ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCE

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. No. 4 (32), Vol. 2. pp. 153–156
DOI: https://doi.org/10.5281/zenodo.24003279
Journal website: https://cajournal.kz

UDC 006.91

QUALITY ASSURANCE IN TESTING SMART HOME APPLIANCES

Toleubay Zarema Maulenovna
Satbayev University, Almaty, Kazakhstan

Toleubay Zarema Maulenovna — Master's student 2 year, Satbayev University, Almaty, Kazakhstan.

© Toleubay Zarema Maulenovna, 2026

Abstract: Fast-paced growth in IoT hardware and complex software integration presents a practical quality control challenge for modern household devices. This paper outlines an empirical quality assurance method tailored for testing Wi-Fi-enabled home appliances. Focusing on dynamic signal stability, transmission delays, and data loss, we evaluated a commercial robotic vacuum cleaner across realistic operational setups involving distance variations and structural walls. We collected real-time metrics for Received Signal Strength Indicator (RSSI), packet loss, latency, and jitter. To create a definitive threshold for pass/fail decisions, we combined these parameters into a weighted Integral Connection Quality Index (Q). Physical test runs show a clear operational drop-off below –70 dBm RSSI. At this point, packet loss surpasses 4.5% and latency doubles, pulling Q under the critical 0.60 mark and triggering application control failures. Repeated measurements confirmed solid test consistency, with the coefficient of variation staying under 8%. Overall, this study offers testing labs and manufacturers a concrete, metrologically sound process to define product compliance and limit post-sale warranty claims.

Keywords: smart home appliances, quality assurance, functional testing, Wi-Fi connectivity, integral quality index, data transmission reliability, RSSI, packet loss.

1. Introduction

The modern consumer electronics market is experiencing a structural transition driven by the ubiquitous integration of digital communication protocols and intelligent microcontrollers into everyday home appliances. Household equipment—ranging from climate control units and smart lighting to automated floor cleaning systems—has evolved from isolated electromechanical devices into interconnected nodes within the Internet of Things (IoT) ecosystem. This architectural evolution allows products to continuously upload telemetry data, receive firmware updates over-the-air (OTA), and execute remote commands issued from mobile applications or voice-assistant platforms. However, combining heterogeneous hardware, embedded operating systems, sensor micro-arrays, and radio frequency (RF) transceivers dramatically expands the potential failure surface of modern home appliances.

Unlike traditional electrical appliances, whose operational reliability depends primarily on component durability and power supply stability, the functional performance of a smart appliance is intrinsically tied to the quality and persistence of its wireless connection. In field conditions, a device does not operate in an isolated RF environment. Instead, it must navigate crowded 2.4 GHz and 5.0 GHz frequency bands, physical attenuation caused by structural partitions, multipath signal reflections, and ambient electromagnetic interference generated by adjacent household electronics. Under these dynamic conditions, even minor network degradations—such as momentary latency spikes, packet dropouts, or transceiver signal attenuation—can degrade real-world performance. In

consumer usage, these technical flaws manifest as failed application synchronization, incomplete task execution, unexpected offline states, and severe input lag. For manufacturers producing items at scale, these connectivity failures cease to be isolated technical anomalies; they become systematic reliability hazards that directly fuel customer dissatisfaction, negative product reviews, and rising warranty return rates.

Despite the growing operational reliance on wireless data transfer, current regulatory frameworks and testing standards have failed to keep pace with industry needs. Standard conformity assessment procedures for consumer appliances—such as ISO/IEC guidelines and national technical regulations—focus overwhelmingly on electrical insulation, thermal resistance, mechanical durability, and basic electromagnetic emissions [1]–[3]. While standards like IEEE 802.11 define the underlying physical and medium access control (MAC) layers for wireless communication, they do not prescribe standardized metrological methods for evaluating functional data integrity under realistic, noise-heavy operating environments. Testing laboratories are frequently forced to rely on binary "connected/disconnected" pass/fail indicators or qualitative observations, which yield poor measurement reproducibility and high uncertainty across different testing environments.

To address these quality assurance gaps, there is a clear need for a metrologically grounded, quantitative testing framework capable of evaluating integrated wireless performance under realistic operational conditions. This study proposes an empirical testing methodology tailored for smart household devices equipped with IEEE 802.11 b/g/n modules. Using an automated robotic vacuum cleaner as a representative test subject, this work investigates how physical distance and structural obstacles degrade key data transmission metrics.

The primary objective of this research is to establish a repeatable quality assurance framework for evaluating wireless interface stability in smart appliances. To accomplish this objective, the study addresses three specific research tasks:

1. Identify and measure the primary physical and network layer metrics—specifically RSSI, packet loss, latency, and jitter—that characterize connection stability under simulated residential noise.
2. Develop a composite Integral Connection Quality Index (Q) that normalizes multi-metric data and applies expert weighting based on parameter impact on device functionality.
3. Establish quantitative operational boundaries and pass/fail acceptance criteria across variable physical ranges and structural partition setups.

2. Materials and Methods

2.1. Test Subject and Environmental Parameters

We evaluated an IEEE 802.11 b/g/n Wi-Fi module embedded within a commercial robotic vacuum cleaner that features mobile app control and cloud telemetry.

Testing took place in a residential layout designed to replicate everyday environments. The space included concrete load-bearing walls, interior drywall partitions, household furniture, ambient electromagnetic noise, and competing 2.4 GHz network traffic.

