信链路（空中接口）安全、通信链路（网络传输）安全及管理单元安全共五个子类给出，每个子类分别划分为 2 个等级：基本级和增强级。RFID 系统应至少满足基本级安全技术要求。文件中增强级要求仅列出了除基本级技术要求外的增强级要求。增强级应在符合基本级安全技术要求的基础上满足增强级要求。基本级安全技术要求参照 GB/T 22239-2019 中安全通用要求和物联网安全扩展要求的第一级安全保护能力要求；增强级安全技术要求参照 GB/T 22239-2019 中安全通用要求和物联网安全扩展要求的第二级安全保护能力要求。

5）增加射频识别系统等级要求与射频识别系统密码应用技术要求国家标准提出的射频识别系统安全级别的对应关系

为有效引导射频识别产品发展安全功能，本标准结合射频识别系统各构成部分产品技术现状、运算能力等要求，明确了本标准提出的射频识别系统等级要求与 GB/T 37033.1-2018 信息安全技术 射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别中提出的射频识别系统安全级别的对应关系。具体对应关系如下：

电子标签基本级安全技术要求参照 GB/T 37033.1-2018 中的第二级要求、增强级安全技术要求参照 GB/T 37033.1-2018 中的第三级要求，阅读器/读写器基本级安全技术要求参照 GB/T 37033.1-2018 中的第三级要求、增强级安全技术要

求参照 GB/T 37033.1-2018 中的第四级要求，通信链路（空中接口）基本级安全技术要求参照 GB/T 37033.1-2018 中的第二级要求、增强级安全技术要求参照 GB/T 37033.1-2018 中的第三级要求，通信链路（网络传输）基本级安全技术要求参照 GB/T 37033.1-2018 中的第二级要求、增强级安全技术要求参照 GB/T 37033.1-2018 中的第三级要求，管理单元基本级安全技术要求参照 GB/T 37033.1-2018 中的第三级要求、增强级安全技术要求参照 GB/T 37033.1-2018 中的第四级要求。

6）增加了阅读器/读写器安全功能要求中的唯一性标识和身份鉴别要求

自 2017 年 12 月中共中央总书记习近平提出推动实施国家大数据战略，加快完善数字基础设施，加快建设数字中国以来，各行各业均陆续启动了大数据建设。作为一种采用射频识别（RFID）技术的自动识别和数据采集系统，射频识别（RFID）系统在大数据建设中具有重要作用。尤其是刚过去的 2021 年 9 月 29 日，工业和信息化部、中央网络安全和信息化委员会办公室、科学技术部、生态环境部、住房和城乡建设部、农业农村部、国家卫生健康委员会、国家能源局等八部门近日联合印发《物联网新型基础设施建设三年行动计划（2021-2023）》明确到 2023 年底，在国内主要城市初步建成物联网新型基础设施，社会现代化治理、产业数字化转型和民生消费升级的基础更加稳固。构成物联网感知层的标签、阅读器/读写器等硬件设备及具有自动识别和数据采集重要价值的射频识别（RFID）系统有望迎来规模化联网应用。基于此，标准起草组本次修订增加了阅读器/读写器安全要求中的唯一性标识和身份鉴别要求，为未来物联网新型基础设施建设和各行各业大数据建设中的射频识别（RFID）系统规模化应用奠定技术基础。

7）增加了阅读器/读写器安全要求中的审计日志要求

近年来，存储芯片成本下降，阅读器/读写器的存储空间相对增大，存在增加审计日志安全技术要求的现实基础。因此，标准起草组本次修订增加了阅读器/读写器安全要求中的审计日志要求，明确了审计日志的审计数据生成、日志内容、授权查阅、数据完整性保护等内容。不仅如此，本次修订还在增强级要求中增加了审计日志机密性保护内容，要求阅读器/读写器采用安全的密码算法对存储的审计日志进行加密。

