GTI

Research Report on Universal Testing Methodology for Ambient-IoT Devices —Research on Building a Testing and Certification System for the Ambient-IoT Devices

https://gtigroup.org/

GTI

GTI Research Report on Universal Testing Methodology for Ambient-IoT Devices —Research on Building a Testing and Certification System for the Ambient-IoT Devices

Version:	V1.0.0
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Program	**5G Enterprise Network Solutions**
Project	**Joint Research on Universal Testing Methodology for Ambient-IoT Devices**
Source members	China Mobile Communications Group
Support members	CICT Mobile Communication Technology, Datang LinkTester Technology, Huawei Technologies, Beijing Hwa-tech Information System, Matrix Technology, MaxWave Microelectronics, Qualcomm Incorporated, Rohde & Schwarz (China) Technology, Shanghai Fudan Microelectronics Group, Shanghai Quanray Electronics Technology, Shanghai Tejet Communications Technology, Shenzhen Institute of Standards and Technology, Sichuan Kiloway Technologies, Xiamen

	Xindeco IOT Technology, ZTE (In Alphabetical Order by Company Name)
Editor	**CMCC**: Dan SONG, Shanpeng XIAO, Shuai MA, Yanyan CAO, Yuan LI, Shiying Zheng, Pengzhan LIU; **CICT**: Jiye TANG; **Huawei**: Haiping XU; **Hwa-tech**: Nan ZHANG; **Matrix Tech**: Jie YANG, Xingxiu YAN; **MaxWave**: Xuexian WANG, Junliang YANG; **Qualcomm**: Bin HAN, Ting WANG; **R&S**: Lilei WANG; **Shanghai Fudan Microelectronics**: Lei WANG, Kun ZHANG; **Shanghai Quanray**: Zhiwei LU, Yinan CHEN; **Shanghai Tejet**: Jiankun DENG, Zidong CHEN; **SIST**: Qihong DAN, Yuanhong LI, Yumin LUO; **Sichuan Kiloway**: Honghai GU, Xiaohui XU; **Xindeco IOT**: Lei REN, Yanwei QIU, Yun YANG; **ZTE**: Hong CHANG, Ni CAO, Jianbin HU, Dai XU. (In Alphabetical Order by Company Name)
Last Edit Date	July 22, 2026
Approval Date	August 6, 2026

Document History

Date	**Meeting #**	**Version #**	**Revision Contents**
06-08-2026	Post GTI 45th Workshop	V1.0.0	

Table of Contents

1 Executive Summary

Addressing the issues of absent testing and certification systems for Ambient IoT devices, fragmented standards, and disconnection between testing and real-world scenarios, this report systematically studies the necessity and feasibility of constructing an Ambient IoT device testing and certification system. The report proposes conducting testing specification research oriented toward real application scenarios based on the GTI (Global Technology Association of InfoComm) international industry platform. It proposes building a "Chip—Device—Application" 3-tier testing and certification system, achieving coordinated evolution between the testing certification process and the industry ecosystem, and enhancing the scalability and industrialization level of the testing certification system. This report provides theoretical support and practical pathways for promoting the construction of Ambient IoT testing and certification systems and facilitating the large-scale deployment of Ambient IoT.

2 Abbreviations

Abbreviation	**Explanation**
A-IoT	Ambient Internet of Things
AGV	Automated Guided Vehicle
AIOTF	Ambient IoT Function
AMF	Access and Mobility Management Function
ARC	Arkansas Radio Compliance
BPSK	Binary Phase Shift Keying
CQC	China Quality Certification Centre
CW	Carrier-wave
DUT	Device Under Test
EHS	Energy Harvesting Sensitivity
EMI	Electromagnetic Interference
EPCglobal	Electronic Product Code Global
EVM	Error Vector Magnitude
FDX	Full Duplex
FFS	For Further Study
GS1	Global Standards One
HDX	Half Duplex
HF	High Frequency
ID	Identification
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
LF	Low Frequency
MAC	Media Access Control
NFC	Near Field Communication
NLoS	Non-Line-of-Sight
OOK	On-Off Keying
OTA	Over The Air
PCB	Printed Circuit Board
RF	Radio Frequency
RFID	Radio Frequency Identification
RRU	Radio Remote Unit
rUC	reference Use Case

SNR	Signal-to-Noise Ratio
TIPP	Tagged-Item Performance Protocol
UHF	Ultra High Frequency

3 Introduction

3.1 Research Background

With the accelerated commercialization of 5G-Advanced (5G-A) technology and the gradual clarification of the 6G vision, the global information and communications industry is entering a new era of "ubiquitous connectivity, zero power consumption, and full-scenario coverage" IoT development. Traditional cellular mobile networks primarily serve high-power communication devices with continuous power supply capabilities such as smartphones and mobile devices. However, the massive "dumb devices" called for in the IoT era—including sensor devices, asset identifiers, and environmental monitoring nodes—have entirely different requirements for communication technology: extremely low power consumption, extremely low cost, maintenance-free operation, and even self-power generation. This demand has given rise to the rapid development of Ambient IoT technology and industry attention.

The essence of Ambient IoT technology lies in enabling devices to free themselves from dependence on traditional batteries by harvesting weak energy from the environment (including natural light energy, thermal energy, vibrational energy, and environmental radio frequency signals) to drive device operation, and by implementing information exchange with readers or base stations through backscatter communication technology. Compared with traditional active IoT technology, Ambient IoT offers the following significant advantages: device service life can exceed ten years, hardware costs can be reduced to one-tenth or even lower of traditional active devices, no on-site battery replacement maintenance is required, and "deploy and forget" maintenance-free operation can be achieved after deployment. These characteristics make Ambient IoT technology a key enabling technology for connecting massive lightweight IoT nodes, filling coverage gaps left by traditional technologies, and lowering the threshold for large-scale IoT deployment.

From the perspective of industry development stage, Ambient IoT technology is currently at a critical turning point from technology verification to large-scale commercialization. At the international standardization level, 3GPP completed preliminary analysis of Ambient IoT use cases and deployment scenarios during the Release 18 phase, completed the standardization specification for Device 1 type devices during the Release 19 phase (formally frozen in December 2025), covering the physical layer, MAC layer, network protocols, and base station technical requirements. The Release 20 phase will further expand toward wide-area scenarios. At the industry practice level, multiple global operators, equipment vendors, and chip manufacturers have actively carried out technology verification and commercial pilots. As of June 2026, solutions based on 5G-A Ambient IoT have been deployed in multiple industry showcases in areas such as smart warehousing, industrial manufacturing, office parks, and commercial retail, with technical feasibility and industry value having been initially verified.

However, while technology standards and industry practices are advancing rapidly, the testing and certification system construction—serving as the critical bridge connecting technical specifications and commercial applications—has severely lagged behind industry demands. Currently, there is no unified, authoritative Ambient IoT testing and certification standard system covering the entire process from chips to devices to application scenarios globally. Specifically, the industry faces the following core challenges:

1. **Testing and Certification System Gaps**: Although existing RFID device testing and certification systems (such as UHF RFID) are relatively mature, their testing methods and certification frameworks primarily target traditional frequency band device products such as 13.56 MHz and 860 MHz to 960 MHz, and cannot be directly applied to Ambient IoT devices operating based on cellular networks. The latter have essential differences from traditional RFID in terms of operating frequency bands, modulation methods, energy harvesting mechanisms, and network access procedures, requiring entirely new testing methods and certification frameworks to support them.
2. **Incomplete Coverage of Testing Specifications**: Although 3GPP RAN5 is building a complete set of testing specifications for Ambient-IoT passive devices at the basic communication level, testing specifications are still lacking for application-layer testing, scenario adaptability testing, production line testing, and platform testing, which may lead to potential risks such as poor device and actual network interoperability, difficulties in upstream and downstream coordination, low recognition from industry customers, and high application deployment risks.
3. **Disconnection Between Testing Systems and Real Scenarios**: Existing communication device testing is generally conducted under ideal laboratory conditions, and the measured sensitivity, coverage distance, and concurrent capacity indicators often fail to truly reflect device performance in actual deployment. For Ambient IoT devices, the high complexity of actual deployment environments—including dense cargo stacking, metal surface reflections, multi-base-station signal superposition, strong electromagnetic interference, and extreme temperature and humidity changes—pose far greater challenges to device environmental adaptability, robustness, and reliability than laboratory conditions. If the testing system is disconnected from real scenarios, certified devices may still experience performance degradation and functional failures in actual deployment, damaging confidence among all industry parties.
4. **Lack of Chip-Device-Application Coordination Mechanism**: The Ambient IoT industry chain involves multiple links such as chip design, device manufacturing, antenna processing, base station equipment, and application platforms. The current testing system has not effectively achieved layered decoupling and result reuse across the upstream and downstream. When the same chip model is paired with different antennas, different packaging processes, or different application scenarios, complete sets of tests often need to be repeated, causing massive repeated testing and resource waste, and hindering industry-scale efficiency improvements.
5. **Cost Barriers Constraining Industry Adoption**: The procurement and operation costs of high-precision Ambient IoT testing systems are high, and testing capabilities are highly concentrated in a few head laboratories or large vendors.

Small and medium-sized vendors find it difficult to bear the cost of building their own testing capabilities, and relying on external testing submission may face difficulties in obtaining testing resources, long cross-border testing cycles, and high costs, objectively raising industry entry barriers.

It is based on the above industry background and problem awareness that this report systematically studies the pathways for constructing general testing methods and a certification system for the Ambient IoT ecosystem, aiming to provide theoretical support and practical guidance for promoting the construction of Ambient IoT testing and certification systems and accelerating industry large-scale deployment.

3.2 Research Purpose and Significance

3.2.1 Research Purpose

This research aims to systematically construct a general, reusable, and scalable testing method and certification system framework for the Ambient IoT ecosystem, addressing core issues such as the absence of Ambient IoT device testing and certification systems, fragmented standards, and disconnection between testing and application scenarios. The specific research objectives include:

1. **Systematically reviewing the mature experience and limitations of existing RFID device testing and certification systems**: Through comprehensive research on protocol conformance testing, performance testing, and certification mechanisms for UHF RFID, HF RFID, and LF RFID—the three mainstream passive device categories—this report summarizes referable system architectures and best practices while identifying gaps between these systems and Ambient IoT device testing requirements, providing a starting reference for constructing the new system.
2. **In-depth analysis of the necessity and feasibility of building an Ambient IoT certification system**: From multiple dimensions such as ensuring device interoperability and compatibility, improving real-environment reliability, establishing industry trust mechanisms, and reducing market transaction costs, this report demonstrates the importance of system construction, while assessing feasibility in terms of technical foundations, industry conditions, and organizational mechanisms, providing sufficient argumentative support for decision-makers.
3. **Proposing a systematic Ambient IoT certification system framework design**: Including certification philosophy, certification level division, certification process design, technical support platform construction, etc., forming an operational and implementable system plan.
4. **Building a "Chip-Device-Application" 3-tier separated testing system**: Through vertical decoupling and result reuse mechanisms, achieving clear responsibility division among upstream and downstream industry chains and stepped allocation of testing and certification costs, improving the industrialization efficiency and economics of the testing system.
5. **Designing a testing specification system oriented toward typical application

scenarios: For core scenarios such as smart warehousing, logistics tracking, industrial manufacturing, and smart elderly care, extracting the mapping relationships between scenario characteristics and testing indicators, forming scenario-driven differentiated testing plans, ensuring close alignment between the testing system and actual deployment requirements.

6. **Exploring coordination and advancement mechanisms based on international industry platforms such as GTI**: Studying pathways for coordinating industry chain forces and jointly building and sharing testing specifications and certification ecosystems through international industry organizations, laying foundations for the global promotion of the system.

3.2.2 Research Significance

The significance of this research is reflected at both theoretical value and practical application levels:

From the perspective of **theoretical value**, this research is the first to systematically introduce general testing method research into the Ambient IoT field, building a bridge connecting technical standards and industry practices. Currently, academia and industry attention to Ambient IoT technology is primarily focused on technical dimensions such as communication technology evolution, energy harvesting circuit design, and network architecture optimization, while research on testing and certification systems is relatively lagging. By introducing the "Chip-Device-Application" 3-tier separated testing concept, scenario-driven testing design methods, and open collaborative specification development mechanisms, this research enriches the theoretical content of IoT testing engineering, laying a methodological foundation for subsequent research.

From the perspective of **practical application**, the certification system framework and testing methods proposed by this research have multiple values for promoting the healthy development of the Ambient IoT industry:

a. Providing a unified evaluation benchmark and quality standard for industry chain parties: Chip manufacturers, device manufacturers, system integrators, and end users can make objective product selection and technical decisions based on certification results, reducing transaction costs and trust risks caused by information asymmetry.

b. Providing a technical tool for government regulation and industry management: The certification system can connect with regulatory mechanisms such as radio transmission equipment type approval, network access licensing, and product recall, promoting compliant industry development and preventing safety hazards and market disorders.

c. Providing quantifiable risk assessment foundations for financial institutions and insurance companies: Certified devices can serve as quality asset targets, supporting innovative business models such as supply chain finance based on IoT data, equipment financing lease, and asset insurance, reducing financial barriers to technology promotion.

3.3 Research Content and Technical Route

3.3.1 Research Content

Centering on the core proposition of "constructing general testing methods and a certification system for the Ambient IoT ecosystem," and following the logical thread of "status survey—problem analysis—system design—scenario implementation—mechanism guarantee," this research conducts systematic research in the following five modules:

Module 1: Survey of Existing RFID device Certification Systems and Production Line Testing Status

This module conducts a comprehensive survey of protocol conformance testing and performance testing certification systems for UHF RFID, HF RFID, and LF RFID—the three major categories—deeply analyzing the organizational structure, core specifications, testing processes, certification mechanisms, and actual operation effects of each system. At the same time, it surveys the full-process procedures, quality control requirements, and special management mechanisms of device production line testing and chip production line testing. Through systematic review, it identifies limitations of existing systems in addressing Ambient IoT testing requirements, including testing method differences, frequency band adaptation issues, and insufficient scenario coverage, providing a starting reference for new system design.

Module 2: Ambient IoT Testing and Certification System Construction Research

Starting from technical characteristics and ecosystem needs, this module demonstrates the necessity of system construction in ensuring device interoperability and compatibility, improving real-environment reliability and stability, and establishing industry trust mechanisms, while assessing feasibility in terms of technical foundations, industry conditions, and organizational mechanisms. On this basis, it proposes the overall framework design of the certification system, including the four core concepts of "open, universal, scalable, and verifiable," five certification levels (basic function certification, universal compatibility and interoperability certification, environmental adaptability certification, lifecycle and reliability certification, and security certification), and a complete certification process (application—testing—scenario verification—expert review—certificate issuance). It also plans the construction concept for a highly intensive, automated, and intelligent technical support platform.

Module 3: Construction of "Chip-Device-Application" 3-tier Testing and Certification System

This module is the core methodological innovation of this report. It systematically elaborates the separation principles and usage rules of the 3-tier testing system, clarifying the core testing content, judgment criteria, and expected technical indicators of each tier (chip testing tier, device testing tier, and application testing tier), as well as the access conditions, certification transfer paths, and result reuse mechanisms among the three tiers. The chip testing tier focuses on chip protocol implementation completeness and basic functional correctness. The device testing tier focuses on RF consistency, wireless resource management consistency, and mechanical environmental durability after chip and antenna integration. The application testing tier verifies system-level performance in final business scenarios. Through 3-tier progressive testing, it achieves clear responsibility division among industry chain links and stepped allocation of testing costs.

Module 4: Construction of Application Scenario-Driven Testing Requirements System

This module systematically analyzes typical Ambient IoT application scenario characteristics, including outdoor continuous networking capability, complex deployment environment adaptability, full-scenario management capability, high-concurrency inventory requirements, mobile scenario support, environmental sensing capability, and security assurance requirements. For multiple vertical scenarios such as supply chain warehousing and logistics, industrial manufacturing and tooling equipment management, smart buildings and fire protection corridors, data center machine room environmental control and asset management, retail and luxury anti-counterfeiting, medical surgical instrument management, power grid equipment monitoring, and elderly care facility personnel management, it extracts the mapping relationships between scenario characteristics and testing indicators. At the same time, it studies scenario-oriented testing specification design methods. Referring to the "Scenario-Indicator-Method" three-element model, it proposes differentiated testing plan design guidelines.

