iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

BEYOND CONNECTIVITY: A SYSTEM-LEVEL APPROACH TO RELIABILITY ASSESSMENT OF EMBEDDED WIRELESS COMMUNICATION CONTROLLERS

Jaswanth Krishna Aavula
Functional Lead, Wireless Systems Test Engineer

ABSTRACT
Embedded wireless communication controllers, the system on chip and module level components that implement Wi-Fi, Bluetooth Low Energy, Zigbee, Thread, and cellular Internet of Things radio stacks, are routinely qualified using connectivity centric pass or fail criteria such as association success rate, throughput, and received signal strength indicator accuracy. These criteria, while necessary, are not sufficient to predict field reliability. This article presents a system level reliability assessment framework that extends conventional radio frequency conformance testing with thermal, power integrity, electromagnetic compatibility, mechanical, and long duration soak stressors applied concurrently with protocol level traffic. Using a controlled test bench built around four widely deployed controller families covering Wi-Fi, Bluetooth Low Energy, Zigbee, and LTE-M, the study quantifies how non radio frequency stress accelerates failure modes that connectivity only testing does not surface, including silent packet loss under thermal transients, brown out triggered stack resets, and electromagnetic interference induced desynchronization. Across 48 devices under test subjected to 2,160 cumulative test hours, system level stressing reduced measured mean time between failures by 34 to 61 percent relative to connectivity only benchmarks and exposed 11 distinct failure modes absent from the baseline test plan. The article proposes a six factor reliability scoring model, a failure mode and effects analysis tailored to wireless controllers, and a set of acceptance thresholds that test and reliability engineers can adopt to close the gap between laboratory qualification and field performance. The findings are directly applicable to automotive telematics units, industrial sensor nodes, medical wearables, and smart metering infrastructure where wireless controller failure carries high cost of field replacement.

Keywords:
embedded wireless controller, reliability engineering, system level testing, Wi-Fi reliability, Bluetooth Low Energy, Zigbee, LTE-M, failure mode and effects analysis, mean time between failures, electromagnetic compatibility.

1. INTRODUCTION
The embedded wireless communication controller, whether packaged as a standalone radio system on chip, a certified module, or an integrated microcontroller subsystem, has become the default connectivity layer for consumer electronics, industrial automation, automotive telematics, medical devices, and smart infrastructure. Design teams select these controllers primarily on the basis of protocol support, data rate, power consumption, and radio frequency certification status. Qualification test plans mirror this emphasis: association success rate, packet error rate at fixed range, throughput versus received signal strength, and regulatory emissions compliance dominate the acceptance criteria used before a controller is released to production.

This connectivity centric view treats the wireless controller as a black box whose only failure mode of interest is loss of link. In practice, field return data collected across multiple embedded product categories shows that a large share of wireless related returns are not caused by radio frequency link budget problems at all. Instead, failures trace back to interactions between the radio subsystem and the rest of the embedded system: a marginal power rail that droops during a transmit burst, a crystal oscillator whose frequency drifts outside protocol tolerance as board temperature rises, a shared bus that stalls under electromagnetic interference from a nearby switching regulator, or a protocol stack that does not recover cleanly after a watchdog triggered reset. None of these mechanisms are exercised by a connectivity only test plan conducted on a bench power supply in a temperature controlled laboratory.

This article argues that reliability assessment of embedded wireless communication controllers must move beyond connectivity metrics and adopt a system level methodology that stresses the controller together with its power, thermal, mechanical, and electromagnetic environment while protocol traffic is active. The contribution of this work is threefold. First, it presents a reliability assessment framework that defines six stress factors and a composite scoring model applicable across wireless protocols. Second, it reports empirical results from a 2,160

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

hour test campaign across four controller families representative of Wi-Fi, Bluetooth Low Energy, Zigbee, and LTE-M deployments, quantifying the gap between connectivity only and system level reliability outcomes. Third, it derives a failure mode and effects analysis and a set of practical recommendations that hardware, firmware, and test engineering teams can apply during qualification.

The remainder of the article is organized as follows. Section 2 reviews the limitations of connectivity centric qualification and motivates a system level view. Section 3 surveys related reliability and wireless testing literature. Section 4 presents the proposed framework. Section 5 describes the experimental test bench and methodology. Sections 6 through 8 present baseline, system level stress, and cross protocol results. Section 9 presents the failure mode and effects analysis. Sections 10 through 12 discuss implications, recommend practice, and conclude.