8）在管理单元部分增加了信息系统等级保护的对应安全能力要求

结合 GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求中的安全通用要求和物联网安全扩展要求，本标准在管理单元部分增加了信息系统等级保护的对应安全能力要求。如身份鉴别、访问控制、恶意代码防范、可信验证、数据备份恢复、访问控制、数据完整性、数据保密、入侵防范、可恢复性、安全审计等。

5、解决的主要问题

本标准编制过程中重点解决了以下几个主要问题：

a）射频识别系统安全要求的保护范围

标准明确射频识别系统的保护范围涵盖标签、阅读器/读写器、通信链路及管理单元等四个组成部分。考虑标签与阅读器/读写器之间的空中接口通信链路的无线及开放式设计特征与阅读器/读写器与后端系统之间的网络传输通信链路对安全功能的要求存在差异性，分别对空中接口通信链路和网络传输通信链路提出安全技术要求。

b）射频识别系统安全功能要求的分级问题

GJB 7369-2011.2679 中将军用射频识别系统及各个组成部分的安全防护等级划分为 A 级、B 级、C 级、D 级及 E 级。由于本标准为信息安全技术范畴，依据 RFID 系统组成，本标准将射频识别系统通用安全功能要求按标签安全、阅读器/读写器安全、通信链路（空中接口）安全、通信链路（网络传输）安全及管理单元安全共五个子类给出，每个子类分别划分为 2 个等级：基本级和增强级。其射频识别系统应至少满足基本级安全技术要求。文中增强级要求仅列出了除基本级技术要求外的增强级要求。增强级应在符合基本级安全技术要求的基础上满足增强级要求。同时对技术要求给出了测试评价方法。

c）射频识别系统安全功能的设计、开发依据问题

标准编制组在标准标准过程中，广泛调研、分析了射频识别系统当前面临的安全威胁问题，并通过试验方式模拟捕获或攻击，获取射频识别系统读、写数据口令，控制读写器发送读、写命令对标签用户区数据进行获取和改写，确认各类威胁的严重性。在此基础上，提出射频识别系统的安全功能要求，为具有安全技术要求的射频识别系统整体及构成射频识别系统的各类RFID标签、读写器、通信

链路及管理单元的安全功能的设计、开发和使用提供标准依据，为提高国内射频识别系统的安全性，促进国内射频识别技术的发展，及国内RFID系统使用机构的敏感信息安全提供强有力的技术支撑。

三、主要试验[或验证]情况分析

公安部第三研究所为本标准的主要负责编制单位，单位下属的检测中心一直从事射频识别（RFID）系统及其标签、阅读器/读写器、管理单元等的检验检测工作。在本标准的编制过程中，检测中心依据该标准的要求，对多家厂商所生产的射频识别（RFID）系统及相关产品进行了验证测试。根据验证测试结果，对标准中所提出的部分安全技术要求及测试评价方法进行了相应的调整。

《GB/T 35290-2017 信息安全技术 射频识别系统通用安全技术要求》标准中规定了射频识别（RFID）系统安全技术相关的基本性要求和增强性要求，本标准结合射频识别（RFID）系统技术进步情况及 GB/T 22239-2019 中的安全通用要求和物联网安全扩展要求，修改提高了射频识别系统安全技术相关基本性要求和增强性要求，并针对相关技术要求给出了详细的测试评价方法。本标准编制过程中工作组也开展了相关射频识别系统安全威胁问题分析及可能的技术解决方案分析，为提出适当的安全功能要求及测试评价方法提供技术支持。