Module 5: Research on Coordination Mechanisms for Testing Specification Development

This module focuses on the industry collaboration mechanisms required for certification system implementation. It advocates a specification development model led by international industry platforms such as GTI with participation from all industry chain parties, designs the organizational structure, member composition, and operation mechanisms of testing specification project groups, and proposes an iterative advancement process of "open solicitation—expert review—pilot verification—specification release." At the same time, it studies key topics such as global mutual recognition mechanism construction, international standard alignment, and industry ecosystem cultivation, providing pathway guidance for the global promotion of the system.

3.3.2 Technical Route

This research adopts the technical route of "literature survey—field survey—theoretical analysis—framework design—scenario verification—mechanism research," specifically as follows:

Phase 1: Literature Survey and Data Collection

Systematically search and analyze 3GPP Release 18/19/20 Ambient IoT-related technical specifications, ISO/IEC 18000 series RFID international standards, EPCglobal/GS1 TIPP/ARC and other mature certification system specifications, domestic and foreign academic literature and industry technical reports, fully mastering the evolution and development trends of technical standards and certification mechanisms. At the same time, collect and organize domestic operator, equipment manufacturer, chip manufacturer, and device manufacturer pilot cases and technical documents in the Ambient IoT field.

Phase 2: Industry Chain Field Survey

Visit major domestic and foreign RFID device certification institutions, chip packaging testing manufacturers, device manufacturing production lines, and operator IoT laboratories to conduct field surveys, deeply understanding the actual operation status, production line testing processes, quality control mechanisms, and pain points of existing testing and certification systems. Simultaneously conduct interview surveys with chip manufacturers, device manufacturers, application parties, and other industry chain parties, collecting real demands and improvement suggestions for testing and certification systems from the front lines of industry.

Phase 3: Theoretical Analysis and Framework Design

Based on survey information, using research methods such as system analysis, comparative analysis, and inductive deduction, analyze the successful experiences and deficiencies of existing systems, extracting methodological principles applicable to Ambient IoT testing and certification. On this basis, design the overall framework of the certification system, including core concepts, level division, process design, and platform concepts, repeatedly refining through discussion and demonstration.

Phase 4: 3-tier Testing System Construction

Deeply research the feasibility demonstration and specific plan design of "Chip-Device-Application" 3-tier separated testing, clarifying the core objectives, test case design, judgment criteria setting, and expected technical indicators of each tier. Simultaneously research the connection and transfer mechanisms and result reuse rules among the three tiers, ensuring rigorous logic and strong operability of the system.

Phase 5: Scenario Testing Specification Development

For typical application scenarios, extract scenario characteristic parameters, construct scenario-to-testing-indicator mapping models, design differentiated testing environment configurations and judgment criteria. Develop typical scenario test cases, clarify testing conditions, judgment thresholds, and implementation processes, forming scenario-based testing specifications that can directly guide testing practice.

Phase 6: Coordination Mechanism Research and Output

Research the coordination mechanism design based on international industry platforms such as GTI, forming project group formation plans, iterative advancement processes, and global mutual recognition pathways for specification development. Finally, form a complete research report, outputting unified testing methods and a certification system framework to guide industry practice.

4 Survey of Existing RFID device Certification Systems and Production Line Testing Status

4.1 Analysis of Mainstream RFID device Certification Systems

Radio Frequency Identification (RFID) is a wireless communication identification technology that can complete specific target identification and data reading/writing based on radio signals without establishing mechanical or optical contact between the the Reader and the target device. Since the concept of the Internet of Everything was proposed and developed, RFID technology has become the most important underlying technology for IoT to achieve item digital management and full-process traceability, thanks to advantages such as multi-device batch reading, long-distance identification, rewritable capability, and strong environmental adaptability. With the rapid iteration of the entire RFID industry chain and global application proliferation, supporting RFID device testing and certification systems have become increasingly complete with continuously improving standardization. RFID device testing and certification is the core management mechanism for ensuring product compliance, interoperability, and actual application performance, and is also a cornerstone for the standardized and large-scale development of the global RFID industry. Currently, the industry's comprehensive quality evaluation of devices is mainly divided into two core areas: protocol conformance and device performance.

According to working frequency classification, mainstream passive RFID devices in the market are divided into three major categories: Low Frequency (LF), High Frequency (HF), and Ultra High Frequency (UHF). UHF RFID relies on long-distance identification and multi-device reading advantages, dominating the global retail and logistics supply chain market, and is also the category with the most complete certification system and highest internationalization degree globally. HF RFID focuses on short-distance communication, widely used in areas such as access control, public transit, financial payment, and archive management, with mature technology and a huge civilian market. LF RFID features good compatibility with non-metallic media and strong anti-interference capability, and is widely applied in niche scenarios such as animal identification, industrial anti-theft and special industrial identification. devices in different frequency bands have significant differences in corresponding protocol specifications, application scenarios, and certification systems. For protocol conformance, UHF RFID devices have an EPCglobal certification. In terms of LF and HF devices, laboratory testing and verification are primarily conducted based on ISO protocol standards. For device performance,, UHF RFID devices have two international certification systems: one is the TIPP certification published by GS1, and the other is the ARC certification launched by Auburn University Laboratory in the United States. Additionally, China's Quality Certification Centre (CQC) has also launched UHF RFID device performance classification certification, mainly serving China IoT project acceptance and industry bidding. By comparison, testing is the primary means for LF and

HF devices. The two major areas form device quality constraints from two dimensions—communication compatibility capability and field implementation performance—jointly constituting the RFID device quality management framework.

4.1.1 Protocol Conformance Testing and Certification

The core objective of protocol conformance work is to verify device consistency with international universal air interface protocols, ensuring interoperability between different manufacturers' devices and reader devices.

4.1.1.1 UHF RFID devices

The mainstream UHF RFID operating frequency band is 860 MHz to 960 MHz, and the current core standard ISO/IEC 18000-63:2021 evolved from the early industry-universal ISO/IEC 18000-6C. In the early stage of industry development, various RFID product communication protocols were not compatible, and equipment from different manufacturers could not interconnect. To solve this pain point, international standards organizations jointly prepared the ISO/IEC 18000 series air interface standards with industry chain organizations. Among them, Version 6C was specifically for 860 MHz to 960 MHz passive UHF RFID, uniformly specifying underlying communication rules such as signal modulation, data coding, reader-writer interaction commands, and multi-device anti-collision algorithms. After technical iteration and version integration, the 6C specification was officially updated to ISO/IEC 18000-63:2021 as the global UHF RFID universal underlying communication protocol. Based on this international underlying communication standard, EPCglobal further expanded the standard boundaries, supplementing and improving supporting content such as EPC item coding rules, upper-layer application interaction specifications, and storage area data formats, building a complete standard system for the global supply chain. On this standard system, UHF RFID devices have formed a dual qualification assessment mechanism of testing plus certification:

I. General Testing

Using the accompanying ISO/IEC 18047-63:2023 as the protocol conformance testing method standard, it provides standardized testing processes, judgment thresholds, and test cases. Conducting tests according to the testing methods accompanying ISO/IEC 18047-63:2023 is an essential step for product research and development and production line quality inspection. All device manufacturers must pass this test to ensure products meet basic protocol requirements:

Core Testing Items:

Mainly includes frequency range, demodulation capability, link frequency deviation, link time T1, link time T2, etc., comprehensively verifying whether devices fully match protocol specifications.

Among them:

- **Link frequency deviation**: The maximum allowed deviation range between the device's actual backscatter frequency and its nominal backscatter frequency. Backscatter frequency is the bandwidth frequency at which the device communicates to the reader.

- **Link time T1**: The time from the reader transmission to the device response.
- **Link time T2**: The time from the device response to the reader's next transmission.

Implementation Process:

1. Sample submission: Enterprises submit finished devices, chip samples, and product technical materials.
2. Laboratory testing: Complete tests item by item according to standards.
3. Problem rectification: Non-conforming items are re-submitted after the enterprise optimizes design/process.
4. Report issuance: Issue third-party test reports after passing testing.

Implementation Cycle:

Normal submission cycle is 3 to 7 working days; if non-conforming items require rectification, the cycle extends to 1 to 2 weeks depending on problem complexity.

II. EPCglobal Certification

EPCglobal certification is the earliest certification related to UHF RFID. Testing work is executed by globally authorized third-party laboratories designated by EPCglobal. On the basis of conformance testing, it adds interoperability testing and technical document review. After passing, an official certification certificate is issued. This certification has global mutual recognition effect and is the mainstream entry requirement for cross-border retail and logistics supply chain:

Core Certification Items:

On the basis of fully covering all ISO/IEC 18047-63 protocol conformance test items, it adds two core certification contents:

1. **Interoperability testing**: Verifying product adaptation and interconnection capability with industry mainstream benchmark reader devices, and multi-device dense reading stability.
2. **Product technical document review**: Checking the completeness, standardization, and product consistency of materials such as product specifications, protocol implementation descriptions, memory mapping tables, and functional parameter documents.

Implementation Process:

1. Qualification application: Enterprises submit formal "Certification Application Form" to authorized laboratories, specifying product models, manufacturer information, protocol versions, declared supported functional items, and application scenarios. Submit the required number of samples and technical documents.
2. Authorized laboratory testing work: Certification testing is strictly divided into protocol conformance testing and interoperability testing. Conformance testing must be passed first before entering interoperability testing. Both are executed according to unified testing specifications published by GS1.
3. Issuing formal test report: After all test items pass, the laboratory issues a complete official test report including testing environment, test case list, each test result, and conclusion explanation, submitted to GS1 Global Headquarters after

signature and seal.

4. GS1 global final review and certificate issuance: Authorized laboratories submit test reports, application materials, sample information, and original test records to GS1 global headquarters certification department. GS1 headquarters conducts final review of testing process compliance, report completeness, and result validity. After confirmation that products fully comply with certification standards, the official certification certificate is uniformly issued by GS1 headquarters. Certificates carry unique certification numbers and official marks. Products are simultaneously included in the GS1 global certified product list, publicly searchable on the GS1 website for global customers to verify authenticity.
5. Certificate issuance: Electronic certificates are sent to applicant enterprises, and paper certificates can be applied for as needed. Authorized laboratories simultaneously notify enterprises of certification completion.
6. Post-certification maintenance and change management: Certificates are valid for the corresponding model and version indefinitely. If GS1 protocol standards are significantly upgraded, enterprises can autonomously choose whether to upgrade certification.
7. Product change notification: When product hardware, firmware, or protocol implementation changes, it must be notified to GS1 and authorized laboratories. Minor changes (such as packaging process optimization without affecting protocol logic) can maintain the original certificate after notification. Major changes (such as chip revision, protocol function changes, significant antenna design adjustments) must reapply for complete certification.

Implementation Cycle:

Without rectification, the entire process from formal project initiation to obtaining the certificate takes approximately 6 to 10 weeks. If rectification and retesting are involved, the cycle extends accordingly depending on rectification difficulty.

4.1.1.2 HF RFID devices

HF RFID devices primarily operate in the 13.56 MHz frequency band, and the industry has formed two parallel international standards. The first type is ISO/IEC 14443 (Type A/B), for near-field communication scenarios within 10 cm, with mature technology and widespread application. Typical implemented products include access cards, transit cards, and mobile payment cards. The second type is ISO/IEC 15693, supporting medium-distance reading/writing within 1 m. With better reading/writing distance and anti-interference performance suitable for item batch management, it is widely used in scenarios such as library book management, archive storage, and asset inspection. Both product types use third-party test reports as the main protocol compliance basis.

Core Testing Items:

The basic testing content of the two protocol conformance systems is largely consistent. Common test items include: carrier frequency, RF modulation parameters, communication timing, basic command response, data integrity verification, and basic anti-collision capability. At the same time, differentiated special tests are set according to different application scenarios:

- **ISO/IEC 14443 (A/B)**: Focus on adding test items such as secure encrypted interaction, identity authentication, and card wake-up and sleep mechanisms to adapt to high-security scenarios including finance and government affairs, adapting to high-security requirement scenarios such as finance and government affairs. If such products connect to mobile NFC ecosystems and global payment networks, they can additionally apply for NFC Forum and EMVCo industry certifications.
- **ISO/IEC 15693**: Focus on group addressing command response and extended medium-distance communication timing, oriented toward large-scale item management scenarios.

Implementation Process:

1. Sample submission: Enterprises submit finished devices, chip samples, and product technical materials.
2. Laboratory testing: Complete tests item by item according to corresponding standards.
3. Problem rectification: Non-conforming items are re-submitted after the enterprise optimizes design/process.
4. Report issuance: Issue third-party test reports after passing testing.

Implementation Cycle:

Normal testing cycle is 2 to 5 working days. If security items and multi-device special retesting are involved, the cycle extends slightly.

4.1.1.3 LF RFID devices

LF RFID devices have typical operating frequency bands of 125 kHz and 134.2 kHz, widely used in niche scenarios such as animal identification, industrial anti-theft, and special industrial identification. The corresponding standards are divided into two major categories: general standards and industry-specific standards:

1. **General standards**: ISO/IEC 18000-2:2009 defines FDX and HDX—the two mainstream communication modes in this frequency band—adapting to general industrial identification and vehicle anti-theft scenarios.
2. **Industry-specific standards**: Mainly refer to ISO 11784:2024 and ISO 11785:2026 standards specifically for the global animal identification field. Many countries' livestock and pet import/export regulations mandate that products comply with these standard specifications.

Core Testing Items:

- **General devices:** Test communication modes, carrier parameters, data coding, command interaction, and reading/writing stability according to ISO/IEC 18047-2:2012.
- **Industry-specific animal identification devices:** Execute industry special tests according to ISO 11784:2024 and ISO 11785:2026 supporting test standards. In addition to basic protocol items, they focus on setting specialized test items such as ID coding format verification, data storage specifications, and living medium simulation for livestock application scenarios.

Implementation Process:

The implementation framework for general tests and special tests of LF RFID tags is basically the same, and the main difference lies in the internal laboratory testing phase. Animal identification devices additionally require strictly demanding special tests such as living medium simulation and multi-environment reliability, with more test items and higher judgment thresholds, resulting in a longer overall testing cycle.

1. Sample submission: Enterprises submit finished devices, chip samples, and product technical materials.
2. Laboratory testing: Complete tests item by item according to corresponding standards.
3. Problem rectification: Non-conforming items are re-submitted after the enterprise optimizes design/process.
4. Report issuance: Issue third-party test reports after passing testing.

Implementation Cycle:

Normal industrial device testing cycle is 2 to 4 working days. Animal identification special devices have a cycle of approximately 3 to 6 working days due to more stringent test items.

4.1.2 device Performance Testing and Certification

Device performance certification primarily conducts classification and admission evaluation of RFID device RF performance indicators, scenario adaptability, and reading/writing stability, serving as the core basis for evaluating the actual application effect. Affected by technical routes and the globalization degree of application scenarios, performance certification systems for different frequency band passive RFID devices vary significantly: UHF RFID has TIPP, ARC international certification and CQC certification. HF and LF RFID mainly rely on third-party testing and evaluation.

4.1.2.1 UHF RFID devices

UHF RFID performance systems are divided into four parts: general performance testing, TIPP certification, ARC certification, and CQC certification. General performance testing is the unified underlying technical foundation for the other three certification types. TIPP targets global all-category supply chain general selection. ARC focuses on North American head retail and logistics entry. CQC primarily serves China IoT project bidding and acceptance.

I. General Performance Testing

General performance testing is the basic testing form in the UHF RFID industry. Conducted according to ISO/IEC 18046-3:2020, this is the globally unified device performance underlying standard, specifically specifying testing environments, equipment configurations, test procedures, indicator calculations, and judgment rules. It applies to all manufacturer R&D self-testing, third-party laboratory routine testing, project acceptance, and is also the technical foundation for TIPP, ARC, and CQC certifications.