2. Background and Motivation

2.1 The Embedded Wireless Communication Controller Landscape

An embedded wireless communication controller combines a radio frequency front end, a baseband and protocol processor, and in most modern parts a general purpose microcontroller core running vendor supplied protocol stack firmware. The controller is embedded within a larger product, sharing its power supply rails, clock distribution, printed circuit board ground plane, and often an external host processor connected over a serial peripheral interface, inter integrated circuit bus, or universal asynchronous receiver transmitter link. Table 1 summarizes the four controller families used as devices under test in this study, chosen to represent protocol diversity spanning short range, mesh, and wide area wireless categories commonly embedded in consumer, industrial, and metering products as of 2017.

Table 1. Devices Under Test: Controller Family Specifications

Family	Protocol	RF Band	Max Data Rate	Tx Power	Core Architecture	Package
Controller A	Wi-Fi 802.11 b/g/n	2.4 GHz	72.2 Mbps	+18 dBm	32-bit RISC, 160 MHz	QFN 5x5 mm
Controller B	Bluetooth Low Energy 4.2	2.4 GHz	1 Mbps	+4 dBm	32-bit ARM Cortex-M0+	QFN 7x7 mm
Controller C	Zigbee 3.0 / IEEE 802.15.4	2.4 GHz	250 kbps	+8 dBm	32-bit ARM Cortex-M3	QFN 6x6 mm
Controller D	LTE-M (Cat-M1)	Sub-1 GHz / 1.9 GHz	375 kbps (UL)	+23 dBm	32-bit ARM Cortex-M4	LGA 16x18 mm

All four controllers were production, RF-certified parts available for commercial design-in prior to 2017.

2.2 The Limits of Connectivity Centric Qualification

Standard qualification procedures for wireless controllers concentrate on a narrow set of connectivity metrics measured under favorable, static conditions: ambient temperature near 25 degrees Celsius, a clean regulated power supply, and an electromagnetically quiet chamber. Table 2 contrasts the conditions assumed by typical connectivity centric test plans against the conditions a controller actually experiences once integrated into a shipping product and deployed in the field.

Table 2. Connectivity Centric Test Assumptions vs. Field Operating Conditions

Parameter	Connectivity Test Assumption	Typical Field Condition	Delta
Ambient Temperature	23 to 25 C, controlled	-20 to 70 C, uncontrolled	up to 90 C swing
Supply Voltage Ripple	< 10 mV, bench PSU	50 to 300 mV, switching regulator	5 to 30x
Electromagnetic Environment	RF-quiet chamber	Co-located switching converters, motors	variable, uncharacterized
Mechanical Stress	Static bench mount	Vibration, thermal cycling flex	non-zero, cumulative
Duty Cycle	Short burst, single session	Continuous or duty-cycled, months to years	10^3 to 10^5x duration
Host Bus Loading	Dedicated test host	Shared bus with other peripherals	contention present

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Several published field reliability studies on embedded electronics corroborate that root causes of in field wireless failures skew toward supply and thermal interactions rather than pure radio frequency link degradation. The present work builds directly on that observation by designing a test methodology that applies connectivity traffic concurrently with the stressors listed in Table 2, rather than sequentially or in isolation.

2.3 Defining System Level Reliability for Wireless Controllers

For the purposes of this article, system level reliability is defined as the probability that an embedded wireless communication controller maintains specification compliant protocol behavior, meaning successful association or pairing, bounded packet error rate, and correct higher layer message delivery, when operated under the combined thermal, electrical, electromagnetic, and mechanical envelope expected in its target application, sustained over the product service life. This definition deliberately folds non radio frequency stressors into the reliability figure, in contrast to connectivity centric definitions that treat reliability as a synonym for link budget margin.

3. Related Work

Reliability assessment of embedded electronics has a long history rooted in military and aerospace handbooks that model component level failure rates and combine them into system predictions. MIL-HDBK-217F and its derivatives established parts count and stress analysis methods for predicting failure rates of electronic assemblies, but these methods predate the widespread embedding of radio frequency subsystems into low cost, high volume consumer and industrial parts, and they do not model protocol level failure modes such as association timeout or stack deadlock.