如我们通过手持频谱仪、示波器等便携波形采集设备对目前使用射频识别系统区域进行数据的监控和采集，可轻易捕捉和截获如图 1 所示的射频识别读写器和标签的通信信号。

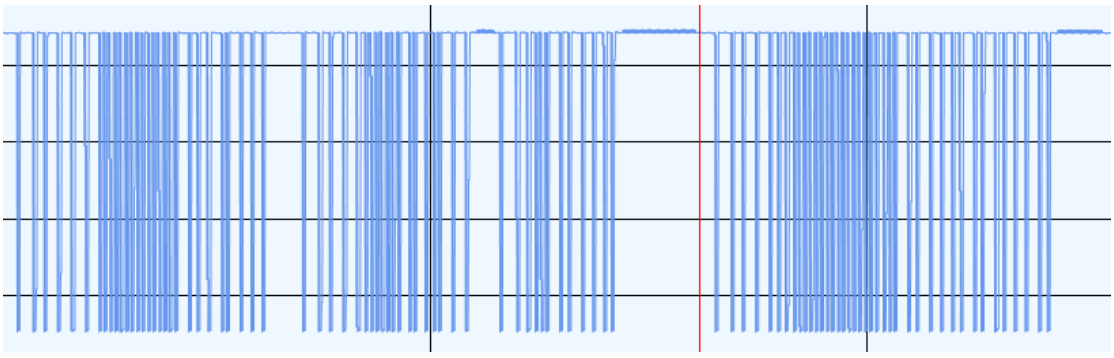

图 1 截获的 RFID 读写器和标签的通信信息

分析捕获到的读写器的发送指令以及标签返回的信号，通过把反向信号放大，得到图 2 的反向信号图谱：

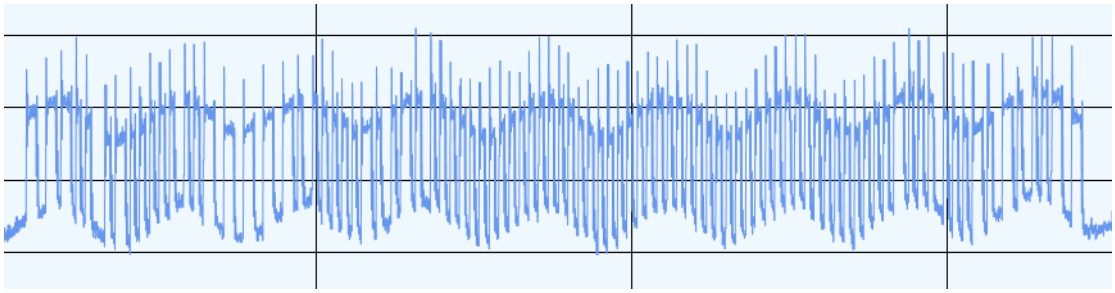

图 2 放大后的反向信号图谱

虽然捕捉到的反向信号存在毛刺，但还是可以清晰的看出反向信号的高低电平以及持续时间，再通过参照对应的射频识别标准可通过事先编制好的软件进行解调，得到如图 3 所示的解调后数据。