Core Testing Items:

Testing is conducted on RF performance and application performance. Core items mainly include: sensitivity threshold, extreme working capability, azimuth and attenuation characteristics, anti-interference capability, and reading/writing stability.

Implementation Process:

1. Sample submission: Enterprises submit finished devices, chip samples, and product technical materials.
2. Laboratory testing: Complete tests item by item according to corresponding standards.
3. Problem rectification: Non-conforming items are re-submitted after the enterprise optimizes design/process.
4. Report issuance: Issue third-party test reports after passing testing.

Implementation Cycle:

Normal testing cycle is 2 to 4 working days. Complex project retesting cycles extend slightly.

II. TIPP Certification

TIPP stands for tagged-Item Performance Protocol. Jointly built by GS1 (International Article Number Association) together with global retail, supply chain, and technology enterprises, it aims to solve industry problems of non-unified UHF RFID device performance standards and difficulty in cross-subject performance benchmarking among different manufacturers, establishing a globally universal, quantifiable device performance classification system. Currently, TIPP is widely adopted by many international brands, small and medium-sized retail enterprises, and system integrators. This certification conducts testing and classification based on unified international standards. GS1-authorized laboratories are located in many places globally, which significantly reduces submission thresholds and time costs for manufacturers worldwide.

TIPP certification is centered on standardized laboratory testing, conducting quantitative classification and evaluation around device basic RF performance and multi-scenario adaptability, outputting classified test reports and official filing certification. This certification uses a unified classification naming rule and judgment threshold, which has extremely strong universality, and is the mainstream reference for UHF RFID device performance benchmarking globally.

Core Testing Items:

Strictly conducted according to GS1-published TIPP testing methods. Core focus is on two modules: single device basic performance and multi-device stacking performance.

- **Single device classification testing (S series)**: Focuses on testing RF sensitivity, backscatter power, all-direction angle adaptability, and frequency band compatibility, verifying device comprehensive RF capability under normal single-item working conditions.
- **Multi-device stacking testing (M series)**: Simulates retail scenario 2-piece and 11-piece stacking conditions, testing batch reading rate under dense arrangement, anti-collision capability, stacking sensitivity, and backscatter stability.

Implementation Process:

1. **Data submission and preliminary confirmation**: Enterprises, based on their product application scenarios, select target TIPP performance levels and submit enterprise information, device technical parameters, product descriptions, and other materials to GS1-authorized laboratories. The laboratory completes

preliminary material review and confirms the testing plan.

2. **Sample mailing and sampling preparation**: Enterprises mail sufficient representative samples according to standards. The laboratory randomly samples for testing, avoiding result bias caused by manual sample selection and ensuring testing fairness.
3. **Standardized classification testing**: All-item testing is executed in standard shielded rooms, completing single-device posture/sensitivity/backscatter, multi-device stacking reading/writing, frequency band compatibility, and other items in sequence. Sample compliance with corresponding level indicators is judged. Complete testing data is recorded.
4. **Result judgment and report issuance**: After testing passes, the laboratory issues a test report with clear TIPP levels. If the target level is not reached, enterprises optimize products and resubmit for retesting.
5. **Official filing and information disclosure**: Enterprises can apply to have classification information recorded in the GS1 global TIPP system for official filing. After filing is completed, relevant level information is searchable on the GS1 platform, gaining globally universal classification credibility.

Implementation Cycle:

Normal full-process cycle is 3 to 6 weeks, primarily constrained by sample mailing and filing review. Testing execution itself is relatively quick due to high automation.

III. ARC Certification

ARC certification originated from the North American retail industry. In the early 21st century, leading US retailers such as Walmart, Macy's, and Target began comprehensively promoting UHF RFID product traceability and inventory management solutions. To solve difficulties in supplier entry and unified product quality management, the University of Arkansas led the creation of a set of device performance testing rules and entry standards closely matching retail real scenes. This was the prototype of ARC certification. Later, the laboratory moved to Auburn University. Due to its origin, current certification testing resources are highly concentrated at the Auburn University RFID Lab in the US.

ARC certification is overall divided into two parts: standard performance test items and custom test items, where custom test items are proposed by end customers. All testing is completed in ARC-dedicated standard test anechoic chambers. After all tests pass, reports are issued and included in the ARC global qualified list. This certification has unique test specifications for different customers, rigorous judgment standards, and is also the core entry requirement for North American head retail and logistics enterprises to select device suppliers.

Core Testing Items:

- **Standard performance test items**: Mainly conduct single-device multi-medium sensitivity, backscatter, angle adaptability, and full-frequency-band stability testing. Simultaneously simulate dense arrangement conditions, verifying multi-device anti-collision and batch reading capability, comprehensively examining device basic RF performance and general scenario adaptability.
- **Custom test items**: Proposed by end customers, mainly targeting jeans, plastic

bags, underwear, etc. devices are placed in different ways on or inside these items. Final requirements are to achieve certain indicators.

Implementation Process:

1. **Qualification and material preliminary review**: Enterprises first confirm exclusive test specifications corresponding to cooperative customers, fill out laboratory official application forms, and simultaneously submit enterprise information, product technical materials, device parameters, and other materials. The laboratory completes written material review.
2. **Sample mailing**: Mail sufficient representative samples according to standards. The laboratory removes obviously non-conforming samples and randomly samples, ensuring testing objectivity.
3. **Full-item sample performance testing**: Samples are sent to ARC standard test anechoic chambers, conducting single-device, multi-device, and other tests in sequence. Results are judged strictly according to corresponding indicator thresholds. All tests must pass before entering the next link.
4. **Comprehensive review, certification issuance, and list inclusion**: After all materials and sample tests pass, devices are entered into the ARC global public qualified list. Formal certification certificates are issued and publicly disclosed. Products obtain supplier qualification for head retail and logistics enterprises.

Implementation Cycle:

Full cycle is normally 8 to 16 weeks. If sample rectification, tight review scheduling, or cross-ocean logistics delays are involved, the cycle may extend to 20 weeks or more.

IV. CQC Certification

China Quality Certification Centre (CQC) launched UHF RFID device performance classification certification in 2015. This certification is conducted according to CQC9217-2015 supporting implementation rules, mainly serving China enterprise bidding, and IoT project acceptance.

Core Testing Items:

Complete RF performance testing including device sensitivity, reading/writing distance, multi-device reading, frequency band stability, and multi-medium adaptability.

Implementation Process:

1. **Data submission**: Enterprises submit product technical parameters and application scenario descriptions to CQC.
2. **Sample submission**: Mail representative samples to designated laboratories.
3. **Type testing**: Complete full-item performance testing and classification evaluation according to technical specifications.
4. **Result evaluation**: Classify performance levels based on test data and issue classified reports.
5. **Certification issuance and supervision**: Issue CQC mark certification certificates and conduct post-certification supervision.

Implementation Cycle:

China laboratory localized testing has streamlined processes, with a normal cycle of 2 to 4 weeks.

4.1.2.2 HF RFID devices

HF RFID devices are mainly divided into ISO/IEC 14443 and ISO/IEC 15693 two technical systems, widely used in scenarios such as access control, public transit, financial payment, archive management, and asset inspection. Differentiated testing content is divided according to the two mainstream application standards, mainly including general testing and special testing.

Core Testing Items:

- **General testing**: Includes RF basic working performance, reading/writing distance and stability, power consumption, and frequency response characteristics.
- **Special testing**: devices based on ISO/IEC 14443 standard, oriented toward high-security scenarios such as finance and government affairs, focus on encryption interaction, identity authentication, and security protection testing. devices based on ISO/IEC 15693 standard, mostly used for archive and asset batch management, focus on stacking reading, anti-interference, multi-device batch polling and concurrent reading, and group addressing performance testing.

Implementation Process:

1. Sample submission: Enterprises submit finished devices, chip samples, and supporting technical materials.
2. Laboratory testing: Complete performance testing and special testing item by item according to corresponding international standards.
3. Problem rectification: Resubmit after optimizing product design or production process for non-conforming items.
4. Report issuance: Third-party institutions issue performance test reports after passing testing, serving as product compliance and delivery basis.

Implementation Cycle:

Normal performance testing cycle is 2 to 5 working days. If security performance, multi-device concurrency, and other complex special retesting are involved, the testing cycle extends accordingly.

4.1.2.3 LF RFID devices

LF RFID devices have typical operating frequency bands of 125 kHz and 134.2 kHz. This frequency band is divided into two directions: general and animal identification special. Product market circulation uses third-party test reports as the main basis.

Core Testing Items:

General devices mainly include RF basic performance, reading/writing distance, signal penetration capability, anti-interference capability, high-low temperature environmental adaptability, and long-term static working stability.

Animal identification special devices additionally include multiple field living condition special tests for basic RF performance, focusing on biological tissue signal attenuation and living body movement adaptability. Simultaneously simulate complex environments such as subcutaneous tissue, mud/water soaking, and high-low temperature high humidity, verifying device aging resistance, corrosion resistance, and long-term reliable working capability.

Implementation Process:

The overall testing process framework is basically the same for general tags and special tags for animal identification:

1. Sample submission: Enterprises submit finished devices, chip samples, and product technical materials.
2. Laboratory testing: Complete full-item performance and special condition testing according to corresponding standards.
3. Problem rectification: Complete retesting after optimizing process or design for non-conforming items.
4. Report issuance: Issue third-party performance test reports after passing testing.

Implementation Cycle:

Normal industrial device testing cycle is 2 to 4 working days. Animal identification special devices have an overall cycle of approximately 3 to 6 working days due to more test items and strict condition simulation.

4.2 RFID device Production Line Testing Process and Quality Control Mechanism

With a segmented testing framework embedded throughout all production processes, standardized inspection methods and a sound quality control system, defective products can be quickly identified and isolated at every production node to effectively reduce production losses and guarantee product quality. This section systematically describes production line testing processes and quality control mechanisms from three dimensions: core objectives of device production line testing, full-process procedures, and special quality control requirements.

4.2.1 Core Objectives of device Production Line Testing

Combining passive RFID device production process characteristics, international protocol standards, and downstream diversified application scenarios such as retail, logistics, access control, and industry, production line testing sets six core management objectives around five dimensions: electrical performance, RF indicators, protocol function, appearance structure, and process management. These cover quality requirements from core components to finished products:

1. **Chip bonding quality verification**: Comprehensively detect chip and device antenna electrical connection status, investigate process defects such as cold solder joints, desoldering, open circuits, and short circuits, ensuring stable and reliable physical connection of core components.
2. **Antenna performance consistency control**: Strictly controlling same-batch device antenna parameter dispersion, avoiding RF performance unevenness caused by antenna differences.
3. **Conformance verification**: Verify device response capability to commands specified by international standards, ensuring protocol compatibility and that

devices can normally communicate with reader devices of different brands and models, achieving cross-device interconnection.

4. **RF indicator compliance**: Test the RF parameters of tags to ensure compliance with radio regulations and frequency band standards of target markets.
5. **Appearance and mechanical quality inspection**: Use visual inspection and physical verification to identify and eliminate appearance and structural non-conforming products such as printing defects, surface bubbles, film scratches, die-cutting offsets, corner damage, and overflow, ensuring product appearance and mechanical strength meet standards.
6. **Full-batch traceability**: Bind unique identification IDs to each device, associating production stations, times, raw materials, operators, and testing data, building a full-chain traceability system from chips and antennas to finished products.

4.2.2 Full-Process device Production Line Testing

Currently, the industry mainstream adopts the mode of segmented process testing plus finished product full inspection plus outbound sampling inspection. Corresponding detection processes are embedded at key process nodes such as antenna preparation, chip bonding, composite lamination, and die-cutting printing, following the principle of "early discovery, early isolation, and no transfer of non-conforming products." Basic quality control requirements are embedded within each production link. Complete production line testing is divided into six stages:

Stage 1: Incoming Quality Control

As the first quality gate of production, inspection is conducted on all raw and auxiliary materials used in device production, including chips, antenna base materials, laminating films, inks, and adhesives. Antenna base materials are tested for conductivity, material uniformity, and dimensional specifications. Auxiliary materials are verified for specifications, environmental indicators, and physical characteristics. All non-conforming inspection materials are directly returned to suppliers, strictly preventing entry into production processes.

Stage 2: Chip Bonding Testing

After chips are combined with antennas through flip-chip or welding processes, connectivity testing and basic communication testing are conducted. Key focus is on investigating bonding failures, chip offset, and poor contact.

Stage 3: Inlay Composite Testing

After device Inlay completes lamination and pressing, basic RF performance testing are conducted. Hidden faults such as delamination, bubbling, and pressing damage causing functional failure are investigated. This process is equipped with high-speed online testing and sorting equipment to realize automatic inspection of semi-finished products and marking of defective items. For products requiring data writing, online automatic encoding and code comparison verification are completed here to ensure the data is accurate, readable and writable.

Stage 4: Finished Product Printing and Die-Cutting Testing

After devices complete pattern, encoding printing, and finished die-cutting, simultaneous appearance visual inspection and dimensional verification are conducted. Focus is on dimension deviation, identifying printing errors, character defects, surface stains, die-cutting deformation, and corner damage, ensuring finished product appearance and marking compliance. For products requiring data writing, online automatic encoding and code value comparison verification are completed in this process, ensuring data accuracy and readability.

Stage 5: Final Quality Control

Before all finished products are packaged, 100% full-item testing is executed. Testing content includes all items such as protocol compatibility, reading/writing performance, RF indicators, and appearance status. This is the most critical quality control gate before product shipment.

Stage 6: Packaging and Outbound Quality Control

After product boxing and labeling are completed, reinspection is conducted according to industry sampling standards. In addition to sampling and testing device performance, packaging integrity, batch numbers, outer box markings, and transportation protection structures are simultaneously checked. Shipping is arranged only after all sampling tests pass.

4.2.3 device Production Line Special Quality Control Mechanisms

Combining RFID device chip electrostatic sensitivity, stringent production environment requirements, and long process chains, special quality control mechanisms are established on top of routine testing processes to avoid various quality risks during production:

1. **ESD Protection Control**

Passive RFID chips are highly susceptible to electrostatic discharge. Exclusive ESD protection areas are designated throughout the production area. Operators must wear anti-static wristbands and anti-static work clothes. Production equipment, workbenches, and material transfer containers are all reliably grounded. ESD protection facilities are regularly inspected and tested for effectiveness, preventing permanent damage or hidden failure of chips caused by ESD.

2. **Temperature and Humidity Control**

Workshop temperature and humidity are strictly controlled using constant temperature and humidity systems. This prevents antenna oxidation and lamination bulging caused by excessive humidity, while also preventing chip bonding accuracy and device electrical performance degradation caused by large temperature and humidity fluctuations.

3. **Production Equipment Management**

Establish daily equipment inspection, regular calibration, and maintenance records. RF testing instruments, bonding equipment, and visual inspection equipment perform self-check at daily startup, with periodic calibration using standard samples to ensure test data accuracy and stable process parameters.

4. **Process Change Management**

For change behaviors such as raw material replacement, production process adjustment, and equipment parameter modification, implement application, verification, approval, and trial operation management processes. After changes, small-batch trial production testing is conducted first. After confirming no product quality abnormalities, comprehensive implementation follows.

5. **Full-Batch Traceability Management**

Relying on unique device IDs to connect full-process production data, complete records are maintained for each batch's raw material batches, production stations, processing times, testing results, and operators. When quality problems occur, problem links and impact ranges can be quickly located.

6. **Non-Conforming Product Management**

Non-conforming products detected at each process are classified, marked, and stored separately, distinguishing types such as process defects, functional defects, and appearance defects. Regular statistical analysis of non-conforming products is conducted. Root causes are reviewed and processes are optimized, forming a closed loop of "testing-analysis-improvement."

4.3 RFID Chip Production Line Testing Process and Quality Control Mechanism

RFID chips are core semiconductor components of passive RFID devices, with manufacturing processes, testing precision, and quality standards far exceeding those of device finished products. Chip RF performance, logic function, stability, and service life directly determine comprehensive performance of devices. Compared with device assembly production lines, chip production line testing systems are more complex with stricter quality control requirements. Affected by the semiconductor industry vertical division of labor model, incoming material control and testing processes differ significantly from device production lines. This section mainly introduces chip production line testing core objectives, full-process procedures, and special quality control requirements.