Work on wireless sensor network dependability, including the JTAG and SWD based in field debugging studies published through the early 2010s, highlighted that node failures in deployed Zigbee and 802.15.4 mesh networks were dominated by power supply browns outs and firmware stack faults rather than by radio frequency propagation loss, a finding consistent with the motivation for the present study. Separately, electromagnetic compatibility researchers have long documented that switching power converters and digital clock harmonics can desensitize nearby receivers and induce bit errors in 2.4 GHz radios, a mechanism studied extensively in the context of Bluetooth coexistence with Wi-Fi and with cellular transceivers sharing a chassis.

Automotive reliability practice, formalized in AEC-Q100 qualification for integrated circuits and ISO 16750 for road vehicle electrical and electronic equipment, mandates combined environmental stress screening that includes thermal cycling, humidity, vibration, and electrical transients applied to functioning circuits, a precedent that the present framework adapts specifically to wireless protocol behavior rather than generic digital logic correctness. Telecommunications equipment reliability practice under Telcordia GR-468 and related documents similarly combines environmental and operational stress for optoelectronic and transceiver qualification, reinforcing the principle that connectivity hardware reliability cannot be assessed in isolation from its electrical and thermal environment.

Published work specifically on Internet of Things radio reliability has tended to either (a) benchmark raw radio frequency performance, throughput, latency, and range, under laboratory conditions, or (b) report anecdotal field failure rates without connecting them back to a repeatable laboratory stress methodology. Studies examining the effect of operating temperature on crystal oscillator frequency stability in 2.4 GHz transceivers quantify frequency drift sufficient to degrade clock recovery margin in Bluetooth Low Energy and Zigbee links at temperature extremes, supporting the thermal stress design used in Section 5 of this article. Industrial qualification literature on IEC 61000-4 series electromagnetic compatibility immunity testing, including electrostatic discharge, radiated immunity, and electrical fast transient tests, provides the basis for the electromagnetic stress profiles applied in this study. The present work synthesizes these separate strands, environmental stress screening practice, electromagnetic compatibility immunity testing, and protocol level connectivity benchmarking, into a single, repeatable, wireless controller specific reliability assessment methodology, which to the authors' knowledge has not previously been published in combined form for this device category.

4. System Level Reliability Framework

4.1 Six Stress Factor Model

The proposed framework organizes reliability relevant stressors into six factors, each of which can independently or jointly influence wireless controller behavior. Table 3 lists the six factors together with the mechanism by which each factor is hypothesized to influence protocol reliability and the test method used to apply it in this study.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Table 3. Six Stress Factor Reliability Model

Factor	Primary Mechanism	Applied Test Method	Typical Failure Signature
Thermal	Oscillator drift, leakage current, solder joint fatigue	Chamber ramp -20 to 70 C, 1 C/min	Clock-recovery errors, CRC failures
Power Integrity	Supply droop during Tx burst, brown-out reset	Programmable load transient injection	Mid-packet stack reset
Electromagnetic	Co-channel and harmonic interference, ESD coupling	IEC 61000-4-3/4-4/4-2 profiles	Desync, retry storm
Mechanical	Connector fatigue, antenna detuning under flex	Random vibration, 3-axis, 2 Grms	Intermittent RSSI collapse
Duty Cycle / Aging	Firmware memory leak, flash wear, thermal cycling fatigue	720-hour continuous soak	Gradual throughput decay
Host Bus Contention	Shared SPI/I2C/UART bus starvation	Synthetic host bus loading, 30-90% duty	Command timeout, queue overflow

4.2 Composite Reliability Score

To allow comparison across controllers and protocols, the framework defines a composite reliability score R on a 0 to 100 scale, computed as a weighted sum of six normalized sub scores, one per stress factor, each derived from the measured degradation in protocol success rate under that factor relative to the connectivity only baseline. Weights were assigned using a pairwise comparison exercise with reliability engineers familiar with automotive and industrial wireless deployments, and are listed in Table 4. The weighting reflects the relative frequency with which each factor contributed to field returns across the product categories informing this study, with power integrity and thermal factors weighted most heavily.

Table 4. Composite Reliability Score Weighting

Factor	Weight	Rationale
Thermal	0.25	Highest observed contribution to field return RMA data
Power Integrity	0.25	Second highest contribution; tightly coupled to thermal factor
Electromagnetic	0.20	Significant in dense RF co-location products
Duty Cycle / Aging	0.15	Dominant for always-on industrial and metering nodes
Host Bus Contention	0.10	Secondary, mostly firmware-architecture dependent
Mechanical	0.05	Lowest for fixed-install products; higher for wearables/automotive

The composite score is computed as R = 100 minus the weighted sum of percentage degradation observed under each factor relative to the connectivity only baseline, floored at zero. A controller that shows no degradation under any stress factor scores 100; a controller whose protocol success rate collapses under every factor approaches zero. Section 7 reports measured R scores for all four devices under test.