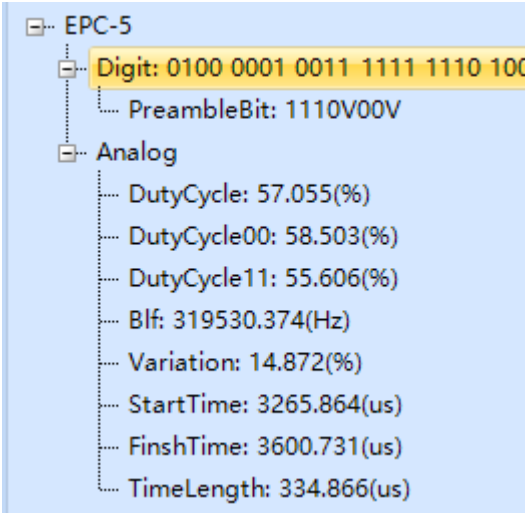

图 3　解调后的反向信号

通过遵照射频识别公开标准制作的解调软件，即可完整解调出读写器的前向信号和标签的反向信号，如图 4 所示。

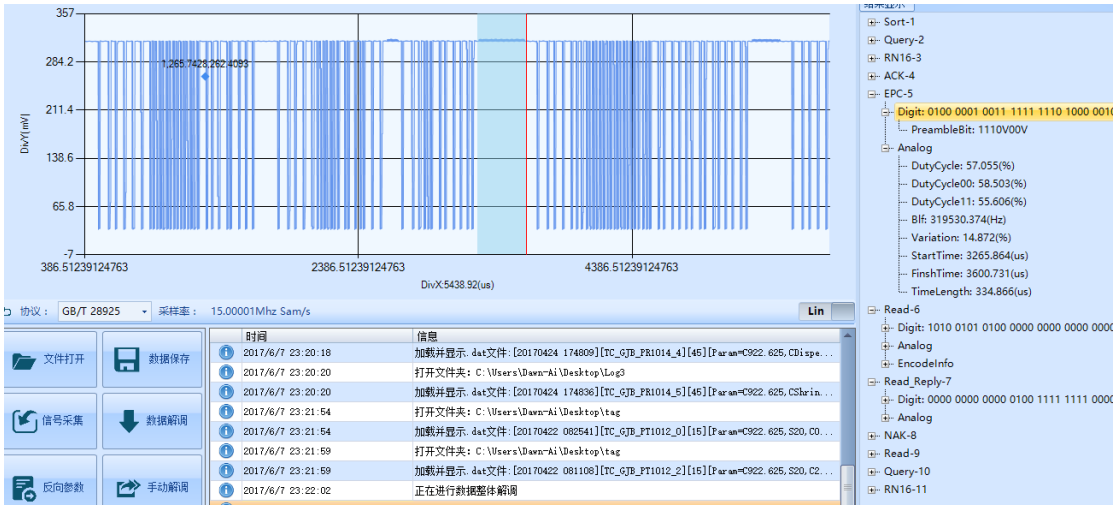

图 4 完整解调读写器和标签的通信信号

实验中，通过轻易获取射频识别系统读、写数据口令，控制读写器发送读、

写命令对标签用户区数据进行获取和改写，确认了目前使用的射频识别系统的安全问题的严重性。在此基础上，分析安全问题产生的原因，提出射频识别系统的信息安全技术要求及测试方法。

四、知识产权情况说明

标准内容中涉及的测评方法，公安部第三研究所已申请并获国家版权局授权了一项软件著作权，登记号为2016SR108995，证书号为软著登字第1287612号，名称为“一种UHF射频识别（RFID）空中接口安全性协议测试软件1.8.0”。因软件著作权不属于严格意义上的专利，故不在本标准中明确专利处理意见。

在标准编制过程中，未发现本标准的某些技术内容涉及具体专利。但不排除本标准中涉及加密算法的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

五、产业化情况、推广应用论证和预期达到的经济效果

RFID技术在中国的应用已有近20年的时间，RFID技术经过多年的发展，已经被证明在物品流通领域的自动化识别和数据交换方面具备得天独厚的优势，越来越多的制造、物流企业采用RFID技术提升其企业内部管理水平，降低流通环节成本，提高市场快速反应能力。受益于着我国智慧城市和物联网战略的稳步推进，中国RFID产业经历了一段高速成长阶段。然而，受限于RFID芯片较低的算力，一直以来，符合特定行业管理要求，具备安全能力的RFID系统及产品始终发展不尽如人意且未能实现产业化。

GB/T 35290-2017《信息安全技术 射频识别（RFID）系统通用安全技术要求》发布实施后，部分具备RFID标签芯片、RFID读写器芯片或读写器模块研制能力的RFID产业链头部企业积极按照GB/T 35290-2017的要求研发具备安全功能要求的RFID产品。但因该标准未明确与技术要求相对应的测试方法，其实际安全功能要求研发进度缓慢，目前大多难以满足实战单位的特定安全需求。

2021年9月，工信部等八部门联合印发《物联网新型基础设施建设三年行动计划（2021-2023年）》。《计划》明确，到2023年底，在国内主要城市初步建成物联网新型基础设施，社会现代化治理、产业数字化转型和民生消费升级的基础更加稳固。突破一批制约物联网发展的关键共性技术，培育一批示范带动