4.3.1 Core Objectives of Chip Production Line Testing

Production line testing works around five directions: function verification, parameter consistency verification, defect screening, reliability verification, and performance classification. It comprehensively ensures mass-produced chip quality and scenario adaptability:

1. **Full-function verification**: Conduct item-by-item testing of all circuit modules inside chips such as RF circuits, logic operation units, data storage modules, and command response units. Investigate manufacturing defects such as circuit open circuits, logic errors, and command response abnormalities, ensuring all chip functions operate normally.
2. **Performance parameter consistency verification**: Strictly verify key parameters such as RF sensitivity, communication timing, frequency characteristics, power consumption, and command response speed. Strictly control same-batch chip parameter dispersion, ensuring batch product performance consistency.

3. **Manufacturing defect screening**: Relying on professional high-precision testing equipment, detect hidden damage and circuit abnormalities generated during wafer fabrication, cutting, and packaging processes. Completely eliminate non-conforming chips, preventing defective products from entering downstream processes.
4. **Reliability verification**: Through high-low temperature cycling, damp heat aging, mechanical vibration, ESD impact, and long-term powered aging tests, simulate complex working condition environments, ensuring chips can achieve long-term stable operation.
5. **Performance classification screening**: Classify qualified chips into performance grades according to parameters such as RF sensitivity, reading/writing capability, and power consumption. Different grade chips are matched to differentiated application scenarios, achieving precise product matching and value maximization.

4.3.2 Full-Process Chip Production Line Testing

RFID chip testing runs through the entire lifecycle of chip R&D to finished product shipment, adopting progressive screening and layer-by-layer verification modes, embedding quality requirements into each process:

Stage 1: Incoming Material Inspection

As the first quality gate of chip production, upstream semiconductor manufacturers have already completed wafer-level full-parameter testing. This production line does not repeat full-function retesting. This link only verifies material appearance, dimensions, packaging, and batch information, with sampling retesting of material purity, microstructure, and basic electrical characteristics. Incoming materials failing inspection are directly returned to suppliers, prohibited from entering production processes, avoiding raw material quality risks from the source.

Stage 2: Design Verification and Wafer Test

This link belongs to pre-production R&D verification stage. Comprehensive testing is conducted on chip prototype samples, focusing on verifying circuit design logic, protocol compatibility, and basic RF performance. Design defects are identified early and circuit parameters are optimized. All testing data is completely retained. After design problems are rectified and retesting passes, mass production wafer fabrication begins. Throughout wafer fabrication, online systems are relied upon for real-time monitoring of equipment parameters and environmental status. Process deviations immediately trigger machine stoppage and adjustment.

Stage 3: Wafer-Level Testing

This process is the first critical quality control gate for chips. After entire wafers complete fabrication processes, each bare die on the wafer is tested with power-on detection using probe equipment. Bare die electrical parameters, RF indicators, and basic functions are checked, and non-conforming bare dice are marked on the wafer surface. Non-conforming bare dice are precisely marked and records are established. Good and non-conforming areas are strictly divided, prohibiting defective bare dice from entering the cutting process. Testing equipment performs daily self-check and regular precision calibration, ensuring test data accuracy.

Stage 4: Chip Cutting and Sorting

Completed wafer-tested entire wafers are cut into individual bare dice. Marked non-conforming products are eliminated based on wafer testing data. Simultaneously, initial performance classification of qualified bare dice is completed based on measured performance parameters. Different grade dice are clearly marked and stored by grade, completely preventing mixing issues. Simultaneously eliminate appearance and structural non-conforming products caused by cutting processes. Non-conforming product types are classified for process optimization.

Stage 5: Packaging Testing

After bare dice are packaged, full-item functional and performance retesting is conducted after packaging. Key focus is on investigating pin contact poor, circuit damage, and signal attenuation problems caused during packaging.

Stage 6: Reliability Testing

Samples are extracted according to semiconductor industry sampling standards. Reliability tests such as high-low temperature cycling, damp heat aging, mechanical vibration, ESD impact, and long-term powered aging are conducted. If sample testing fails, corresponding batch flow is immediately suspended. Problem roots are comprehensively investigated and rectified. Production continues only after retesting passes.

Stage 7: Factory Testing and Batch Sampling

Before packaged chip products are packed, 100% full-item final testing is executed. Functional status, performance parameters, and classification results are comprehensively verified. Final sorting and isolation are completed, strictly controlling finished product quality. Before product shipment, secondary outbound sampling inspection is conducted according to industry sampling rules. Batch information, product specifications, testing reports, and packaging integrity are checked. Simultaneously, full-process testing records are organized to meet customer traceability requirements.

4.3.3 Chip Production Line Special Quality Control Mechanisms

Beyond procedural testing and basic quality control, four special management mechanisms are established combining RFID chip manufacturing processes, high reliability requirements, and semiconductor workshop production characteristics, further strengthening full-process quality assurance:

1. **Cleanroom Control**

Core processes such as chip wafer fabrication, wafer testing, and packaging are conducted in high-grade cleanrooms. Airborne dust and particulate matter concentrations are strictly controlled. Personnel entry/exit procedures, dress standards, and operating behaviors are standardized to prevent fatal defects such as dust causing circuit short circuits and pin contamination. Temperature and humidity and air pressure regulation systems are linked to maintain long-term stable workshop environmental parameters.

2. **Nanometer-Level Precision Control**

Chip manufacturing is nanometer-scale precision processing. All production equipment and high-precision testing instruments implement periodic calibration systems. Micron to nanometer-level control is implemented for key process parameters such as displacement, pressure, and timing for critical processes such as lithography, etching, probe contact, and bonding, ensuring processing and testing precision meet design standards.

3. **Failure Analysis Mechanism**

Professional failure analysis laboratories are built. For non-conforming chips detected on production lines and reliability test failure samples, techniques such as microscopic observation, circuit analysis, and signal testing are used to locate failure root causes. Chip design, production processes, and testing plans are inversely optimized based on analysis results, forming closed-loop management of "testing-analysis-optimization," continuously reducing product defect rates.

4. **Full-Lifecycle Data Traceability**

Unique identity codes are established for each wafer and each chip. Full records are maintained of wafer fabrication batches, process parameters, testing data at each stage, classification results, and warehouse flow information. Full-lifecycle data traceability from design and manufacturing to testing and device application is achieved, meeting stringent semiconductor industry quality traceability requirements.

4.4 Analysis of Pain Points in Ambient IoT device Testing and Certification

Currently, Ambient IoT devices have multi-dimensional industry pain points in testing and certification, concentrated in areas such as standard systems, certification mechanisms, testing methods, application adaptation, equipment costs, and supply chain management:

1. **Incomplete Testing and Certification System**

At present, there is no unified testing and certification system in the passive IoT device industry, which restricts the standardized development of the sector. When supplying the same product to different downstream clients, enterprises have to repeatedly conduct customized tests, driving up costs and resulting in wasted testing resources. While two major performance certification systems, TIPP and ARC, have been established for UHF RFID devices, they operate independently with limited industry openness. The whole industry lacks unified evaluation specifications. Equipment manufacturers, device producers and testing institutions mostly adopt self-developed testing methods and judgment criteria, leading to incompatible test data and great difficulties in the mutual recognition of test results across organizations.

2. **High Redundancy in Testing Modes**

Existing industry testing systems have not achieved split testing between chip inherent performance attributes and additional performance changes brought by antennas and device structures. The general mode of complete repeated testing of finished products is uniformly adopted. When the same chip model is paired with different antennas, laminating materials, or finished product sizes, complete protocol, RF, and performance testing must be repeated. Massive repeated testing continuously raises enterprise testing costs and industrialization deployment thresholds.

3. **High Threshold for High-End Testing Capability**

The procurement and operation & maintenance costs of high-precision RFID testing systems are high. Professional testing capabilities are mainly concentrated among leading manufacturers and a small number of authorized laboratories. Most small and medium-sized enterprises lack the capacity to conduct key tests such as sensitivity, frequency stability and multi-device anti-collision, resulting in deficiencies in product R&D verification and factory quality control.

4. **Lack of Chip Quality Evaluation System**

Chips are core to determining device performance. Currently, there is a lack of unified performance classification and quality certification standards. Chips from different manufacturers and different batches vary significantly. Without authoritative and uniform criteria for model selection and incoming inspection, downstream device manufacturers face greater pressure in testing and quality control.

5. **New device Certification Specification Gaps**

For new-generation low-power, novel passive IoT products such as Ambient IoT devices, no supporting systematic standards have been formed globally. Unified device performance testing methods, complex scenario evaluation indicators, and tiered certification systems are lacking, severely constraining large-scale commercial deployment of novel passive devices.

6. **Lack of Security Performance Testing Specifications**

Financial payment, government affairs documents, and confidential asset devices have stringent security performance requirements for encryption mechanisms, tampering prevention, and cracking prevention. However, mainstream RFID certification systems currently focus primarily on basic communication and RF performance tests, with inadequate coverage of security aspects. Meanwhile, international security certification for RFID also remains underdeveloped.

5 Ambient IoT Testing and Certification System Construction Research

5.1 Ambient IoT Technical Characteristics and Ecosystem Needs

5.1.1 Definition

Ambient IoT is a next-generation IoT technology standard system continuously promoted by 3GPP during Release 18 to Release 20, aimed at providing cellular network connectivity for passive or micro-energy devices, opening the next phase of the Internet of Everything. According to 3GPP's official definition, an Ambient IoT device device is an IoT device powered by energy harvesting, not carrying batteries or only having limited energy storage capability (for example, using capacitors). Device complexity is low, size is small, capability is limited, and power consumption is significantly lower than IoT devices such as NB-IoT/eMTC previously defined by 3GPP. An Ambient IoT network device is an extension of traditional cellular mobile communication network capabilities. By introducing core capabilities such as backscatter signal demodulation, RF energy radiation control, and low-complexity device access management at the base station, relying on existing resources of public cellular networks, wide-area coverage and large-scale access of Ambient IoT devices can be achieved.

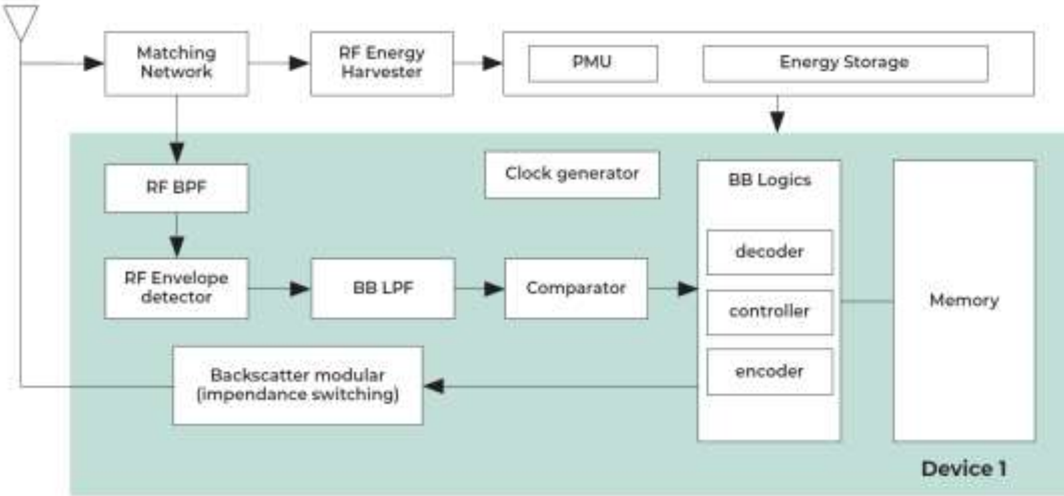

Figure 5-1 The Architecture of Ambient IoT Device 1 in 3GPP

Ambient IoT Device Architecture

From a broader technical paradigm perspective, the core of Ambient IoT lies in enabling IoT devices to operate without depending on traditional battery power. Instead, they harvest weak energy from the environment (such as environmental RF signals, thermal energy, vibration, or energy supplied by dedicated supply nodes) to support their operation, using backscatter communication mode for data transmission. Correspondingly, cellular base stations need to simultaneously assume dual functions of downlink excitation source and uplink signal receiver—downlink provides harvestable environmental RF energy and excitation signals needed for backscatter communication to devices. Uplink needs to achieve high-sensitivity detection, demodulation, and decoding of weak modulated signals backscattered from devices. To support massive concurrent access of passive devices, the network side needs to design targeted multiple access mechanisms, collision avoidance algorithms, and lightweight connection management processes, while remaining compatible with existing 5G network architecture. This technical architecture, with essential characteristics of ultra-low power consumption, passive operation, and ubiquitous connectivity, aims to connect massive "dumb devices" that traditional IoT technologies struggle to cover, providing massive data support for digital twins and the intelligent world.

3GPP, in Release 18, completed preliminary analysis of Ambient IoT use cases, deployment scenarios, traffic characteristics, device constraints, service requirements, and key performance indicators through working groups SA1 and TSG-RAN, simultaneously conducting feasibility research on network deployment architecture, base station RF indicators, and core network adaptation plans, clarifying basic network-side capability requirements for supporting backscatter communication. Release 19 standardized version "Device 1" was formally frozen in December 2025, simultaneously solidifying network-side technical specifications such as base station physical layer reception algorithms, multi-user scheduling mechanisms, and random access procedure optimization. Release 20 further advances toward wide-area scenarios, with standard freezing expected in the first half of 2027.

5.1.2 Core Characteristics

(1) Passive Operation and Energy Harvesting

The core characteristic of Ambient IoT is that devices do not require traditional batteries but instead harvest energy from the environment (including natural energy—solar, thermal, and vibrational; auxiliary energy—environmental RF signals; and directional energy supplied by dedicated supply nodes) to drive operation. Devices primarily use backscatter as the communication method—that is, passively modulate external reader-provided carriers through simple circuits, "reflecting" information back to the network, rather than actively generating RF signal transmissions, thus almost consuming no own energy. According to 3GPP definition, Ambient IoT devices contain no active RF transmitting components internally. Device-to-reader transmission is completed by passively modulating external RF carriers, relying only on stored small amounts of energy for short-term power supply.

(2) Ultra-Low Power Consumption and Ultra-Low Cost

According to 3GPP TR 38.769 clause 3.1, peak power consumption target for Ambient IoT Device 1 is as low as approximately 1 microwatt (μW), multiple orders of magnitude lower than existing low-power wide-area network technologies such as NB-IoT. To achieve this goal, devices use extremely simple designs: the receiver is only a simple envelope detector that can only sense overall signal power changes without decoding complex OFDM signals. Uplink transmission uses extremely simple modulation methods such as OOK or binary phase-shift keying (BPSK), canceling complex processing links in traditional communication protocols such as scrambling, interleaving, MIMO, independent control channels, and L1 layer HARQ. Simple components with wide manufacturing tolerances and insensitivity to environmental changes can be used, achieving extremely low device costs and paving the way for large-scale deployment.

(3) Long Life and Maintenance-Free

Because battery replacement or charging is unnecessary, Ambient IoT devices can achieve ultra-long service life exceeding 10 years, with no need for manual intervention during operation. This characteristic enables devices to be deployed in harsh environments where battery replacement is extremely difficult or even infeasible (such as high temperature, high humidity, high pressure, and enclosed spaces), or embedded in disposable consumer application scenarios including building materials and product packaging.

(4) Cellular-Level Coverage

Relying on licensed spectrum and cellular base station power advantages, Ambient IoT achieves coverage ranges far exceeding traditional passive RFID technology. At the base station side, large-power transmission on licensed spectrum combined with multi-device joint power supply technology significantly enhances coverage. At the device side, advanced coding and efficient modulation waveforms further extend coverage distance. Through flexible scheduling and joint demodulation technology, distributed joint reception is implemented, effectively solving interference problems and achieving continuous networking coverage. This combination of technologies gives Ambient IoT coverage 3 to 5 times that of RFID technology, and it continues to improve.