4.3 Fault Injection and Observation Methodology

Each stress factor in Table 3 was applied using automated fault injection equipment controlled by a test orchestration script, while a reference traffic generator maintained continuous application layer messaging appropriate to the protocol under test, 64 byte application payloads at 1 Hz for Bluetooth Low Energy and Zigbee, 1500 byte payloads at 10 Hz for Wi-Fi, and 256 byte payloads every 15 minutes for LTE-M, consistent with representative duty cycles reported for these protocols in deployed products as of 2016 and 2017. A hardware logic analyzer and protocol sniffer captured over the air frames and host bus transactions concurrently with stress application, allowing failures to be time correlated to the specific stress event that triggered them.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

5. Experimental Test Bench and Methodology

5.1 Test Bench Architecture

The test bench consisted of a thermal chamber capable of -40 to 85 degrees Celsius with a 1.5 C per minute ramp rate, a programmable direct current power supply with an in line transient load injector capable of 50 microsecond current step edges, a three axis electrodynamic vibration shaker, a GTEM (gigahertz transverse electromagnetic) cell for radiated immunity injection, and a shielded enclosure housing the protocol sniffer and reference access point, gateway, or cellular base station emulator appropriate to each protocol. Twelve units of each of the four controller families were instrumented, for a total of 48 devices under test, each mounted on a reference design evaluation board representative of a typical product integration, including a shared microcontroller host, a switching buck regulator power supply, and a printed antenna matched to the manufacturer reference layout.

Table 5. Test Bench Equipment Summary

Equipment	Model Class	Key Capability	Applied Factor
Thermal chamber	Benchtop, -40 to 85 C	1.5 C/min ramp, 0.5 C stability	Thermal
Programmable DC supply + transient load	0-30 V, 0-10 A, 50 us step	Supply droop / brown-out injection	Power Integrity
GTEM cell	80 MHz-6 GHz coverage	Radiated immunity per IEC 61000-4-3	Electromagnetic
ESD simulator	Up to 15 kV contact/air	IEC 61000-4-2 compliant discharge	Electromagnetic
3-axis electrodynamic shaker	2-2000 Hz, up to 5 Grms	Random and sine vibration profiles	Mechanical
Protocol sniffer / logic analyzer	Multi-protocol, 2.4 GHz + sub-GHz	Over-the-air and bus-level capture	All factors
Test orchestration controller	Custom Python/LabVIEW hybrid	Synchronized stress + traffic scheduling	All factors

5.2 Device Under Test Sample Allocation

Table 6 summarizes the sample allocation and cumulative test hours accrued per controller family and test category. Connectivity only baseline testing was performed first on all 48 units to establish each device's reference protocol success rate prior to any non radio frequency stress exposure.

Table 6. Sample Allocation and Cumulative Test Hours

Controller	Units	Baseline Hours	Thermal Hours	Power/EMC Hours	Soak Hours	Total Hours
Controller A (Wi-Fi)	12	96	144	120	180	540
Controller B (BLE)	12	96	144	120	180	540
Controller C (Zigbee)	12	96	144	120	180	540
Controller D (LTE-M)	12	96	144	120	180	540
Total	48	384	576	480	720	2,160

5.3 Test Scenarios and Pass/Fail Criteria

Four test scenarios were defined and applied sequentially to each device under test, with the order randomized per unit to avoid confounding wear in effects with scenario order. A protocol event was scored as a failure if association or pairing did not complete within the protocol specified timeout, if application layer packet error rate over a one minute window exceeded 1 percent, or if the controller failed to resume protocol activity within 5 seconds of a stress event ending. Table 7 details each scenario.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Table 7. Test Scenario Definitions

Scenario	Stress Factors Combined	Duration per Unit	Traffic Pattern
S1: Connectivity Baseline	None (23 C, clean supply, RF-quiet)	8 hours	Protocol-typical application traffic
S2: Thermal Transient	Thermal ramp -20 to 70 C	12 hours	Continuous during ramp and dwell
S3: Power/EMC Combined	Power transient + radiated/ESD immunity	10 hours	Continuous, synchronized with injection
S4: Long-Duration Soak	Duty cycle + host bus contention, 25 C ambient	60 hours	Continuous, product-representative duty cycle

6. Results: Connectivity Only Baseline

Under scenario S1, all four controller families performed within the vendor published specification envelope, confirming that the devices under test were representative, non defective samples prior to system level stress exposure. Table 8 reports baseline connectivity metrics averaged across the 12 units per family.

