Software & Firmware Anomalies (Runtime Diagnostics):

If the hardware passes visual inspection, boot the system in an isolated test-bench environment and pull raw telemetry using tools like HWiNFO, CPU-Z, or command-line tools like dmidecode (Linux).

1. **Generic, Incomplete, or Blank SPD Fields:** Counterfeiters often forget to populate or correctly match all fields when flashing a fake SPD profile. Watch out for serial numbers that read exactly 00000000, 12345678, or Unknown. Check if the Manufacturer ID matches the brand on the stick's sticker. If the sticker says Micron but the software reads a generic or different silicon manufacturer, the device has been tampered with.

2. **Part Number Discrepancies:** Copy the exact part number reported by your OS/diagnostic tool and search for it on the official manufacturer's website. Re-mapped modules often reveal themselves here; for instance, the software might report a part number meant for a 2133MHz 8GB stick, even though the seller labeled it as a 3200MHz 16GB stick.

3. **Mismatched XMP/AMP/JEDEC Profiles:** Review the memory timings and profiles. Fraudulent memory may list high performance speeds (e.g., DDR5 6000) on the sticker, but when you check the JEDEC baseline tables in software, it only supports low fallback speeds.

4. **Early Failures in Loop Testing**: Run a rigorous multi-pass test using a utility. Chips that have been "re-mapped" at the firmware level to hide bad blocks will frequently choke, throw hardware errors, or trigger sudden system halts such as: FAULT_HARDWARE_CORRUPTED_PAGE or MEMORY_MANAGEMENT FAULT or blue screens, when the chip temperature is significantly increased while running under a sustained multi-hour load.