In physical layer design, for complex environments (large spaces, high ceilings, dense cargo stacking, severe signal blocking), Ambient IoT integrates 5G distributed MIMO technology, significantly enhancing penetration capability and ensuring reliability of indoor-outdoor continuous coverage.

(5) Cellular Identity Based on Licensed Spectrum and High Reliability

Unlike non-licensed spectrum technologies such as Wi-Fi and Bluetooth, Ambient IoT operates based on operator-licensed spectrum, possessing the following unique advantages: devices have identity authentication capability, supporting device discovery and authentication protocols; inventory accuracy can reach over 99.9% through multi-Pico RRU joint reception, polling inventory, and air interface enhancement technologies; supports quasi-positioning functions (field-strength positioning plus fingerprint positioning can achieve meter-level accuracy, triangular field-strength positioning meets fast item-finding needs), and provides higher connection reliability than traditional RFID.

(6) Multi-Scenario Flexible device System

3GPP defines three device types to adapt to different value scenarios: Device 1 type devices adapt to indoor and low-value scenarios; Device 2b type devices are used for scenarios requiring wide coverage; Device C type devices focus on outdoor high-value scenarios, providing a flexible device selection system for diverse application needs.

Among them, Device 1 type device specifications were completed in Release 19. Technical research and specification development for Device 2b and Device C type devices will be conducted in Release 20.

5.1.3 Typical Scenarios

(1) Smart Warehousing and Indoor Asset Management

This is the representative use case focused on by 3GPP Release 19 standardization (rUC1: indoor item inventory; rUC4: indoor command delivery). Ambient IoT can real-time track warehouse cargo location and status, achieving fully automated inventory and full-lifecycle management from large pallets to individual items. In practical verification, the "one-code-through" solution based on 5G-A Ambient IoT achieved 100% inventory accuracy in a certain manufacturing factory pilot, reducing inventory cycles from monthly to half a day, achieving full-process visibility and controllability from production to delivery. Indoor inventory and asset management is the first breakthrough for Ambient IoT commercial deployment.

(2) Logistics Tracking and Supply Chain Visualization

Ambient IoT uses passive identification to achieve "one-code-through" for goods, supporting full-process traceable logistics trajectories and real-time visible status, significantly improving supply chain circulation efficiency and digital management capability. Unlike traditional passive RFID, which can only read data at specific scanning points, Ambient IoT can provide continuous data visibility throughout the entire chain of transportation, storage, loading/unloading, and inventory—including environmental sensor data (temperature, humidity, vibration, etc.)—providing underlying data support for supply chain digital twins.

(3) Environmental Monitoring and Ubiquitous Sensing

Ambient IoT can be deployed in key industries such as electric power, healthcare, agriculture, and security to achieve real-time passive data return of various sensor data such as temperature, humidity, gas leakage, and security protection. For example, in cold chain logistics, tracking food/vaccine temperature changes throughout the process can effectively prevent losses caused by temperature overruns. In medical scenarios, base station modules can simultaneously support IoT and communication services, achieving integrated applications for asset, consumable, and patient management.

(4) Industrial Inventory and Manufacturing Full-Factor Networking

In industrial manufacturing scenarios, large numbers of "dumb devices" such as raw materials, production tools, valuable assets, and returnable containers have historically been difficult to obtain real-time data on. Ambient IoT provides automated, ultra-low-power, maintenance-free IoT solutions, achieving automated inventory of production lines and real-time material management, effectively reducing material shordevicees and improving production efficiency.

(5) Item Traceability and Asset Management

Ambient IoT can be attached to various items for asset positioning and management at home or enterprise levels, including finding household items, valuable asset tracking, and equipment maintenance reminders. In wide-area scenarios, asset management, logistics tracking, and person-finding functions will gradually achieve full indoor-outdoor visibility and management with the advancement of Release 20 standards.

(6) Smart Transportation and Smart Cities

With Release 20's advancement toward wide-area scenarios, Ambient IoT is expected to play important roles in smart transportation and smart city fields, including municipal facility monitoring, traffic sign networking, and road-side infrastructure status sensing. As of June 2026, equipment manufacturers and multiple operators have implemented smart warehousing, industrial manufacturing, office parks, commercial retail, and other industry showcases based on 5G-A Ambient IoT solutions, with technical feasibility and industry value having been adequately verified.

(7) Smart Elderly Care and Elderly Care Facility Refined Management

Smart elderly care is one of the core vertical scenarios for Ambient IoT oriented toward livelihood services, adapting to diverse needs of elderly care facility indoor-outdoor comprehensive management. Cellular Ambient IoT technology, relying on maintenance-free, wide-coverage, and lightweight core advantage, can achieve full-domain digital management of elderly care facility personnel and assets. After equipping elderly with passive identity devices, relying on cellular network continuous coverage capability, indoor-outdoor activity trajectory tracking, restricted area boundary early warning, and rapid positioning can be achieved, effectively reducing elderly wandering risks. devices are small and require no power supply, can be stably worn long-term, significantly reducing maintenance workload and equipment damage costs. For mobile assets such as wheelchairs, rehabilitation equipment, and nursing equipment within facilities, Ambient IoT can achieve automated inventory and real-time location management, improving asset turnover efficiency and utilization. After passive identification of medicines and medical consumables, full-process traceability and automated inventory can be completed, reducing human errors and ensuring the compliance and safety of material management. Combined with passive environmental sensing devices, normalized passive monitoring of ward temperature and humidity and bed status can be achieved. With extremely low deployment and maintenance costs, this helps elderly care facilities build a smart elderly care service system with full-domain sensing and efficient management.

(8) Generalized Public Services and ToC Applications

Ambient IoT can also expand to broader public service and consumer-grade application scenarios, including but not limited to: soil/climate sensors in smart agriculture, building structural health monitoring, public facility asset inventory, and identity identification in wearable consumer products. As the industry chain matures and costs continue to decline, generalized public services and ToC applications will show vast growth space in the mid-to-long term.

5.2 Necessity of Ambient IoT Certification System Construction

5.2.1 Ensuring Interoperability and Compatibility of Ambient IoT

The Ambient IoT industry chain involves multiple types of entities such as chip design, device manufacturing, base station equipment, core network functions (AIOTF), and application platforms. Since 3GPP standards only define protocol frameworks and interface specifications without mandating specific implementation methods (for example: energy harvesting circuit design, backscatter modulation parameters, slot ALOHA access algorithms, and device identification coding rules), A-IoT devices produced by different manufacturers may have compatibility defects when accessing the same operator network, such as:

- **Power supply and wake-up mismatch**: Some devices' energy harvesting circuits have inconsistent sensitivity to base station downlink square wave OOK modulation, causing certain devices to fail normal wake-up.
- **Backscatter signal mutual interference**: devices from different manufacturers have differences in reflected modulation waveforms within the same time slots, possibly causing base station demodulation failure and reduced inventory accuracy.
- **Identification resolution conflicts**: If TS 23.003/23.369 specified permanent

AIoT device identification structures are not uniformly followed, device identity duplication or resolution errors may occur during cross-platform data exchange.

The certification system can formulate conformance testing specifications to conduct standardized verification of devices at key links such as the physical layer (modulation/demodulation and backscatter), MAC layer (wireless signaling interaction and data packet format), network layer (NAS signaling interaction and AIOTF registration process), and identification coding format, ensuring that any certified A-IoT device can normally complete device discovery, authorization, inventory, and command delivery in RAN equipment and core network environments from different manufacturers. This not only reduces operators' multi-vendor procurement integration risks but also provides device users with "plug-and-play" procurement convenience. It is the cornerstone of Ambient IoT moving from closed single-vendor solutions toward an open industry ecosystem.

5.2.2 Improving device Stability and Reliability in Real Complex Environments

Although 3GPP standards define a series of performance indicators (such as inventory accuracy ≥99.9%, coverage distance >100 meters, device peak power consumption ~1μW), these indicators are typically measured under ideal channel models (such as AWGN and indoor static line-of-sight). In actual deployment, Ambient IoT devices face challenges far exceeding laboratory environments:

- **Complex electromagnetic environment**: Dense cargo stacking in smart warehouses, metal shelf reflections, and multi-base-station signal superposition cause uneven distribution of power supply carrier field strength, with "energy voids" forming in some areas.
- **Multi-user strong interference**: In factory inventory scenarios, hundreds or even thousands of A-IoT devices simultaneously respond to base station polling. Backscatter signals are extremely weak (typically 20 to 30 dB lower than ambient noise), prone to collision and packet loss.
- **Energy harvesting fluctuations**: When indoor natural light is insufficient or devices are blocked, devices relying on solar or environmental RF harvesting may experience intermittent power loss, causing discontinuous reported data or device disconnection.
- **Extreme environmental stress**: Low temperatures in cold chain logistics, high humidity/sand in outdoor asset tracking, and high vibration in industrial production lines may accelerate aging of device internal capacitors or antenna matching circuit drift.

The certification system can design scenario-driven reliability test suites, including but not limited to:

Test Dimension	Specific Content	Aligned Typical Scenarios
Power supply	Dynamic field strength range (-28 dBm ~ -4	Warehouse shelf

robustness	dBm), energy interruption recovery time	shadow areas, container interiors
Anti-interference capability	Same-frequency multi-device concurrency (≥100 devices), adjacent-frequency base station interference	Large-scale industrial inventory, logistics sorting centers
Environmental adaptability	Temperature-humidity cycling (-25°C~70°C, RH 95%), salt spray/dust protection	Cold chain transportation, outdoor municipal facilities
Mechanical reliability	Drop, vibration (ISTA 3A standard compliant)	Express package sorting, vehicle mobile tracking

Certified devices can obtain clear applicable scenario classification marks (such as Type 1 Indoor General / Type 2 Industrial Enhanced / Type 3 Outdoor Wide-Area). Application parties can select products of appropriate classification based on deployment environments, avoiding asset missed inventory, data errors, or maintenance cost surges caused by device failures. This is particularly critical for scenarios requiring extremely high continuity such as logistics tracking, industrial automation, and public infrastructure monitoring.

5.2.3 Establishing Industry Trust Mechanisms, Providing Reliable Certification Endorsements for Governments, Enterprises, and Financial Institutions

Ambient IoT, as an emerging technology integrating cellular communication and passive sensing, is in the early stage of technology dividend release and commercial deployment acceleration. However, due to the lack of authoritative third-party certification systems, the market has the following trust deficits:

- **Performance falsification chaos**: Some manufacturers exaggerate their products' coverage distance, inventory speed, etc., making it difficult for users to distinguish.
- **Security compliance blind spots**: A-IoT devices access core networks through licensed spectrum, but their identity authentication, data encryption, and privacy protection mechanisms, if not strictly audited, may become network security weak points.
- **Investment and financing barriers**: When financial institutions and insurance companies conduct risk assessment or credit extension for IoT projects, they lack quantifiable product reliability bases, often requiring additional collateral or increasing insurance premiums, raising technology promotion costs.

Establishing an Ambient IoT certification system led by government guidance and industry associations or third-party testing institutions can achieve the following multiple values:

1. **Providing technical tools for government regulation**: The Ministry of Industry

and Information Technology and other departments can, based on certification results, incorporate Ambient IoT into radio transmission equipment type approval, network access licensing, and other management systems, ensuring legal and compliant industry development.

2. **Reducing enterprise selection decision costs**: Operators, system integrators, and end users can directly trust certification reports, avoiding repeated testing and shortening procurement cycles.
3. **Outputting credit anchors for financial institutions**: Certified devices and solutions can serve as quality asset targets, supporting innovation in movable property pledge, insurance actuarial science, and supply chain finance based on IoT data. For example, certified cold chain devices can be incorporated into inventory financing sensor data verification systems.
4. **Building international mutual recognition bridges**: If the Ambient IoT testing and certification system led by GTI can achieve mutual recognition with the Global Certification Forum (GCF) or other regional certification systems, it will help the Ambient IoT industry quickly establish a healthy industry ecological environment globally.

Additionally, the testing and certification system can issue different security-level certificates, providing differentiated trust guarantees for high-value asset tracking (such as medical equipment and luxury logistics).

Ultimately, testing and certification will become a critical milestone for the Ambient IoT industry to move from "available" to "trustworthy."

Constructing an Ambient IoT certification system is not only a natural extension after technology standards are implemented but also a systematic solution to the three core pain points of current industry fragmentation, scenario adaptation difficulty, and market trust deficit. It unblocks industry chain bottlenecks through interoperability testing, improves product survival capability in real environments through scenario reliability evaluation, and builds a mutually trusted industry ecological foundation for governments, enterprises, and financial institutions through third-party authoritative endorsement. With the freezing of 3GPP Release 19 standards and commercial launch in 2026, certification system construction work urgently needs to start synchronously with standardization progress, escorting large-scale deployment of Ambient IoT in smart logistics, Industry 4.0, and digital twin city fields.

5.3 Ambient IoT Certification System Framework Design

Against the backdrop of gradual maturation of 3GPP Ambient IoT standards (Release 19 was frozen in December 2025, covering RF/RRM/signaling protocol and other dimensions. A-IoT testing and certification system construction was fully launched at the end of 2025. Core specification frameworks were all completed by March 2026. Full-series five testing specifications are expected to be officially released in December 2026), constructing a systematic, implementable, and operable certification system framework is a critical bridge connecting technical standards and industry large-scale application. The framework design is expanded below from four aspects: core concepts, certification levels, certification processes, and technical support platforms.

5.3.1 Core Concepts

The certification system construction follows four core concepts: "Open, Universal, Scalable, and Verifiable."

5.3.1.1 Open

The certification system is open to all industry chain participants. Equipment manufacturers, chip designers, module suppliers, and system integrators can all apply for certification equally. Certification standards, test case libraries, and certification results are publicly disclosed to society. Simultaneously,competition and capability mutual recognition among laboratories are encouraged, preventing single certification institutions from forming monopoly barriers.

5.3.1.2 Universal

Certification testing methods and judgment criteria are not limited to specific manufacturers' implementation solutions but use 3GPP standards and industry specifications as unified benchmarks. Test case design pursues universality. One set of testing procedures applies to multiple device architectures (Device 1, Device 2b and Device C three-device system) and multiple deployment topologies, fundamentally reducing repeated testing costs across supply chain links.

5.3.1.3 Scalable

The certification system must have dynamic iteration capability. As 3GPP standards continuously evolve (from Release 19 focusing on indoor inventory scenarios to Release 20 expanding toward wide-area scenarios), and new application scenarios (such as smart transportation and smart cities) propose new differentiated needs for certification, certification levels, test items, and judgment criteria are all designed as pluggable and scalable modular structures. New scenario certification capabilities can be quickly launched online.

5.3.1.4 Verifiable

All certification results must be independently verifiable through records, retesting, and reviews. Certification processes leave complete traces. Key testing data is traceable and auditable. Testing conclusions should have uniqueness, reproducibility, and objective fairness, ensuring the public credibility of the certification system.

5.3.2 Certification Levels

The certification system, following the logic from basic to complex, from single unit to system, and from ideal environment to real scenarios, is divided into the following five certification levels.

5.3.2.1 Basic Function Certification

Basic function certification is an assessment of A-IoT devices' most basic network access capability, ensuring devices meet minimum functional requirements defined by 3GPP standards. According to 3GPP regulations, A-IoT devices in the Rel-19 phase focus on Device 1 type, with peak power consumption approximately 1 microwatt, equipped with energy storage units (capacitors) and RF envelope detection receivers. D2R transmission depends on external-provided carriers for backscatter. devices contain no active RF transmitting components internally. Basic function certification core content includes:

- **RF basic parameter testing**: According to 3GPP TS 38.191 related sections, testing core RF indicators such as device transmission power control accuracy, frequency error limits, spurious emission levels, occupied bandwidth, and adjacent channel leakage ratio. All indicators must comply with limits published by national radio management authorities and 3GPP-standardized A-IoT device RF conformance requirements. A-IoT device receivers are extremely simple envelope detectors, capable only of sensing overall signal power changes without decoding complex OFDM signals.
- **Modulation/demodulation capability testing**: Verifying device demodulation correctness for downlink square wave OOK modulation, uplink backscatter modulation waveform quality (EVM and Manchester coding accuracy), and initial sampling frequency offset compensation capability. Synchronous testing of device wake-up response time from sleep (from receiving power supply signal to first response must meet time window requirements defined by 3GPP) and energy storage unit (capacitor) working capability maintenance after energy interruption.
- **Protocol compatibility testing**: According to specifications such as 3GPP TS 38.300, verifying compatibility of protocol layer functions such as device discovery procedures, NAS signaling interaction, and AIOTF registration processes. Confirming device identification format complies with permanent A-IoT device identification structure specified by 3GPP (Part 1 Network ID + Part 2 EPC format information), and responses to inventory commands and downlink commands comply with protocol interaction timing requirements.