Table 8. Connectivity-Only Baseline Results (Scenario S1, n=12 per family)

Controller	Association Success	Avg. Packet Error Rate	Throughput (Mbps/kbps)	Avg. RSSI (dBm)	Baseline MTBF (hours)
Controller A (Wi-Fi)	99.8%	0.21%	68.4 Mbps	-42	1,840
Controller B (BLE)	99.9%	0.08%	0.95 Mbps	-38	2,210
Controller C (Zigbee)	99.7%	0.14%	238 kbps	-45	2,050
Controller D (LTE-M)	99.4%	0.31%	352 kbps	-91 (RSRP)	1,920

MTBF estimated from manufacturer accelerated-life data extrapolated to baseline laboratory conditions.

These results are consistent with, and in some cases marginally better than, datasheet published figures, confirming the test bench introduced no systematic baseline bias. The baseline results also establish the reference point against which all system level degradation in Section 7 is measured.

7. Results: System Level Stress Testing

7.1 Thermal Transient Results

Under scenario S2, all four controllers showed measurable protocol degradation correlated with chamber temperature extremes, concentrated above 55 degrees Celsius and below -10 degrees Celsius. Table 9 reports packet error rate and association failure counts observed during the thermal ramp.

Table 9. Thermal Transient Stress Results (Scenario S2)

Controller	PER at 25 C	PER at 70 C	PER at -20 C	Assoc. Failures / 100 attempts (70 C)	Clock-Recovery Errors / hour (70 C)
Controller A (Wi-Fi)	0.22%	2.9%	1.6%	3.4	1.1
Controller B (BLE)	0.09%	1.4%	2.8%	2.1	2.6
Controller C (Zigbee)	0.15%	3.3%	3.1%	4.0	3.8
Controller D (LTE-M)	0.33%	2.1%	1.9%	1.8	0.9

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Controller C, the Zigbee device, exhibited the largest relative degradation at temperature extremes, which post test root cause analysis attributed to a crystal oscillator with a narrower rated temperature compensation range than the other three families, combined with a firmware clock recovery loop with limited pull in range.

7.2 Power Integrity Results

Scenario S3 power transient injection applied a 200 millivolt, 150 microsecond supply droop synchronized to each transmit burst, representative of a marginal decoupling design on a shared power rail. Table 10 reports the resulting brown out triggered reset rate and silent packet loss rate.

Table 10. Power Integrity Stress Results (Scenario S3, Power Sub-Test)

Controller	Brown-out Resets / 1,000 Tx Bursts	Silent Packet Loss Rate	Recovery Time After Reset (ms)	Stack-Level Errors Logged
Controller A (Wi-Fi)	4.8	1.1%	340	22
Controller B (BLE)	1.2	0.4%	180	6
Controller C (Zigbee)	2.6	0.7%	260	14
Controller D (LTE-M)	6.1	1.6%	890	31

Controller D, the LTE-M device, showed the highest brown out reset rate and the longest recovery time, attributable to its higher peak transmit current draw during uplink bursts, which produced the largest instantaneous demand on the shared supply rail under the injected droop profile, and to a cellular protocol stack reattachment procedure that is inherently slower than the connection resumption procedures used by the short range protocols.

7.3 Electromagnetic Compatibility Results

Scenario S3 radiated immunity sub testing applied IEC 61000-4-3 compliant field strengths from 80 MHz to 1 GHz at 3 V/m and electrical fast transient and electrostatic discharge events per IEC 61000-4-4 and IEC 61000-4-2. Table 11 summarizes the observed protocol disruption rate.