作用强的物联网建设主体和运营主体，催生一批可复制、可推广、可持续的运营服务模式，导出一批赋能作用显著、综合效益优良的行业应用，构建一套健全完善的物联网标准和安全保障体系。《计划》还提出聚焦感知、传输、处理、存储、安全等重点环节，加快关键核心技术攻关，提升技术的有效供给。

《物联网新型基础设施建设三年行动计划（2021-2023 年）》为作为物联网感知层重要设备的射频识别（RFID）系统提供了新的战略发展机遇，尤其是明确聚焦安全等重点环节，为具备安全功能要求的射频识别（RFID）系统的技术进步和产业发展创造了良好条件。

本标准发布实施后，将有力助推具备安全功能要求的射频识别（RFID）系统的技术进步和产业发展，为目前已明确提出智能化管理需求的公安装备管理、重要案卷管理、危险化学品管理等强调安全功能要求的管理应用提供符合标准要求的安全射频识别（RFID）系统及产品。在全国持续开展智慧公安建设及危险化学品专项治理行动的时代大背景下，预期将创造百亿计的经济效益及良好的社会效益。

六、采用国际标准和国外先进标准情况

射频识别技术和应用相关国际标准化机构主要有国际标准化组织(ISO)、国际电工委员会(IEC)、国际电信联盟(ITU)、世界邮联(UPU)。此外还有其他的区域性标准化机构，如 CEN;国家标准化机构，如 BSI、ANSI、DIN 等。这些机构均在制订与射频识别相关的区域、国家或产业联盟标准，但已经发布或者是正在制订中的标准主要是与数据采集相关的，主要有电子标签与读写器之间的空中接口、读写器与计算机之间的数据交换协议、RFID 电子标签与读写器的性能和一致性测试规范以及 RFID 电子标签的数据内容编码标准，针对系统安全的标准相对匮乏。目前，在国际标准中，射频识别系统安全相关技术要求主要在 ISO/IEC 18000-1、 ISO/IEC 18000-4、ISO/IEC 18000-6、 ISO/IEC 18000-7 等空中接口协议标准中体现。ISO/IEC SC31 提出修订 ISO/IEC 29176-2011，使之成为与 ISO/IEC 18000 系列标准一一对应的射频识别空中接口安全系列标准，目前尚未查到该系列标准发布，仅在国际标准 ISO/IEC 18000-63-2015《Information technology — Radio frequency identification for item management — Part 63》中涉及一些特殊鉴别指令说明。

本标准编制过程中，主要分析了 ISO/IEC 18000 及 ISO/IEC 14443 系列国际标准，研究了《EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID》等 EPC 系列国际标准，并对以下国家标准进行了学习和借鉴：

GB/T 20271-2006 《信息安全技术 信息系统通用安全技术要求》

GB/T 33848.3-2017 信息技术 射频识别 第 3 部分：13.56MHz 的空中接口通信参数

GB/T 28925-2012 《信息技术 射频识别 2.45GHz 空中接口协议》

GB/T 28926-2012 《信息技术 射频识别 2.45GHz 空中接口符合性测试方法》

GB/T 29261.3-2012 《信息技术 自动识别和数据采集技术 词汇 第 3 部分 射频识别》

GB/T 29768-2013 《信息技术 射频识别 800/900MHz 空中接口协议》

GB/T 35102-2017 《信息技术 射频识别 800/900MHz 空中接口符合性测试方法》

GB/T 37033.1-2018 《信息安全技术 射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别》

GB/T 37033.2-2018 《信息安全技术 射频识别系统密码应用技术要求 第 2 部分：电子标签与阅读器/读写器及其通信密码应用技术要求》

GB/T 37033.3-2018 《信息安全技术 射频识别系统密码应用技术要求 第 3 部分：密钥管理技术要求》

GB/T 22239-2019《信息安全技术 信息系统安全等级保护基本要求》

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 37093-2018《信息安全技术 物联网感知层接入通信网的安全要求》

