ID	Component	Issue	Description / Cause	Severity	Likelihood	Risk Level	Fix / Mitigation
R001	EEPROM	Corrupted EEPROM – causes bad config	- `has_activated` flag may become false - Device keeps activating on every boot	Low	Medium	Low	Check if EEPROM is corrupted; if so, restore to default configuration.
R002	EEPROM	EEPROM wear-out over time	- Frequent writes exceed EEPROM write cycle limits - Device fails to save new configurations	Medium	Medium	Medium	Minimize writes, implement wear leveling, validate writes, backup default configs.
R003	EEPROM	Battery-backed RAM loss	- Power loss during critical updates - Device forgets last state or configuration	Medium	Low	Low	Use atomic writes, checksum validation, and power-fail-safe firmware.
R004	Wi-Fi Module	Unable to connect to Wi-Fi (hardware issue)	- Environmental casing damage causes Wi-Fi module failure - Device never activates or sends readings	Very High	Low	High	Add retry counter and timeout for Wi-Fi connection attempts. Add physical indicator (LED or buzzer) to notify user.
R005	Wi-Fi Module	Unable to connect to Wi-Fi (network down)	- Configured Wi-Fi network unavailable or unstable - Access point goes offline	Medium	Medium	Medium	Retry logic with exponential backoff. Cache unsent readings locally. Notify user of network unavailability.
R006	Wi-Fi Module	IP conflicts / DHCP issues	- Network assigns same IP to multiple devices - Device cannot connect reliably	Low-Medium	Medium	Medium	Use DHCP with fallback to static IP, detect conflict, retry connection.
R007	Wi-Fi Module	CoAP server unreachable	- Server down or network partition - Data loss or delayed transmission	High	Medium	High	Retry sending data, store packets locally, log errors for later sync.

ID	Component	Issue	Description / Cause	Severity	Likelihood	Risk Level	Fix / Mitigation
R008	Wi-Fi Module	Firmware communication bugs	- Bugs in CoAP/Wi-Fi stack - Causes data corruption, retries, or device crash	Very High	Low	High	Extensive unit testing, watchdog timers, firmware validation.
R009	Wi-Fi Module	Interference from other RF devices	- Nearby Wi-Fi, Bluetooth, or industrial RF interference - Packet loss or poor connectivity	Medium	Medium	Medium	Retry logic, channel hopping, error correction, QoS on network.
R010	Wi-Fi Module	DNS or server misconfiguration	- Wrong server addresses, expired domain, or certificate issues - Device cannot send readings or update firmware	High	Medium	High	Implement server fallback addresses, certificate validation, and OTA server health checks.
R011	GPS Module	GPS module failure (only set on first boot)	- GPS module fails or disconnected during first boot - Device cannot acquire initial coordinates	Medium	Medium	Medium	Retry GPS fix multiple times during first boot. Fallback to Wi-Fi-based geolocation. Store obtained coordinates in EEPROM.
R012	GPS Module	Weak GPS signal / indoor use	- GPS cannot acquire fix due to obstructions - Location unavailable or inaccurate	Medium	High	High	Fallback to Wi-Fi geolocation. Provide error flag for unavailable GPS.
R013	GPS Module	GPS drift over time	- Aging or software bugs cause inaccurate coordinates	Low-Medium	Medium	Medium	Periodically recalibrate GPS. Compare with network-based positioning.
R014	Firmware / OTA	OTA update failure / corrupted firmware	- OTA downloads incomplete/corrupted firmware - Device crashes on boot	Very High	Medium	Very High	Dual-partition OTA, checksum/digital signature validation, automatic rollback. Log failed updates to server.