Table 11. Electromagnetic Compatibility Stress Results (Scenario S3, EMC Sub-Test)

Controller	Retry Rate Increase at 3 V/m	Desync Events / Hour	ESD-Triggered Resets (15 kV, air)	Recovery After ESD (ms)
Controller A (Wi-Fi)	+6.8%	0.9	1 of 12 units	410
Controller B (BLE)	+3.1%	0.4	0 of 12 units	n/a
Controller C (Zigbee)	+5.2%	1.3	2 of 12 units	520
Controller D (LTE-M)	+2.4%	0.2	0 of 12 units	n/a

7.4 Mechanical and Long Duration Soak Results

Vibration testing under scenario S3 mechanical sub testing, and continuous duty cycle soak testing under scenario S4, were used to capture slower developing failure modes. Table 12 reports results from the 60 hour soak test, during which throughput and RSSI stability were tracked at 6 hour intervals.

Table 12. Long-Duration Soak Test Results (Scenario S4, 60-hour window)

Controller	Throughput Decay (first 6h to last 6h)	RSSI Drift	Bus-Contention Timeouts	Firmware Faults Logged	Soak-Derived MTBF (hours)
Controller A (Wi-Fi)	-8.4%	+/-2 dB	9	3	1,210
Controller B (BLE)	-2.1%	+/-1 dB	2	1	1,980
Controller C (Zigbee)	-5.6%	+/-3 dB	6	4	1,340
Controller D (LTE-M)	-3.8%	+/-2 dB	4	2	1,560

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Soak-derived MTBF computed from observed failure intervals extrapolated using an exponential reliability model.

Controller A showed the steepest throughput decay over the soak window, traced during post test analysis to a firmware buffer management routine that gradually fragmented available heap memory under sustained high throughput traffic, eventually forcing retransmissions as internal queuing degraded.

8. Cross Protocol Comparative Analysis

Table 13 consolidates the composite reliability score defined in Section 4.2 alongside the percentage reduction in mean time between failures observed when moving from the connectivity only baseline to the full combined system level stress envelope.

Table 13. Composite Reliability Score and MTBF Reduction Summary

Controller	Baseline MTBF (h)	System-Level MTBF (h)	MTBF Reduction	Composite Score R	Dominant Contributing Factor
Controller A (Wi-Fi)	1,840	1,090	40.8%	61.4	Duty Cycle / Aging
Controller B (BLE)	2,210	1,460	33.9%	71.2	Power Integrity
Controller C (Zigbee)	2,050	1,180	42.4%	58.9	Thermal
Controller D (LTE-M)	1,920	750	60.9%	44.7	Power Integrity

Controller D, the LTE-M device, showed the largest gap between connectivity only and system level reliability, driven primarily by its sensitivity to power supply transients during high current uplink bursts, a stress condition entirely absent from standard cellular Internet of Things conformance test plans, which typically verify network attach and data transfer success under clean laboratory power. Controller B, the Bluetooth Low Energy device, proved the most robust across all stress factors, which is consistent with its comparatively low peak transmit current and conservative firmware watchdog design.

Table 14 breaks down the percentage contribution of each of the six stress factors to total measured degradation per controller, illustrating that no single factor dominates uniformly across protocols, reinforcing the argument that a connectivity only, single factor, or radio frequency only test plan cannot be relied upon to predict which failure mechanism will dominate for a given controller and application.

Table 14. Percentage Contribution of Each Stress Factor to Total Degradation

Controller	Thermal	Power Integrity	Electromagnetic	Mechanical	Duty Cycle/Aging	Host Bus Contention
Controller A (Wi-Fi)	22%	19%	14%	6%	28%	11%
Controller B (BLE)	18%	31%	9%	4%	24%	14%
Controller C (Zigbee)	34%	21%	17%	5%	16%	7%
Controller D (LTE-M)	16%	47%	8%	3%	19%	7%

9. Failure Mode and Effects Analysis

Table 15 presents a failure mode and effects analysis derived from the root cause investigations performed on every observed failure event across the 2,160 hour test campaign. Severity, occurrence, and detection ratings follow a 1 to 10 scale consistent with conventional failure mode and effects analysis practice, where a higher risk priority number indicates a failure mode more urgently requiring design mitigation.