This level is the threshold link of the certification system. devices not passing basic function certification do not enter subsequent certification levels.

5.3.2.2 General Compatibility and Interoperability Certification

The Ambient IoT industry ecosystem involves multiple suppliers such as chips, devices, base stations, core network AIOTF, and application platforms. General compatibility and interoperability certification aims to ensure devices from different manufacturers can work together, breaking "silo-style" closed ecosystems. GCF certification experience shows that interoperability testing (IOT) can effectively verify correct operation of key interfaces inside devices and between devices and mobile networks. In the Ambient IoT scenario, core testing at this level includes:

- **Multi-vendor base station linkage capability testing**: Mixing Device 1, Device 2, and Device C three-device types (adapting to different scenarios such as indoor/low-value, wide coverage, and outdoor high-value) with multi-vendor base station and core network equipment for networking, verifying inventory accuracy, coverage continuity, and communication stability. Particularly need to verify correct demodulation of device backscatter signals under cross-vendor infrastructure, ensuring devices of different chip solutions can coexist in the same network.

- **Cross-platform protocol adaptability testing**: Verifying A-IoT device access success rate and service continuity under different network configurations (different AMF/SMF deployment solutions and different AIOTF implementation versions). Simultaneously testing device identity re-authentication and session migration capability in inter-operator roaming scenarios, ensuring device identifiers and authentication credentials can be correctly recognized between different core networks.
- **Stable identification capability testing under multi-reader environments**: Under scenarios with multiple deployed base stations, testing reader anti-collision mechanism execution efficiency, including core indicators such as algorithm slot allocation rationality, frequency switching agility, and spatial resource utilization. Through signal processing methods such as interleaved multiple access, verifying capability of multi-reader joint deployment to detect device signals and network capacity. Testing needs to cover extreme conditions such as large numbers of devices responding concurrently (≥100 devices), adjacent-frequency base station interference, and same-frequency multi-base-station overlapping coverage.

5.3.2.3 Environmental Adaptability Certification

In real application scenarios, Ambient IoT devices face physical environments far more complex than laboratories. Environmental adaptability certification aims to assess device survival capability and performance stability under various real or simulated extreme environments.

- **RFI testing**: Under conditions with same-frequency wireless device interference (such as other operators' base stations, Wi-Fi APs, and Bluetooth devices), testing A-IoT device receiver sensitivity degradation, backscatter signal bit error rate, and device resynchronization capability.
- **Anti-blocking performance and multipath effect tolerance testing**: Simulating scenarios where power supply carrier field strength distribution is uneven due to dense cargo stacking and metal shelf reflections in smart warehouses. 3GPP points out that A-IoT device costs are extremely low, high-precision crystal oscillators cannot be integrated, and frequency offset can reach 10^5 ppm. Combined with complex environmental multipath transmission, this poses major challenges to device signal synchronization capability. Testing needs to evaluate device communication success rate in non-line-of-sight (NLoS) environments, connection stability between devices and base stations during movement (such as on logistics conveyor belts), and recovery time after energy harvesting interruption.

- **High-low temperature and humidity environment stability testing**: According to industrial environment testing standards, conducting wide-temperature range (-40°C~85°C) adaptability testing and corrosion and condensation resistance testing under high-humidity environments above 85% RH. Cyclic damp heat testing can reference procedures of 25°C↔55°C, 95% RH, and 24 hours/cycle, for 10 cycles, monitoring whether device functions are normal. Particular attention should be paid to RF antenna standing wave ratio humidity drift and ionic migration on printed circuit board surfaces.
- **Electromagnetic interference environment compatibility testing**: Simulating strong electromagnetic radiation interference environments from variable frequency drives and high-power motors in industrial production lines, testing A-IoT device signal parsing correctness and data reporting continuity, evaluating device system-level EMC performance in complex electromagnetic environments.

5.3.2.4 Lifecycle and Reliability Certification

Matching the "deploy and forget" maintenance-free operation concept pursued by Ambient IoT, device long-term operational reliability is a prerequisite for commercial large-scale deployment.

- **Durability testing (mechanical reliability)**: Assessing device structural integrity and functional stability under various physical stresses, including but not limited to: bending tests—simulating device substrate bending resistance under flexible packaging or wearable application scenarios; tensile testing—assessing device antenna structural integrity and conductivity under different tensions; vibration testing—simulating effects of sustained vibration during logistics transportation and vehicle mobile tracking on device internal capacitor solder joints and antenna matching circuits. Vibration testing parameters can reference ISTA 3A and other transportation packaging testing standards.
- **Long-term operational stability testing**: Through accelerated aging tests, assessing A-IoT device performance degradation trends under sustained operation. Since 3GPP Ambient IoT devices target service life exceeding 10 years, accelerated aging testing needs to use scientific methods such as the Arrhenius model, using high-temperature acceleration and periodic functional inspection to extrapolate device long-term reliability under normal temperature environments. During testing, key performance indicators (such as energy harvesting efficiency, backscatter signal power, and wake-up success rate) are continuously monitored to draw clear quantifiable service life assessment conclusions.
- **Energy harvesting efficiency degradation testing**: Monitoring capacity degradation rate of device internal capacitors after multiple charge-discharge cycles, and efficiency decline curves of environmental energy harvesting circuits (RF rectification and solar/thermal energy harvesting modules) after long-term operation. Assessing whether devices can maintain minimum energy supply levels within target service life.
- **Low-power mode long-term stability**: Verifying device leakage level in sleep standby state, wake-up success rate after long periods without wake-up, and

consistency of performance recovery after wake-up.

5.3.2.5 Security Certification

As A-IoT devices access core networks through licensed spectrum, security is an unavoidable core concern for the industry chain. 3GPP SA3 working group has conducted security and privacy research on Ambient IoT, clearly stating that bidirectional authentication should be supported between A-IoT devices and 5G networks, with authentication processes based on challenge-response mechanisms. Security certification main content includes:

- **Anti-forgery and anti-cloning capability verification**: Verifying devices have unique and tamper-proof identity identifiers (such as device permanent identifiers), and these identifiers are securely injected during manufacturing. Referencing device-reader bidirectional authentication mechanisms defined in ISO/IEC 29167 series (such as 29167-10 using AES-128 encryption suite), ensuring devices have anti-cloning capability. China's independent innovation TRAIS (device and Reader Air Interface Security) security technology, based on Tri-Element Peer Architecture (TePA) network security architecture, supports three modes—bidirectional authentication, reader unilateral authentication, and device unilateral authentication—providing basic security guarantees under low computational overhead, which can be included in security certification technical options.
- **Data encryption transmission capability verification**: Verifying air interface transmitted data encryption strength and key management mechanisms. Referencing at least 128-bit key strength required by GSMA IoT SAFE standards, ensuring A-IoT devices can achieve effective air interface data encryption while using extremely low-power resources. Need to assess the impact of encryption operations on device energy harvesting budgets, ensuring security mechanisms do not sacrifice communication reliability.
- **Identity authentication capability and network access security verification**: Verifying completeness of device network access bidirectional authentication process, and whether correct handling occurs upon authentication failure (such as refusing service and not leaking sensitive information). Referencing root trust mechanisms based on SIM/eSIM/iSIM defined in GSMA IoT SAFE standards, assessing whether devices can store certificates in tamper-proof hardware roots of trust. Authentication processes need to test device security during identity credential updates and key negotiation, preventing man-in-the-middle attacks and replay attacks.
- **Privacy protection capability**: Verifying whether devices support pseudonymization or dynamic change mechanisms for identifiers during communication, preventing device positioning and trajectory tracking risks caused by malicious monitoring of fixed identifiers. Assessing device data erasure mechanisms upon disposal or recycling, avoiding legacy data leakage.

5.3.3 Certification Process Design

The certification process, referencing best practices of mature certification organizations such as GCF and customized according to Ambient IoT technical characteristics, is designed in five stages:

5.3.3.1 Enterprise Application Submission and device Samples

Enterprises submit formal applications to authorized certification institutions, providing the following materials: enterprise qualification certificates and product technical specifications; detailed device design plans and PICS (Protocol Implementation Conformance Statement); 3GPP standard conformance self-assessment report; applicable scenario declarations (indoor/outdoor/industrial/logistics, etc.), used to determine certification scope and testing levels. Simultaneously submit the required number of certified test prototypes.

5.3.3.2 Laboratory Testing Execution According to Standards (Including Automated Testing Platforms)

Authorized laboratories conduct testing in controlled laboratory environments according to certification Levels 1 through 5 test items. Testing adopts automated testing platforms, maximally reducing manual intervention and ensuring testing result accuracy and reproducibility. Basic function testing (RF parameters, modulation/demodulation, protocol compatibility) and security testing are completed at this stage. Testing data is completely recorded and uploaded to the certification management system.

5.3.3.3 Real Scenario Testing Verification

Outside the laboratory environment, devices need verification in real or highly simulated deployment environments. Scenario testing covers:

- **Typical indoor scenarios**: Including smart warehouse inventory (dense cargo stacking shelves, large-space planes), indoor asset positioning (multiple compartments, metal furniture interference), etc.
- **Logistics scenarios**: Simulating continuous identification during conveyor belt movement, high-speed pass-through reading during package sorting, and dynamic tracking of transport vehicles.
- **Industrial outdoor scenarios**: For Device C (high-value outdoor scenario) devices, coverage distance verification and multi-base-station roaming testing need to be conducted under actual outdoor network environments.

In scenario testing, devices under test need actual network deployment. Inventory accuracy, coverage continuity, and multi-device concurrent processing capability are verified using on-site polling inventory, evaluating comprehensive performance indicators.

5.3.3.4 Expert Review and Result Disclosure

Independent technical expert teams review laboratory test reports and scenario testing results, focusing on reviewing testing data completeness, testing method standard conformance, and rectification plans for non-conforming items. Certification results passing review are disclosed on the certification system official website, accepting social supervision. The disclosure period is generally 15 working days.

5.3.3.5 Certification Certificate and Mark Issuance

After certification passes, graded certification certificates and publicly usable marks are issued to enterprises. Marks are designed as "Ambient IoT Certified" basic level and advanced marks subdivided by certification level (such as Type 1 Indoor General, Type 2 Industrial Enhanced, and Type 3 Outdoor Wide-Area divided by applicable scenarios; Standard/Secure/Enhanced divided by security levels). Certification certificates and marks remain valid before enterprises obtain ongoing surveillance audits . Certification certificates and marks need to have validity periods. Near expiration, testing must be initiated again to maintain validity. If standard versions are iterated during validity periods, testing must be initiated again according to updated standard versions to maintain validity.

5.3.4 Technical Support Platform Construction Concept

In terms of certification system framework operability and efficiency improvement, constructing highly intensive, automated, and intelligent technical support platforms is key.

5.3.4.1 Establishing Open Testing and Certification Platforms

Platforms should simultaneously support online and offline testing modes, serving all industry chain participants.

- **Remote submission and online reservation**: Enterprises can submit certification applications, upload technical documents, select test suites, and reserve testing times through platform portals.
- **Cloud collaborative testing capability**: Referencing mainstream cloud computing-based IoT device conformance testing frameworks, achieving remote cloud execution of some test cases (such as protocol conformance, security certification, and identification format verification).
- **Testing data visualization system**: Dynamically displaying testing progress, detailed results, and highlighted non-conforming items. Enterprises can view testing data online anytime and download test reports.

5.3.4.2 Developing Standard Test Case Libraries

Establishing standard test case libraries covering all levels, aligned with technical constraints and performance indicators defined by 3GPP protocols.

- **Layered case system**: Establish layered and graded test cases according to five certification levels, covering all testing dimensions such as RF performance, protocol stack interaction, interoperability, environmental adaptability, mechanical reliability, and security.
- **Typical scenario mapping**: Case libraries need to cover special testing needs of typical application scenarios such as smart warehousing, logistics tracking, industrial inventory, and environmental monitoring.
- **Continuous update mechanism**: As 3GPP standards evolve toward Release 20 and new services are introduced, case libraries maintain synchronous updates

and iterations.

5.3.4.3 Promoting Testing Equipment and Tool Chain Cost Optimization

Testing costs are core bottlenecks constraining small and medium-sized manufacturers' participation in certification.

- **Low-cost hardware testing solutions**: For A-IoT device characteristics of extremely weak backscatter signals and ultra-low power consumption, promote development of specialized low-cost signal analyzers and simulation testers, reducing dependence on expensive general-purpose instruments.
- **Shared testing resource pools**: Establish equipment sharing mechanisms among different certification institutions, reducing duplicate purchase costs.
- **Automated testing software tools**: Reference TreeATE and other open-source automated testing tools, providing open-source testing software solutions for small and medium-sized manufacturers, lowering testing entry thresholds.
- **Batch certification discount mechanisms**: Provide certain proportions of testing fee discounts for manufacturers simultaneously certifying multiple device models or large quantities of same-model devices.

5.3.4.4 Introducing AI and Big Data Analysis

Using artificial intelligence technology to improve testing efficiency and quality.

- **Assisted testing result analysis**: Apply machine learning models to analyze large volumes of historical testing data, identifying key bottleneck factors affecting device pass rates, providing improvement guidance for enterprises during R&D stages.
- **Anomaly identification and early warning**: During testing execution, AI systems can monitor indicator anomalies in real-time, quickly locating key nodes where performance fails to meet standards, shortening debugging cycles.
- **Automatic test report generation**: Combining large language models, automatically integrate testing data and judgment results, quickly generate structured certification reports, and provide scientific data visualization presentations.
- **Continuous monitoring and recertification early warning**: Continuously track certified devices' performance in the market, use big data analysis to assist in identifying early failure risks, providing data support for certificate renewal and upgraded certification.

5.4 Construction of "Chip-Device-Application" 3-tier Testing and Certification System

To address challenges of Ambient IoT device testing standard fragmentation and disconnection between testing and industry ecosystem, this section constructs a "Chip-Device-Application" 3-tier general testing case system. Through standardized and normalized layered testing systems, it achieves clear industry chain division of labor and stepped reuse of certification results, improving testing scalability and economics.

5.4.1 System Separation Principles and Case Rules

5.4.1.1 Principles for Constructing 3-tier Testing System

When constructing the Ambient IoT certification testing system, the core design principle of "system separation" must be followed. That is, the three levels of chip testing, device testing, and application testing achieve vertical decoupling in testing content, testing methods, and judgment criteria. Each level focuses on its own testing objects and verification objectives, avoiding the impact of non-conformance at one level on objective judgment of testing conclusions at other levels.

The core value of system separation lies in achieving clear responsibility division among upstream and downstream industry chains and stepped reuse of certification results:

- **Chip testing** focuses on the chip's protocol implementation completeness and basic functional correctness. The tested content is unrelated to the device's specific physical form (such as PCB rigid devices, flexible patches, and injection-molded device cards), aiming to conduct low-level certification of the chip's protocol stack and core communication capability.
- **device testing**, based on chips that have passed chip-level certification, evaluates RF performance and link quality under specific device packaging and antenna design. Testing results directly reflect device manufacturers' design and manufacturing levels.
- **Application testing** orients toward final business scenarios, verifying device reliability, robustness, and system-level interoperability in simulated or actual deployment environments.

Applying this separation mode, by integrating certified chips, device product manufacturers can reuse the chip's underlying testing results without repeated testing, thereby achieving cost savings and faster time-to-market. Through 3-tier progressive testing, responsibility boundaries at each industry chain link are clear:

- **Chip manufacturers** are responsible for protocol correctness and basic functions.
- **Device manufacturers** are responsible for RF links and packaging reliability.
- **System integrators and end users** are responsible for scenario adaptability verification.