除 GJ B 7369-2011.2679 《军用射频识别系统安全通用要求》外，其余标准更多关注 RFID 系统的性能功能，而对安全功能要求很少涉及。

GJB 7369-2011.2679 《军用射频识别系统安全通用要求》作为军用领域的标准，适用于军用射频识别系统的研发、生产、测评、订购和使用，主要包括标签安全、读写器安全、通信链路安全、后端系统安全，并针对军用射频识别系统面临的安全威胁和涉密等级划分成 A 级、B 级、C 级、D 级、及 E 级，每个等级

对应的安全要求不同。虽然标准在内容上覆盖了 RFID 系统的组成部分的安全的技术要求，但 RFID 系统框架中的通信链路定义模糊不清、等级划分过细，因此无法普遍适用于射频识别(RFID)系统通用安全技术要求及测试评价方法的使用。

GB/T 28925-2012《信息技术射频识别 2.45GHz 空中接口协议》、GB/T 22351-2015《信息技术射频识别 13.56MHz 空中接口协议》、GB/T 29768-2013《信息技术射频识别 800/900MHz 空中接口协议》主要是 RFID 系统功能方面的技术要求；GB/T 37033 射频识别系统密码应用技术要求系列标准，主要是 RFID 系统涉及密码的应用技术要求，对 RFID 系统本身的安全功能要求未涉及，在本标准中作为规范性引用文件。

本标准未直接采用国际标准和国外标准。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准作为 GB/T 35290-2017《信息安全技术 射频识别（RFID）系统通用安全技术要求》的修订标准，符合国家相关现行法律法规，顺应工信部 2020 年发布的《工业和信息化部办公厅关于深入推进移动物联网全面发展的通知》中“推进移动物联网应用发展”、“推动设备联网数据采集”的产业发展政策，与 GB/T 20271-2006、GB/T 22239-2019、GB/T 22351-2015 、GB/T 28925-2012、GB/T 29261.3-2012、GB/T 29768-2013、GB/T 32915-2016、GB/T 37033.1-2018、GB/T 37033.2-2018 、GB/T 37033.3-2018 等国家标准协调一致。本标准将弥补 GB/T 29768-2013、GB/T 28925-2012、GB/T 28926-2012、GB/T 22351-2015、GB/T 35290-2017 等 RFID 系统空中接口协议标准及符合性测试方法标准中关于安全要求及测试评价方法内容的匮乏与不足，完善现行射频识别技术标准体系。

八、重大分歧意见的处理经过和依据

本标准编制过程中，如标准编制组内部出现重大意见分歧时，由标准编制组组长组织召开内部调解会解决。如果征求意见过程中，各厂家，特别是各部委意见与标准编制组之间出现重大意见分歧，由全国信息安全标准化技术委员会组织召开协调会解决，并认真听取专家意见进行修改。

本标准编制过程中暂无重大分歧意见。

九、标准性质的建议

建议将本标准作为推荐性国家标准在全国实施。

十、贯彻标准的要求和措施建议

本标准为设计、研发、生产和测试评价具备安全技术要求的RFID系统提供指导性意见，建议在全国推荐性实施。在具体贯彻实施该标准时，首先可要求不同的产品测试机构使用该标准作为射频识别系统及其相关产品的测试依据，例如，可使用在产品的销售许可测试、政府采购设备的准入测试、不同需求单位的招标选型测试等，由此可以进一步推动相关研发、生产企事业单位以该标准为依据，达到业界内全面使用该标准的局面，全面提升射频识别系统的安全性，助力国家信息安全建设。

因当前射频识别系统安全功能的设计、开发和使用急需本标准提供技术依据，建议本标准从发布之日起正式实施。

十一、替代或废止现行相关标准的建议

本标准代替GB/T 35290—2017《信息安全技术 射频识别（RFID）系统通用安全技术要求》。

十二、其它应予说明的事项

无。

国家标准《信息安全技术 射频识别（RFID）系统安全技术要求与测试评价方法》

起草工作组

2022-07-25