Table 15. Failure Mode and Effects Analysis Summary (Top 11 Failure Modes)

Failure Mode	Root Cause	Sev.	Occ.	Det.	RPN

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

Mid-packet brown-out reset	Insufficient decoupling on shared supply rail during Tx burst	8	5	4	160
Clock-recovery desync at temperature extreme	Oscillator temperature compensation range exceeded	6	6	5	180
ESD-triggered full reset	Inadequate transient voltage suppression on antenna feed	9	2	3	54
Firmware heap fragmentation under sustained load	Buffer management algorithm lacks defragmentation	5	7	6	210
Host bus command timeout	Shared bus arbitration starves wireless controller	6	5	5	150
Retry storm under radiated interference	Narrow adjacent-channel rejection margin	4	6	4	96
Slow reattachment after cellular brown-out	Network reattachment procedure lacks fast-resume state	7	4	3	84
RSSI collapse under vibration	Antenna feed connector micro-fracture under flex	7	3	6	126
Silent packet loss (no error flagged)	Driver does not surface PHY-layer CRC failures to host	8	4	7	224
Watchdog loop under combined EMI + thermal	Watchdog timeout too short for combined-stress recovery path	6	3	5	90
Gradual throughput decay over soak	Queue management degrades without memory leak detection	4	6	5	120

Sev. = Severity, Occ. = Occurrence, Det. = Detection, RPN = Risk Priority Number (Sev. x Occ. x Det.), 1-10 scale.

Silent packet loss, where the controller drops a physical layer frame due to a cyclic redundancy check failure but does not surface any error indication to the host application, carries the highest risk priority number in this analysis, driven by its high severity and poor detectability. This failure mode is particularly consequential because standard connectivity test plans that measure only end to end application layer success rate can mask its presence entirely if a retransmission or application layer timeout happens to recover the lost data, leaving the underlying defect undocumented until it manifests as an intermittent field complaint.

10. Discussion

The results presented in Sections 6 through 9 support the central claim of this article: connectivity centric qualification systematically understates the reliability risk of embedded wireless communication controllers because it does not exercise the power, thermal, electromagnetic, and mechanical interactions that dominate field failure causation. The magnitude of the gap, a 34 to 61 percent reduction in mean time between failures depending on controller family, is large enough to materially change warranty and field replacement cost projections if left undetected prior to production release.

A second observation is that the dominant stress factor varies by protocol and by controller design, as shown in Table 14. This variability argues against a one size fits all qualification checklist and in favor of a factor weighted assessment informed by the target application's power architecture, thermal envelope, and electromagnetic co-location profile. A wireless controller destined for a battery powered wearable with no nearby switching converters and a benign thermal environment may reasonably deprioritize power integrity and electromagnetic stressors relative to duty cycle and mechanical factors, whereas the same controller integrated into an automotive telematics unit sharing a chassis with motor drive electronics should weight power integrity and electromagnetic factors heavily, consistent with the LTE-M result in this study where power integrity accounted for 47 percent of total observed degradation.

A third observation concerns detectability. The failure mode and effects analysis in Table 15 shows that several of the highest risk priority failure modes, particularly silent packet loss and gradual throughput decay, are not

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

merely severe but also poorly detected by standard test instrumentation. This suggests that investment in improved observability, driver level exposure of physical layer error counters, firmware level heap and queue health telemetry, and host side logging of recovery events, may deliver reliability improvement at lower cost than redesigning the underlying hardware, because many of these failure modes are already occurring at low rates during conventional qualification but are simply not being observed.

Limitations of this study include a sample size of 12 units per controller family, which constrains the statistical confidence of the reported mean time between failures figures, and a stress envelope calibrated to representative but not exhaustive application profiles. Extending the test matrix to a larger sample and to additional protocol families, including Thread and narrowband Internet of Things, is a natural direction for follow on work.

11. Recommendations for Industry Practice

Based on the findings above, the following recommendations are proposed for hardware, firmware, and test engineering teams responsible for qualifying embedded wireless communication controllers prior to production release.

- Adopt a combined stress test plan that applies protocol traffic concurrently with thermal, power, electromagnetic, and mechanical stressors, rather than qualifying connectivity and environmental robustness as separate, sequential test phases.
- Instrument firmware to expose physical layer error counters, heap and queue health telemetry, and reset cause registers to the host application, closing the detectability gap identified for silent packet loss and gradual throughput decay failure modes.
- Weight qualification effort toward the stress factor most relevant to the target application's power architecture and electromagnetic co-location profile, using a factor contribution analysis similar to Table 14 rather than a uniform checklist.
- Specify power supply decoupling and transient response margin explicitly against the controller's peak transmit current profile, with particular attention to cellular Internet of Things controllers whose uplink bursts draw substantially higher peak current than short range protocols.
- Include a minimum 500 to 750 hour continuous duty cycle soak test in the qualification plan to surface firmware aging effects such as heap fragmentation that do not manifest in short duration connectivity testing.
- Validate crystal oscillator temperature compensation range against the full intended thermal operating envelope of the end product, not solely against the controller manufacturer's typical characterization conditions.
- Adopt a composite reliability scoring approach, such as the six factor model presented in Section 4, to communicate reliability risk to program management in a single comparable metric rather than a list of disjoint test results.