To ensure efficient flow of testing and certification results and avoid repeated testing across upstream and downstream, a unified 3-tier flow connection mechanism is established, achieving "one certification, stepped reuse, and deep connection."

Testing Level	Access Input Conditions	Core Testing Content	Certification Output	Downstream Reuse and Flow Path

Testing Level	**Access Input Conditions**	**Core Testing Content**	**Certification Output**	**Downstream Reuse and Flow Path**
Chip Testing Level	Single chip wafer/die and raw physical parameters	Protocol conformance, physical layer RF characteristics, basic logic storage functions, basic inventory functions (single-device/multi-device inventory)	Chip-level general compliance certification report and parameter matrix	As downstream device design access basis. device-level testing directly exempts protocol conformance and other chip physical layer testing.
Device Testing Level	Certified chip + device antenna sample finished product	Overall RF conformance, wireless resource management conformance, air interface OTA activation sensitivity, mechanical physical durability, medium sensitivity	Standard device product compliance certificate and packaging physical property report	As downstream industry system integration application access basis. Downstream scenario testing focuses on macro indicators, exempting physical property testing.

Testing Level	Access Input Conditions	Core Testing Content	Certification Output	Downstream Reuse and Flow Path
Application Testing Level	Certified device + vertical industry-specific software and hardware integrated environment	Multi-device dense reading rate, high-speed mobile robustness, multi-base-station continuous networking service flow	Scenario-level special robustness rating certification report	Guides various vertical industries (such as smart warehousing, power assets, and cold chain logistics) to directly conduct large-scale commercial adoption.

Core Connection and Flow Rules:

1. **Prohibition of Bypass Principle**: Objects that have not passed prior-level certification shall not directly apply for subsequent-level integrated certification. That is, the core chip used by devices must have a valid "chip-level certification report," otherwise device-level certification shall not be accepted.
2. **Result Mutual Recognition and Exemption Mechanism**: In testing at subsequent levels, parameters and conformance indicators already covered by prior levels shall, provided no changes occur at relevant boundaries, be directly trusted and exempted from repeated testing by downstream certification institutions.
3. **Production Line Batch Sampling Linkage**: Application-level testing and production line device factory testing form normalized data linkage. If batch RF degradation caused by packaging processes is discovered at the application end, it will trigger batch sampling review mechanisms for corresponding device-level certifications.
4. **Certification Mark Level Interconnection**: Promote unified "GTI Ambient IoT" stepped certification marks. Marks clearly indicate C (chip-level), D (device-level), and A (application-level) three-dimensional passing status, facilitating vertical industry buyers to clearly assess device compliance capability at a glance.

5.4.1.2 OTA Testing Method (OTA Basic Testing Method)

Since Ambient IoT passive flexible devices (Device 1) typically do not have traditional communication device conducted antenna interfaces, their RF and physical layer characteristics must be tested in Over-The-Air (OTA) testing environments. Testing is based on Device 1 (Ambient IoT device) technical specifications and characteristic requirements defined in 3GPP Release 19, conducted in standard anechoic chambers.

For Device 2b and Device C device types currently in the definition stage in 3GPP Release 20, applicable conducted testing methods or OTA anechoic chamber testing methods need to be determined according to future standard definitions.

1. Core Testing Environment Configuration:

- **Anechoic chamber and polarization configuration**: Microwave full anechoic chambers equipped with high-precision multi-axis turntables are used. Orthogonal polarization antenna arrays are utilized to comprehensively evaluate device RF energy harvesting and reflected modulation performance at different spatial angles.
- **Energy source and Continuous Wave (CW) configuration**: The testing system integrates continuous wave energy transmission sources to provide stable spatial electromagnetic excitation to the Device Under Test (DUT), simulating far-field energy supply from base stations or external excitation sources.
- **Time-gating mechanism**: High-precision timing control is used to separate continuous wave excitation signal streams from device backscatter weak modulation signal streams, ensuring precise capture of air interface testing indicators.

2. Indicator Requirements Baseline: Key physical layer performance indicators such as Device 1 transmission and reception RF requirements and Energy Harvesting Sensitivity (EHS) strictly follow provisions of 3GPP TS 38.191 and other relevant international specifications.

5.4.1.3 Non-Laboratory Environment Testing Methods

As mentioned in Section 3.4.1.2, since Ambient IoT passive flexible devices typically do not have traditional communication device conducted antenna interfaces, their RF and physical layer characteristics must be tested in OTA environments. Compared with conducted testing, OTA testing results in non-laboratory environments such as production lines are greatly affected by environmental stability. Once the testing environment changes, OTA testing results are very likely to change. Therefore, in such scenarios, determining whether Ambient IoT devices testing passes through fixed threshold faces significant uncertainty and challenges.

In such scenarios, high-quality A-IoT device samples (i.e., "Gold devices") can be picked out from mass-produced and verified qualified batches as reference devices. Then, reference devices and devices under test are subjected to the same test steps in the same testing environment. Testing results of devices under test are determined based on data obtained from both reference and tested devices:

Compare the obtained reference device and device under test testing data. Based on the difference between the two testing data sets, determine the testing result of the device under test: if the difference does not exceed the threshold, the device under test passes; if the difference exceeds the threshold, the device under test fails.

5.4.2 Chip-Level Certification Test Cases (C Series)

As the cornerstone of the entire 3-tier system, chip-level testing focuses on verifying Ambient IoT core chip physical layer interoperability, core protocol conformance, and basic logic functions. Conducting independent certification by chip unit can greatly reduce repeated testing costs for downstream device manufacturers. Under normal circumstances, chip-level certification testing is submitted in device form, but the tested functions are all related only to the chip platform, unrelated to the specific form of devices integrating the chip.

Testing Module	**Core Testing Content**	**Expected Technical Indicators**
Protocol conformance testing	Backscatter modulation timing, frame structure, and Anti-collision arbitration mechanism specification verification	Modulation depth ≥ 85%, timing deviation ≤ ±1μs, conflict resolution success rate 100%
RF physical layer testing	Chip demodulation sensitivity, minimum wake-up power, and impedance matching adaptive capability testing	Static power consumption ≤ 10μW, input impedance dynamic adjustment range meets design baseline
Basic function testing (storage and logic functions, single-device/multi-device inventory functions, etc.)	EEPROM/MTP memory area read/write/erase endurance; whether single-device inventory and multi-device inventory are supported	Data retention life ≥ 10 years, read/write cycles ≥ 100,000 times

5.4.3 Device-Level Certification Test Cases (D Series)

device-level testing focuses on overall physical properties and RF performance after chip and antenna integration. By introducing standard substrates and environmental simulation, it evaluates finished device RF conformance and mechanical environmental durability. Physical properties refer to physical durability, including bending resistance, compression resistance, and bending resistance.

Testing Module	**Core Testing Content**	**Expected Technical Indicators**
RF conformance testing	Standard equivalent isotropic radiated power (EIRP), device forward activation sensitivity, backscatter intensity spatial distribution	Activation power threshold spatial direction standard deviation ≤ 1.5 dB, omnidirectional radiation efficiency complies with each frequency band requirement

Wireless resource management conformance testing	RRM test cases defined in 3GPP RAN5 TS 38.591-2, corresponding to verification of device wireless resource management technical requirements defined in 3GPP RAN4 TS 38.191	As specified in 3GPP RAN4 TS 38.191
Mechanical performance testing	device physical deformation and RF attenuation under flexible bending, peel strength, and high-low temperature cyclic changes	Device1 reject rate ≤5% after 1000 bending cycles. Non-conforming Device: response gain >5dB at any frequency within ±10MHz of center resonant frequency on test curve
Medium sensitivity testing	Antenna detuning and electromagnetic boundary deterioration assessment when attached to absorbing media (such as high metal surfaces and aqueous liquid containers)	For anti-metal/special devices against liquids on specific substrates, activation distance degradation ≤ 15%
Performance Test for Dense RFID Devices	Evaluate the variation of sensitivity and identification success rate in a dense deployment environment consisting of 100 RFID devices.	sensitivity degradation ≤ 3 dB, and identification success rate ≥ 98%.

5.4.4 Application-Level Certification Test Cases (A Series)

Application testing is the top tier of the 3-tier testing system. Its core task is to verify that devices certified at chip and device levels demonstrate comprehensive performance in real or simulated business scenarios. Different from the previous two levels, application-level testing does not pursue measuring chip or device extreme physical indicators but focuses on user-perceivable system-level business indicators such as inventory success rate, coverage continuity, and concurrent processing capability. Application-level testing orients toward final commercial deployment scenarios, simulating real dense reading, mobile speed, and network topology environments, verifying overall system robustness in high-complexity industrial scenarios.

Testing Module	**Core Testing Content**	**Expected Technical Indicators**
Scenario special testing	Dense multi-device stacked reading in warehousing logistics, conveyor belt high-speed pass-through (mobile speed dynamic simulation) identification rate testing	Aisle gate dense group reading rate ≥ 99% (50 devices/second), Conveyor belt high speed (≥1.5 km/h, data referenced from carton labels on cotton garments)

Robustness special testing	Group reading stability under cross-multi-base-station cellular continuous networking coverage, multipath fading and complex electromagnetic interference tolerance	——

Test design should cover typical Ambient IoT application scenarios such as retail product inventory, real-time supply chain tracking, and workflow automation as representative use cases.

5.4.4.1 Typical Scenario Testing Environment Construction

For typical Ambient IoT application scenarios, differentiated testing environments are designed to verify device reliability, robustness, and interoperability.

(1) Smart Warehousing and Indoor Inventory

Simulates complex scenarios with dense cargo stacking in large warehouses. Testing focuses include:

- device inventory success rate at different heights (ground level to high shelves)
- Impact of metal shelves and liquid goods on backscatter signal attenuation
- Connection continuity under multi-base-station joint coverage in large spaces
- Testing indicators reference 3GPP targets: indoor scenario connection density is 150 devices per 100 square meters

(2) Logistics Tracking and Mobile Identification

Simulates dynamic identification scenarios such as continuous conveyor belt pass-through and rapid sorting line pass-through:

- device inventory success rate and single-device identification time during movement
- Collision rate and retry efficiency when multi-device packages pass simultaneously
- Per 3GPP design targets, device movement speed reaches at least 10 km/h in indoor scenarios

(3) Anti-Metal and Industrial Environments

Simulates scenarios where devices are attached to metal surfaces or located in strong electromagnetic interference environments in industrial manufacturing:

- Backscatter performance degradation when device antennas are blocked by metal or placed close to metal surfaces
- Signal integrity when working near strong interference sources such as industrial motors and variable frequency drives
- device RF parameter drift under high-low temperature and high-humidity environments

(4) Outdoor Wide-Area Continuous Networking

Simulates outdoor coverage scenarios such as urban blocks and logistics parks:

- Reference coverage distance targets: outdoor maximum distance 50 to 500 meters, single-base-station device inventory success rate
- Service continuity and packet loss rate during multi-base-station handover
- Connection maintenance capability under reference movement speed design

target (10 km/h)

- Testing actual achievability of outdoor scenario connection density target (20 devices per 100 square meters)

5.4.4.2 System Stability Verification Under Complex Conditions

Introducing complex conditions such as automated inspection, multi-reader networking, and blocking interference, comprehensively verifying Ambient IoT system reliability under extreme environments.

Multi-reader coordination testing: Under conditions where multiple base stations simultaneously provide energy, verifying multi-reader joint deployment scenario device demodulation capability, inter-base-station interference management mechanisms, and device access load balancing effects.

Energy void and interruption recovery testing: Simulating scenarios where power supply carrier field strength is insufficient in some areas, testing device energy harvesting module emergency response and resynchronization efficiency and lost data recovery mechanisms after energy recovery.

Random blocking and movement testing: Introducing uncontrollable factors such as random blocking objects, dynamic personnel movement, and random device movement, evaluating system robustness and adaptive capability.

Large-scale concurrent stress testing: Conducting long-duration stress testing near target connection density upper limits, monitoring system inventory accuracy and latency jitter when approaching capacity limits.

5.4.4.3 Smart Warehousing and Indoor Inventory Use Cases

Smart warehousing is the focus use case of Release 19 standardization (rUC1: indoor item inventory; rUC4: indoor command delivery):

Test Item	Test Purpose	Test Conditions	Judgment Criteria
High-shelf inventory	Multi-height shelf device inventory success rate	Shelf height 1 to 10 meters, metal goods	Success rate ≥ 95% at each height
Dense stacked inventory	Inventory success rate in dense cargo stacking environment	Layer spacing <20 cm, ≥100 items	Inventory accuracy ≥ 99.9%
Large-space coverage	device identification capability under single-base-station coverage	Indoor space >1,000 m²	Far-end identification success
Command execution	device response after inventory command delivery	—	Execution success rate ≥ 99%

5.4.4.4 Logistics Tracking and Mobile Identification Use Cases

Test Item	**Test Purpose**	**Test Conditions**	**Judgment Criteria**
Conveyor belt pass-through	device inventory success rate during movement	Speed ≤ 10 km/h	Success rate ≥ 95%
High-speed sorting	High-speed pass-through identification capability	Speed ≤ 20 km/h	Single-device identification time ≤ 100 ms
Batch package identification	Collision handling when multiple packages pass simultaneously	10 to 50 packages pass simultaneously	Identification completeness ≥ 98%
Connection maintenance during movement	Connection continuity during movement	Motion trajectory covers full space	Connection interruption rate ≤ 5%

5.4.4.5 Anti-Metal and Environmental Adaptability Use Cases

Test Item	**Test Purpose**	**Test Conditions**	**Judgment Criteria**
Metal surface attachment	device performance degradation when attached to metal surface	Full contact/partial contact/separation	FFS
Industrial EMI tolerance	Communication reliability in strong electromagnetic interference environment	Variable frequency drive and motor interference	Bit error rate ≤ 10^{-3}
High-low temperature cycling	device stability under wide temperature range	-25°C↔70°C	Performance fluctuation (Normal Temperature)≤ 2 dB
High-humidity environment	RF parameter drift under high humidity	85% RH, 55°C	Parameter drift ≤ 10%

5.4.4.6 Outdoor Wide-Area Continuous Networking Use Cases

Outdoor scenarios are the focus of Release 20 work. Coverage distance and roaming testing need evaluation:

Test Item	**Test Purpose**	**Test Conditions**	**Judgment Criteria**
Single-base-station coverage	Verify single-base-station extreme coverage distance	Reference coverage target 50 to 500 m	Far-end identification success rate ≥ 90%
Multi-base-station handover	Verify service continuity during movement across	Movement speed ≤ 10	Handover success rate ≥ 99%

	base stations	km/h	
Outdoor connection density	Verify outdoor scenario connection density target	20 devices/100 m²	Concurrent processing completeness ≥ 95%

5.4.4.7 System Robustness Use Cases Under Complex Conditions

Test Item	**Test Purpose**	**Test Conditions**	**Judgment Criteria**
Multi-reader coordination	Multi-base-station joint energy supply and joint deployment	2 to 4 base stations coordinated	Inventory accuracy ≥ 99.9%
Energy void recovery	Resynchronization capability after energy interruption	Normal before interruption, recovery after	Recovery time ≤ 5 seconds
Large-scale concurrency	System stability near capacity limits	Per 3GPP target connection density	Inventory accuracy ≥ 99%
Random dynamic blocking	Introduce moving blocking objects and personnel movement	Random blocking rate ≥ 30% of time	Performance decrease ≤ 20%

5.5 Coordination Mechanisms for Testing Specification Development

Constructing general testing methods and a certification system for the Ambient IoT ecosystem is a systematic project involving multiple dimensions such as specification development, technology R&D, and industry deployment. Its successful implementation depends on broad participation and deep collaboration from all industry chain parties. A single institution or a few enterprises cannot independently undertake testing specification development covering the entire chain from chips to devices to applications, nor can they ensure the broad representativeness, fairness, and public credibility of specifications. Therefore, establishing an open, collaborative, and efficient specification development mechanism is a key guarantee for the certification system to truly land, operate, and gain broad industry adoption.

