DDR5 Counterfeit, Altered, and Harvesting

1. **Architectural & Physical Risks (Harvested/Altered DRAM) Accelerated Wear and Latent Defects:**
   a) **Harvested DRAM:** From decommissioned servers has already endured thermal cycling and electrical stress. Cells that are currently "good" may be on the verge of wear-out, leading to early life failure (ELF) once deployed in a new enterprise environment.
   b) **Thermal Dissipation Misalignment:** DDR5 introduces the PMIC (Power Management Integrated Circuit) directly onto the module. Third-party or altered modules often use substandard PMICs or poor thermal interface materials, leading to localized hotspots that accelerate DRAM cell degradation.
   c) **Silicon Strain from Down-Binning:** In modules where bad cells were blocked to achieve a lower capacity, the remaining active blocks are often forced to run at timings or voltages they weren't optimized for, decreasing the safety margins for data retention.

2. **Signal Integrity & Firmware Risks (SPD Reprogramming)Spoofed SPD Data (Counterfeiting):**
   a) **Criminal brokers rewrite the Serial Presence Detect (SPD) EEPROM:** Makes a low-grade, slow, or harvested module register to the server bios as a premium, tier-1 OEM part (e.g., spoofing a Micron, Samsung, or SK Hynix original part number).
   b) **PMIC and Hub Vulnerabilities:** DDR5 modules utilize an SPD Hub and a PMIC that communicate via the I^2C/I3C bus. Reprogrammed or counterfeit firmware can cause initialization failures, incorrect voltage scaling, or lack of support for critical vendor-specific telemetry.
   c) **On-Die ECC Masking:** DDR5 features mandatory on-die ECC to manage internal bit flips. In heavily degraded or harvested chips, the rate of internal bit flips can overwhelm the on-die ECC. If the errors are corrected internally but happen constantly, it introduces severe, unpredictable latency spikes that ruin SLA compliance without triggering a system-level alert.

3. **Enterprise System-Level Risks**
   a) **Side-Band Advanced ECC Failures:** Enterprise servers rely on system-level ECC (Chipkill, Adaptive Double Device Data Correction) to survive DRAM chip failures. If a module is constructed of mixed-batch harvested DRAM with varying degradation levels, multi-channel faults can occur simultaneously, overwhelming the server's ability to correct errors and causing a catastrophic Blue Screen / Purple Screen of Death (BSOD/PSOD).
   b) **Machine Check Exceptions (MCEs):** Unstable timing margins on altered modules cause intermittent MCEs. These are difficult for enterprise IT departments to troubleshoot, leading to dozens of wasted engineering hours chasing "ghost" hardware faults.
   c) **Voided OEM Warranties:** If a fortune-500 enterprise unknowingly populates a tier-1 server (Dell, HPE, Lenovo) with spot-market modules that have altered SPDs, it can void the support contract for the entire chassis if discovered during an on-site vendor audit.