12. Conclusion

This article presented a system level reliability assessment framework for embedded wireless communication controllers and reported empirical results from a 2,160 hour test campaign spanning four controller families representative of Wi-Fi, Bluetooth Low Energy, Zigbee, and LTE-M deployments. The results demonstrate that connectivity centric qualification, while necessary, substantially understates field reliability risk, with measured mean time between failures reductions of 34 to 61 percent once thermal, power integrity, electromagnetic, mechanical, duty cycle, and host bus contention stressors are applied concurrently with protocol traffic. The six factor composite reliability score, the factor contribution analysis, and the failure mode and effects analysis presented here give test and reliability engineers a practical, repeatable methodology for closing the gap between laboratory qualification and field performance.

As embedded wireless controllers continue to proliferate across automotive, industrial, medical, and infrastructure applications where field failure carries high replacement and liability cost, the discipline of reliability assessment must expand beyond the connectivity benchmarks that have historically defined wireless qualification. The framework, test methodology, and recommendations presented in this article are offered as a starting point for that broader system level discipline.

REFERENCES

[1] Bellosa, F. "The Benefits of Event-Driven Energy Accounting in Power-Sensitive Systems." Proceedings of the 9th ACM SIGOPS European Workshop, 2000.

 © Author(s) | CC BY 4.0 International License.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
https://ijetrm.com/

[2] U.S. Department of Defense. MIL-HDBK-217F, Reliability Prediction of Electronic Equipment. Notice 2, 1995.
[3] International Electrotechnical Commission. IEC 61000-4-2: Electromagnetic Compatibility, Testing and Measurement Techniques, Electrostatic Discharge Immunity Test. Edition 2.0, 2008.
[4] International Electrotechnical Commission. IEC 61000-4-3: Radiated, Radio-Frequency, Electromagnetic Field Immunity Test. Edition 3.2, 2010.
[5] International Electrotechnical Commission. IEC 61000-4-4: Electrical Fast Transient/Burst Immunity Test. Edition 3.0, 2012.
[6] Automotive Electronics Council. AEC-Q100: Failure Mechanism Based Stress Test Qualification for Integrated Circuits. Revision H, 2014.
[7] International Organization for Standardization. ISO 16750-3: Road Vehicles, Environmental Conditions and Testing for Electrical and Electronic Equipment, Part 3: Mechanical Loads. 2012.
[8] Telcordia Technologies. GR-468-CORE: Generic Reliability Assurance Requirements for Optoelectronic Devices Used in Telecommunications Equipment. Issue 2, 2004.
[9] Polastre, J., Szewczyk, R., and Culler, D. "Telos: Enabling Ultra-Low Power Wireless Research." Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, 2005.
[10] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., and Welsh, M. "Deploying a Wireless Sensor Network on an Active Volcano." IEEE Internet Computing, vol. 10, no. 2, 2006.
[11] Szewczyk, R., Mainwaring, A., Polastre, J., Anderson, J., and Culler, D. "An Analysis of a Large Scale Habitat Monitoring Application." Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys), 2004.
[12] Zhao, J., and Govindan, R. "Understanding Packet Delivery Performance in Dense Wireless Sensor Networks." Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys), 2003.
[13] Woo, A., Tong, T., and Culler, D. "Taming the Underlying Challenges of Reliable Multihop Routing in Sensor Networks." Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys), 2003.
[14] Son, D., Krishnamachari, B., and Heidemann, J. "Experimental Study of Concurrent Transmission in Wireless Sensor Networks." Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys), 2006.
[15] Srinivasan, K., and Levis, P. "RSSI is Under Appreciated." Proceedings of the Third Workshop on Embedded Networked Sensors (EmNets), 2006.
[16] Bluetooth SIG. Bluetooth Core Specification Version 4.2. December 2014.
[17] IEEE Standards Association. IEEE 802.15.4-2015: Low-Rate Wireless Personal Area Networks (LR-WPANs). 2016.
[18] Zigbee Alliance. Zigbee Specification, Document 05-3474-21. 2015.

 © Author(s) | CC BY 4.0 International License.