2.2. Test Equipment and Instruments

The laboratory setup included:

- A robotic vacuum cleaner equipped with an integrated IEEE 802.11 b/g/n wireless module.
- A dual-band router operating on standard 2.4 GHz and 5.0 GHz bands.
- A dedicated workstation running Wireshark (v4.0.8) alongside RF packet captures for real-time telemetry logging.

2.3. Testing Procedure and Metric Selection

We tracked four core physical and network metrics:

1. **RSSI** (*Received Signal Strength Indicator*), expressed in dBm.
2. **Packet Loss Rate** (L), expressed as a percentage (%).
3. **Latency** (T), representing round-trip time in milliseconds (ms).
4. **Jitter** (J), measuring latency variation in milliseconds (ms).

© Central Asian Scientific Journal, 2026

Measurements were collected at fixed intervals of 1 m, 5 m, and 10 m under both direct Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions through structural walls. To limit random errors, we ran $n \ge 30$ test cycles for every single physical configuration.

2.4. Mathematical Modeling of the Integral Index

To synthesize multi-metric operational data into a single decision-making indicator, a composite **Integral Quality Index** (Q) was developed. Each measured metric was converted to a dimensionless normalized value , where 1 denotes ideal performance and 0 indicates total signal failure:

Where represents the weighting coefficient assigned to parameter , constrained by

Weighting coefficients were assigned through expert evaluation based on functional impact during appliance operation. For the robotic vacuum cleaner, packet loss rate was assigned the highest weighting factor due to its critical role in maintaining command integrity:

- (RSSI) = 0.3
- (Packet Loss) = 0.4
- (Latency) = 0.2
- (Jitter) = 0.1

2.5. Statistical Data Processing

Measurement data were processed using standard statistical techniques to evaluate repeatability and reproducibility [9]:

- Sample arithmetic mean ()
- Standard deviation (
- Coefficient of variation (CV)
- Expanded measurement uncertainty calculated at a 95% confidence level ()

3. Results and Discussion

3.1. Experimental Measurement Analysis

Table 1 summarizes the empirical measurement results recorded across different operational distances.

Table 1. Summarizes the recorded network parameters as distance and structural barriers increased.

Distance (m)	RSSI (dBm)	Packet Loss Rate (%)	Latency (ms)	Jitter (ms)
1	-38	0.2	12	3
5	-55	1.1	18	5
10	-71	4.8	35	11

The findings demonstrate a non-linear relationship between distance, signal strength, and transfer errors. As distance increased 1 m to 10 m with intervening obstacles, signal strength decreased to – 71 dBm. Crossing the – 70 dBm threshold triggered a steep increase in packet loss rate (>4.5%) and doubled latency times (35 ms).

3.2. Evaluation of the Integral Quality Index

Applying the mathematical model yielded the composite Q values presented in Table 2.

Table 2. Calculated Integral Quality Index (Q) across distance setups.

Distance (m)	**Integral Quality Index (Q)**	**Functional State**
1	**0.94**	Optimal operation
5	**0.81**	Stable operation
10	**0.52**	High risk of control loss

When Q drops below **0.60**, device functionality deteriorates significantly, manifesting in failed mobile app synchronization, delayed execution of navigation commands, and potential connection drops.

3.3. Discussion and Comparative Context

Unlike classic compliance testing that stops at electrical safety checks [3], [9], our methodology integrates wireless data integrity directly into the metrological assessment.

The low coefficient of variation (CV < 8%) across test cycles confirms strong reproducibility under real-world residential interference conditions. Integrating the composite metric Q enables testing laboratories to transition from qualitative pass/fail observations to quantitative quality profiling [4], [5], [8].

Study Limitations: Tests were restricted to 2.4 GHz IEEE 802.11 b/g/n protocols on a single device class. Follow-up research will expand this framework to cover Wi-Fi 6 (802.11ax), Bluetooth Mesh, and Matter protocols across multi-device networks.

4. Conclusions

1. Traditional compliance protocols for household electronics insufficiently evaluate wireless communication reliability, creating quality assurance gaps in smart appliance testing.
2. Signal degradation below – 70 dBm serves as a key threshold, inducing a sharp rise in packet loss (>4.5 %) and signal delay that disrupts app control.
3. The proposed Integral Quality Index (Q) effectively consolidates RSSI, packet loss, latency, and jitter into an objective quantitative compliance metric.
4. Statistical evaluation proved high test reproducibility (CV < 8%) under variable environmental conditions.
5. The developed methodology provides a practical framework for accredited testing centers and manufacturers to establish objective product acceptance criteria and reduce consumer warranty claims.

References:

1. International Organization for Standardization, & International Electrotechnical Commission. (2008). *ISO/IEC Guide 98-3:2008 Uncertainty of measurement — Part 3: Guide to the expression of uncertainty in measurement (GUM:1995)*. ISO.
2. International Telecommunication Union. (2021). *Overview of the Internet of Things* (Recommendation ITU-T Y.2060). ITU.
3. IEEE Standards Association. (2016). *IEEE Std 802.11-2016: IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements*. IEEE.
4. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1–31. https://doi.org/10.1016/j.comcom.2014.09.008
5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
6. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
7. Gast, M. S. (2013). *802.11 Wireless networks: The definitive guide* (2nd ed.). O'Reilly Media.
8. Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2014). A survey on Internet of Things from industrial market perspective. *IEEE Access*, 2, 1660–1679. https://doi.org/10.1109/ACCESS.2014.2379034
9. Montgomery, D. C. (2019). *Introduction to statistical quality control* (8th ed.). Wiley.

© Central Asian Scientific Journal, 2026