Construction of coordination mechanisms should follow these core principles:

Openness and Inclusiveness Principle: Specification development work should be open to all industry stakeholders without unreasonable participation barriers. Participants should cover diverse roles such as chip designers, device manufacturers, antenna solution providers, equipment vendors, operators, system integrators, industry application parties, third-party testing institutions, and academic research institutions, ensuring specifications fully reflect various parties' demands and actual situations. Simultaneously, participation opportunities for large, medium, and small enterprises and different regions should be considered, avoiding discourse power monopolized by a few head enterprises.

Consensus-Driven Decision-Making Principle: Major matters during specification development, including testing method selection, performance indicator threshold setting, and certification process design, should be based on technical data and industry practice as decision-making foundations, seeking industry consensus through sufficient technical argumentation and negotiation. For technical routes with genuine disagreements, space for differentiated implementation should be allowed under a unified framework, reflecting specification universality rather than uniqueness.

Scientific Rigor Principle: Testing specification development must be built on solid scientific research and engineering verification foundations. Testing method design should have scientific basis. Performance indicator setting should undergo sufficient theoretical analysis and experimental verification. Judgment criterion determination should reflect rationality and operability. Simultaneously, specifications are encouraged to pass pilot verification and small-range trial use, testing their effectiveness in practice and continuously iterating and optimizing.

Dynamic Evolution and Version Management Principle: Since Ambient IoT technology is still in a period of rapid evolution, 3GPP standards will continuously iterate from Release 19 to Release 20 and beyond. New application scenarios will continuously emerge. New technical solutions will continuously mature. Testing specifications should be designed as pluggable and scalable modular structures, possessing evolving capability to dynamically incorporate new test items, adjust performance indicator thresholds, and adapt to new scenario requirements. Version management systems for specifications should be established, ensuring all industry parties always use the latest effective version of specifications.

Testing specification development should follow an iterative advancement process of "open solicitation—technical discussion—expert review—specification release—pilot verification—continuous iteration," ensuring specification scientific nature, representativeness, and operability.

Given GTI's (Global Technology Association of InfoComm) unique influence in the global information and communications industry, rich experience in specification development, and established broad industry cooperative relationships, it is recommended that GTI serve as the core leading unit, jointly promoting Ambient IoT testing specification development with all industry chain parties. GTI has previously successfully promoted the release of the cellular Ambient IoT global unified identification cooperation initiative. It is recommended to continue leveraging GTI's organizational advantages in integrating Ambient IoT industry chain resources and coordinating forces among parties, further expanding into testing specification and certification system construction areas on the basis of existing work.

6 Construction of Application Scenario-Driven Testing Requirements System

6.1 Typical Application Scenario Characteristics of 5G Ambient IoT

Ambient IoT technology is accelerating penetration into multiple vertical areas of national economic and social development. Deeply understanding core characteristics and differentiated needs of various typical application scenarios is a prerequisite for constructing scenario-based testing specifications.

6.1.1 General Scenario Characteristics

Coverage and Continuous Networking Capability Characteristics: Ambient IoT breaks through traditional RFID's short-distance limitations, achieving 100-meter-level to kilometer-level coverage capability. Systems need to support ultra-large-area continuous networking and seamless connection. In the future, coverage will extend to outdoor active devices at 100-meter-level to kilometer-level.

Deployment Environment Complexity Characteristics: Scenarios such as multi-layer cargo stacking, multi-layer shelves, metal pallets, and steel columns pose severe challenges to device coverage penetration capability and anti-blocking capability. devices need Uplink backscatter signal reflection capability to cope with metal blocking. Flexible devices need to maintain stable coverage and other physical characteristics even when bent on irregularly shaped items.

Full-Lifecycle Management Characteristics: Ambient IoT supports full-process data closed loops from warehousing, transportation, loading/unloading, to end delivery, achieving item full-lifecycle traceability and digital management capability.

High-Concurrency and Mobile Scenario Characteristics: Systems need to meet multi-device inventory efficiency and accuracy requirements during high-density massive device inventory. Simultaneously, in mobile scenarios such as AGV carts, forklifts, and conveyor belts, movement speeds of 3 to 5 kilometers per hour need to be supported.

Sensing and Security Characteristics: devices need temperature, humidity, and other environmental monitoring capabilities. device information needs encrypted storage, supporting tampering prevention and anti-forgery functions, and having lifecycle management capability. Disposed devices can be deactivated.

Ultra-Low Power and Communication Constraint Characteristics: Passive devices rely on external excitation sources for energy and need to support RF energy storage or environmental energy storage. Device cannot actively and continuously transmit signals. Uplink communication relies on the base station sending excitation signals. Transmission distance is mainly local coverage. Single reporting data is only a few to a few dozen bytes. Only intermittent and triggered collection is supported. High-frequency continuous real-time upload is not possible.

Cost and Lifecycle Characteristics: Single-device hardware costs are extremely low, suitable for large-scale deployment of hundreds of thousands to millions of massive endpoint nodes. Service life can reach high up to 15 years. On-site maintenance costs are almost zero.

Environmental Deployment Adaptability Characteristics: devices need to withstand high-low temperatures, corrosion, moisture, dust, and oil pollution. They can be used in special scenarios such as explosion-proof, sterile, and enclosed cavities. However, in fully metal shielded environments or vacuum-sealed environments without light, RF, or vibration, energy harvesting is impossible. Application is limited.

System Architecture Characteristics: Supporting excitation readers or base stations are essential. The device must support communication with readers in a "separated architecture of CW generator and Reader". And the Device should support commands such as inventory and read/write.

6.1.2 Typical Industry Application Scenarios

Intelligent Warehouse Management Scenario's comprehensive requirements include: high-density massive device inventory needs to cope with signal blocking caused by multi-layer cargo stacking, multi-layer shelves, metal pallets, and steel columns. Metal shelf and metal pallet management needs devices with anti-metal characteristics. Irregularly shaped items need flexible devices maintaining coverage and other physical characteristics when bent. Drug and chemical storage needs devices with corrosion resistance capable of working in liquid environments. Cold chain warehouses need devices working normally under low-temperature environments. Tobacco and pharmaceutical warehousing needs temperature, humidity, and other environmental monitoring. Devices need sensing capability. Scenarios such as AGV carts, forklifts, and conveyor belts need devices supporting movement speeds of 3 to 5 kilometers per hour. Full-process flow automation from inbound/outbound, shelving, moving, allocating, picking, outbound, to returns needs bin-level positioning capability. Storage date recording needs devices with multiple read/write capability to achieve expiration warnings. Defective product management needs devices with enable and disable lifecycle management capability.

Supply Chain Warehousing and Logistics Scenario From the logistics center warehouse to the city level warehouse to the distributor warehouse to the retail point, the entire process from production to logistics to retail requires end-to-end management. During peak sorting hours, a large number of packages and trays enter the coverage area simultaneously, requiring support for high concurrency read and write capabilities. There is no need to slow down or align the card reader at close range, and the assembly line can maintain high-speed operation to improve outbound sorting throughput. During the logistics transportation process, it is also necessary to monitor the entire process, and the transportation trajectory and transfer nodes need to be traceable, requiring trajectory tracking and positioning functions. Partial cold chain transportation requires environmental temperature monitoring throughout the entire process. Logistics pallets, plastic boxes, and other vehicles require full lifecycle asset management, which is searchable and recyclable.

Industrial Manufacturing and Tooling Equipment Management Scenario faces special challenges: workshops have high-temperature, oily, and dusty environments. Some areas require explosion-proof. Batteries pose safety hazards. devices need to be embedded in molds and machine tool cavities. Battery replacement is extremely difficult. Reading is only needed during tool changes, inspections, and maintenance—no need for 24-hour continuous monitoring. Tools are cyclically used for more than five years. Passive device lifecycles synchronize with equipment, achieving maintenance-free goals.

Smart Building, Fire Protection, and Utility Corridor Scenarios' core demands include: widely dispersed points and large quantities. Full-house wiring and power supply costs are high. Fire protection regulations require long-term maintenance-free equipment. Lithium battery life cannot meet 5- to 10-year usage standards. Electrical rooms and underground enclosed spaces require explosion and fire prevention, absolutely preventing battery self-ignition and leakage. Normal state has no data. Reading is only triggered during manual inspection or high-temperature anomalies.

Data Center Machine Room Environmental Control and Asset Management Scenario's characteristics include: tight internal cabinet space and dense wiring make it difficult to add power supply lines. Massive active sensors would increase overall machine room power consumption and heat dissipation pressure. Machine rooms are long-term unattended. Thousands of cabinet nodes cannot have batteries individually replaced. Only simple data such as static temperature and cabinet door opening/closing are collected. Reporting frequency is low.

Retail and Luxury Anti-Counterfeiting Scenario requires: per-item deployment makes single-device cost extremely demanding. Flexible paper devices need to be thin and lightweight, not affecting appearance whensticking to clothing or packaging boxes. Checkout lane batch identification replaces manual scanning to improve settlement efficiency. Most are disposable. After products are sold, devices are discarded without need for recovery or recharging.

Medical Surgical Instrument Management Scenario's rigid needs include: need to withstand temperatures above 120°C during high-pressure steam sterilization. Lithium batteries are easily damaged. Sterile environments absolutely prevent battery leakage contaminating surgical instruments and comply with hospital infection standards. Instruments are cyclically reused for many years. devices synchronize lifecycles without replacement. Rapid batch inventory after surgery avoids instruments being left in patients.

Electric Power Grid Equipment Monitoring Scenario's adaptive advantages include: high-voldevicee equipment is sealed and cannot be arbitrarily opened. Battery replacement requires power oudevicees, causing major economic losses. Electromagnetic field energy from equipment can be harvested for self-supply. No external power cables needed. Only periodic inspection temperature measurement is needed. Real-time continuous monitoring is unnecessary.

Elderly Care Facility Personnel Management Scenario's diversified needs include: elderly wandering prevention supports once-daily inventory. Multi-scenario dangerous area long-term staying automatic early warning for elderly. devices need wearable and waterproof, supporting positioning and electronic fence functions. Daily body monitoring needs blood pressure, heart rate, and sleep sensing functions. Medicine dispensing and infusion verification needs elderly identity verification. Medical records and allergy information need encrypted storage, tampering prevention, and anti-forgery to protect medical privacy.

6.2 Application Scenario-Oriented Testing Specification Design

The "Scenario-Indicator-Method" three-element model can be considered for constructing testing standards, ensuring testing content tightly centers on real application scenario needs, enabling testing results to effectively support scenario-based product selection decisions.

Application Scenarios	Scenario-based Testing Requirements										
	Single-Device Inventory	Multi-Devices Inventory	Information Writing	Blocking Scenarios	Aisle Gate Scenarios	Cardboard Medium	Metal Medium	Other Special Media	Special Environment	Safety Testing	Wide Beam Antenna
Warehouse Management	√	√	√	√	√	√	√	Wooden Plastic	Waterproof/Dustproof/Corrosion-resistant	√	
Supply Chain Logistics	√	√	√	√ e.g. the spacing between device and blocking is 5 cm:	√	√	√	Wooden. Plastic	Waterproof/Dustproof/Corrosion-resistant		
Industrial Manufacturing	√	√	√	√	√	√	√	Plastic Glass	Strong electromagnetic interference, waterproof, dustproof, chemical corrosion resistant, bend-resistant, impact-resistant,		

									high-temperature		
Asset management / Building	√	√	√	√	√	√	√	Plastic Glass	Waterproof/Dustproof	√	√
Hospital/Nursing Home	√	√	√	Complex environment	√	√	√	Plastic Glass Liquid	Waterproof/Dustproof	√	√
Power Equipment Management	√	√	√	Complex Environment			√		Strong electromagnetic interference/high temperature	√	√

Compared with traditional RFID device microwave anechoic chamber testing, Ambient-IoT device microwave anechoic chamber testing has the following main differences, which need consideration in testing specification development:

1. Unlike RFID scanning devices that can manually adjust positions, Ambient IoT readers and CWs have fixed positions, requiring Ambient IoT device antennas to support wider beam angles.
2. When testing indicators such as RFID device receiving sensitivity involving low-power small-signal input, RFID scanning devices can be used for testing. However, Ambient IoT base station readers' output power is far higher than RFID scanning devices, and they are located in the narrow space of anechoic chambers. Even if reader transmission power is adjusted to the minimum, it may be difficult to provide low-power small signals meeting testing requirements, potentially facing testability issues.It is recommended to use third-party instrument to simulate base station signals for testing and verification.
3. RFID charging signals and excitation signals are both provided by scanning devices, meaning RFID charging signals and excitation signals are in the same direction. However, in actual Ambient IoT base station deployment, readers and CWs are mostly installed at spaced distances—that is, charging signals and excitation signals are in different directions.
4. RFID supplementary test cases mainly target footwear and apparel scenarios. Ambient IoT needs to focus on testing high-value scenarios such as cartons and metal.

7 Conclusions and Recommendations

7.1 Main Research Conclusions

Currently, the "ubiquitous connectivity, zero power consumption, and full-scenario coverage" IoT vision is accelerating implementation. However, Ambient IoT devices lack unified standards in application-layer testing, scenario adaptability testing, production line testing, and platform testing, which may lead to potential risks such as poor device and network interoperability, uneven quality, difficulties in upstream and downstream coordination, and high application deployment risks, constraining industry large-scale processes.

Based on existing device certification systems and production line testing status, this research report systematically analyzes core pain point issues and proposes a testing and certification system construction plan for the Ambient-IoT ecosystem:

1. **Establishing "Open, Universal, Scalable, and Verifiable" core concepts**, promoting establishment of international coordination mechanisms with GTI as the platform, filling global industry gaps.
2. **Constructing a "Chip-Device-Application" 3-tier testing system**, decoupling protocol conformance, RF performance, and application scenarios, allowing "chip-based" partial basic testing and certification, reducing device repeated testing costs, and improving industrialization efficiency.
3. **Advocating application scenario-driven testing specification design**, incorporating anti-metal and networking identification rate indicators for real environments such as warehousing and logistics into testing projects, ensuring certification results truly reflect device actual deployment capability.

7.2 Future Outlook

In the future, GTI will, based on this system, formulate a series of technical specifications and testing methods targeting industry customers' scenario-based application needs, helping industry customers deploy a stable and reliable Ambient IoT device certification system, continuously driving Ambient IoT test case iteration and industry mutual recognition, and providing solid guarantees for the commercial prosperity of the trillion-level Ambient IoT ecosystem.

Establishing this system is not only a technical necessity but also a hallmark of industry ecosystem maturity. Through GTI leading and the entire industry chain jointly participating in specification development, this system is expected to become a critical bridge for Ambient IoT "moving from laboratories to the real world," providing reliable quality endorsement for Ambient IoT industry customers, accelerating Ambient IoT large-scale deployment in fields such as smart logistics, industrial manufacturing, and environmental monitoring, and ultimately nurturing the sustained prosperity of the global communications industry ecosystem.

8 References

[1] ISO/IEC 18000-6C:2017 RFID System General Standard.

[2] Arc Certification Program, Impinj, Inc.

[3] EPCglobal device Data Standard (TDS).

[4] 3GPP TS 38.591-1: 5GS; Ambient IoT device conformance specification; Part 1: Common test environment.

[5] 3GPP TS 38.591-2: NR; Ambient IoT device conformance specification; Part 2: Radio transmission, radio reception and radio resource management.
[6] 3GPP TS 38.591-3: 5GS; Ambient IoT device conformance specification; Part 3: Protocol.
[7] 3GPP TS 38.191: Ambient IoT device radio transmission and reception
[8] 3GPP TS 38.194: Ambient IoT Base Station (BS) and Carrier-Wave (CW) node radio transmission and reception.
[9] 3GPP TS 38.291: NR; Ambient IoT Physical layer.
[10] 3GPP TS 38.391: Ambient IoT Medium Access Control (MAC) protocol.
[11] 3GPP TR 38.769: Study on solutions for Ambient IoT (Internet of Things) in NR
[12] Gan Q. UHF RFID-IoT Technology, Products and Applications[M]. Beijing: Tsinghua University Press, 2021.