ID	Component	Issue	Description / Cause	Severity	Likelihood	Risk Level	Fix / Mitigation
R015	Firmware / OTA	Firmware incompatibility	- New OTA incompatible with hardware revision - Device crashes or misbehaves	Very High	Low	High	Verify hardware version before update. Maintain rollback mechanism.
R016	Firmware / OTA	Partial update / interrupted OTA	- Network failure or power loss during OTA - Corrupted firmware	Very High	Medium	Very High	Dual-partition OTA, checksum verification, automatic rollback.
R017	SIM Module	SIM module connection failure	- SIM card not detected due to poor contact, loose socket, or corrosion - Device cannot register on network	High	Medium	High	Detect SIM presence and registration. Retry initialization with backoff. Alert user if SIM remains undetected.
R018	SIM Module	SIM network unavailability or poor signal	- Device cannot connect due to low signal, roaming restrictions, or network downtime	Medium	High	High	Automatic reconnection attempts with increasing intervals. Store readings locally until connectivity returns.
R019	SIM Module	SIM card expires or is deactivated	- SIM subscription ends or account blocked - Device cannot connect to network	High	Low	Medium	Monitor registration failures. Notify user to replace SIM.
R020	Sensor Module	Corrupted sensor readings	- Data read by chip is invalid - Device sends CoAP packets but server drops them	Very High	Medium	Very High	Notify user if ≥50% of readings are faulty.
R021	Sensor Module	Sensor failure / hardware damage	- Environmental exposure (humidity, vibration, heat) causes sensor malfunction	Very High	Medium	Very High	Monitor sensor health, anomaly detection, notify user.

ID	Component	Issue	Description / Cause	Severity	Likelihood	Risk Level	Fix / Mitigation
R022	Sensor Module	Calibration drift	- Aging sensors cause measurements to gradually become inaccurate	Medium	Medium	Medium	Implement periodic recalibration or self-calibration routines.
R023	Power / Battery	Low battery	- Extended operation without recharge or failed power-saving routines - Device shuts down unexpectedly	High	Medium	High	Battery monitoring, low-battery alerts, controlled shutdown.
R024	Power / Battery	Power surge or spike	- External power instability - MCU or peripheral damage	Very High	Low	High	Surge protection, voltage regulators, fuses.
R025	Power / Battery	Battery leakage or swelling	- Poor battery quality or overcharging - Physical damage or short-circuit risk	Very High	Low	High	Battery monitoring, overcharge protection, high-quality batteries.
R026	Power / Battery	Excessive current draw	- Short circuits or sensor failure - Rapid battery drain or device shutdown	High	Medium	High	Current limiting, fuse protection, monitor energy usage.
R027	Security	Unauthorized access / hacking	- Weak Wi-Fi password, exposed ports, unencrypted communication - Firmware tampering or data leak	Very High	Medium	Very High	Secure OTA, encrypt CoAP/Wi-Fi traffic, strong authentication.
R028	Security	Data tampering in transit	- Man-in-the-middle attack alters device data	High	Medium	High	Use HMAC, TLS/DTLS over CoAP to secure communication.
R029	Security	Compromised OTA server	- Attacker pushes malicious firmware	Very High	Low	High	Sign firmware, verify signatures, secure OTA channels.
R030	Security	Replay attacks on communication	- Attacker resends old CoAP packets	High	Medium	High	Include timestamps, sequence numbers, or nonces in packets.

ID	Component	Issue	Description / Cause	Severity	Likelihood	Risk Level	Fix / Mitigation
R031	User / Operational	Misconfigured device	- User inputs wrong node ID, Wi-Fi credentials, or SIM details	Medium	Medium	Medium	Input validation, configuration verification, setup wizards.
R032	User / Operational	Delayed maintenance / calibration	- Users ignore service intervals - Sensors drift, battery degrades, GPS outdated	Medium	Medium	Medium	Notify users periodically, automatic health checks, remote diagnostics.
R033	Environmental / Physical	Extreme temperature or humidity exposure	- Device placed outdoors or in industrial environments - Sensor drift, MCU malfunction, battery degradation	High	Medium	High	Specify operational limits, environmental shielding, conformal coating.
R034	Environmental / Physical	Physical damage / tampering	- Accidental drops, vandalism, or unauthorized opening - Sensor or module damage	Very High	Low	High	Rugged enclosure, tamper-evident design, alert on enclosure breach.
R035	Security	Serial console exposure	- Unauthorized person connects to the serial console and observes device operation or sensitive data - Could reveal GPS, network credentials, HMAC keys, or operational state	High	Medium	High	Disable unnecessary serial output in production firmware, require authentication for console access, log serial access attempts.